

### **Software Safety and Dependable Systems**

Sungdeok (Steve) Cha Dept of Computer Science and Engineering Korea University Seoul, Korea

### http://dependable.korea.ac.kr/



KOREA UNIVERSIT



UCI, 1981



**KAIST** 1994~2008







KNICS (Korea Nuclear I&C System)

Reactor Protection Software



Artificial Heart (HVAD)

#### MIT, 2013



# **KNICS** Project

#### Software qualification for digital safety system $(2001 \sim 2007)$

IEEE Software.

May/June 2009

embedded software.

#### **Formal Modeling** and Verification of Safety-Critical Software

Junbeom Yoo, Konkuk University

Eunkyoung Jee, Korea Advanced Institute of Science and Technology Sungdeok Cha, Korea University

A formal-methodsbased process for developing safety-critical software supports development verification and validation, and safety analysis and has proven to be effective and easy to apply.

igorous quality demonstration is important when developing safety-critical software such as a nuclear power plant's reactor protection system (RPS). Although stakeholders strongly recommend using formal modeling and verification, domain experts often reject such methods because the candidate techniques are overabundant, the notations appear complex, the tools often work only in isolation, and the output is frequently too difficult for domain experts to understand and to extract meaningful information.

also developed CASE tools to let nuclear engineers underlying formalism in depth. In this article, we describe more than seven years' experience working with nuclear engineers in developing RPS software and applying formal methods. Nuclear engineers and regulatory personnel found the process effective and easy to apply with our integrated tool

To overcome such obstacles, we developed a a digital control system for the APR-1400 reactor, formal-methods-based process that supports de- At the project's start, project managers made two velopment, verification, and safety analysis. We decisions that strongly influenced our process:

- apply formal methods without having to know the such as an RPS, we would use formal methods whenever it was practical to do so.
  - Software development would be based on the programmable logic controller (PLC), using function block diagram (FBD) as the implementation language.







# **More on KNICS Project**

- Programmable Logic Controller(PLC)-based software development
  - Using function block diagram (FBD) as the implementation language
  - "Project environment" to our group
- Formal methods were used whenever practical
  - To automate as much analysis as possible
  - To reduce human errors
  - To provide greater safety assurance
  - Our group's own decision





## **Our Approach**



LTL Linear temporal logic



### **Requirements Engieering**





# **Requirements Modeling**





Fig. 7. Finite state machine for history variable node.

| Conditions          |   |   |   |   |
|---------------------|---|---|---|---|
| Cond₁               | ٦ | Γ | - | Т |
| Cond <sub>2</sub>   | F | - | Т | - |
| Cond <sub>3</sub>   | - |   | F | Т |
|                     |   |   |   |   |
| Actions             |   |   |   |   |
| Assign <sub>1</sub> | ) | < |   |   |
| Assign <sub>2</sub> |   |   | Х |   |
| Assign <sub>3</sub> |   |   |   | Х |

Fig. 6. Structured decision table for a function variable.

#### Function node



Fig. 3. Timed transition system for th\_X\_Trip.



# **Requirements Modeling**

- Attempted to balance between readability, expressiveness, and analyzability
  - Preference of stakeholder, in particular the regulatory body, was taken into consideration
  - Approval experience on Wolsung NPP 2-3-4 shutdown system (1995~1997)





# **Requirements Modeling**

• Defined notations AND formal semantics

#### Automated much of requirements analysis

- Completeness, consistency, ...
- Model checking



Available online at www.sciencedirect.com



The Journal of Systems and Software 74 (2005) 73-83

The Journal of Systems and Software

www.elsevier.com/locate/jss

#### A formal software requirements specification method for digital nuclear plant protection systems

Junbeom Yoo<sup>a,\*</sup>, Taihyo Kim<sup>a</sup>, Sungdeok Cha<sup>a</sup>, Jang-Soo Lee<sup>b</sup>, Han Seong Son<sup>b</sup>

 <sup>a</sup> Department of Electrical Engineering and Computer Science, Korea Advanced Institute of Science and Technology (KAIST) and AITrc/SPIC, 373-1, Kusong-dong, Yusong-gu, Taejon 305701, South Korea
 <sup>b</sup> Korea Atomic Energy Research Institute (KAERI), MMIS team, 150, Deokjin-dong, Yusong-gu, Taejon, South Korea

Received 18 March 2003; received in revised form 29 September 2003; accepted 5 October 2003 Available online 30 December 2003

#### Abstract

This article describes NuSCR, a formal software requirements specification method for digital plant protection system in nuclear power plants. NuSCR improves the readability and specifiability by providing graphical or tabular notations depending on the type of operations. NuSCR specifications can be formally analyzed for completeness, consistency, and against the properties specified in temporal logic. We introduce the syntax and semantics of NuSCR and demonstrate the effectiveness of the approach using reactor protection system, digital protection system being developed in Korea, as a case study.



# **SRS Model Checking**



| <b>DSMV</b> input generatior | ۱ |
|------------------------------|---|
| from NuSCR spec.             |   |
|                              |   |
|                              |   |

NuSCR2SMV translator

| SW DEFINE                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                             | 💩 C:WDocuments and Set                                                                     | tingsW지은경WMy Document           | sWEclipsePrjWNuSRS 🔀                    |  |  |  |  |  |  |  |  |
|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|--------------------------------------------------------------------------------------------|---------------------------------|-----------------------------------------|--|--|--|--|--|--|--|--|
| Cerinie Constants Constant Constan                                                                                                                                                                                                                                                                                                                                                                                                                         | SMV                                                                                        |                                 |                                         |  |  |  |  |  |  |  |  |
| - Constants<br>two = 1;<br>fulse = 0;<br>-(m-state_name > state = state_name);<br>inlmL_ = STATE = s1;<br>-(m-state_name = name = name & enable_cond)<br>FROM_InIL_TO-s0-enabled = in_state_name & enable_cond)<br>FROM_InIL_TO-s0-enabled = in_state_name & enable_cond)<br>FROM_InIL_TO-s0-enabled = in_state_name & enable_cond)<br>FROM_InIL_TO-s0-enabled = in_state_name & enable_cond)<br>FROM_InIL_TO-s0-enabled = in_state_d(I_HLLOO_POWER_Opb_Perm_In = failse & (I_HLLOO_POWER_O<br>FROM_INIL_TO-s0-enabled = in_state_d(I_HLLOO_POWER_Obb_Perm_In = failse & (I_HLLOO_POWER_O<br>FROM_INIL_TO-s0-enabled = in_state_d(I_HLLOO_POWER_Obb_Perm_In = failse & (I_HLLOO_POWER_O<br>FROM_INIL_TO-s0-inabled = In_state_d(I_HLLOO_POWER_Obb_Perm_In = failse & (I_HLLOO_POWER_I<br>FROM_INIL_TO-s1-inable = FROM_INIL_TO-s0-inabled;<br>FROM_INIL_TO-s1-inables = FROM_INIL_TO-s0-inabled;<br>FROM_INIL_TO-s1-inables = FROM_INIL_TO-s0-inabled;<br>FROM_INIL_TO-s1-inables = FROM_INIL_TO-s0-inabled;<br>FROM_INIL_TO-s0-inabled;<br>FROM_INIL_TO-s0-inabled;<br>FROM_INIL_TO-s0-inabled;<br>FROM_INIL_TO-s0-inabled;<br>FROM_INIL_TO-s0-inabled;<br>FROM_INIL_TO-s0-inabled;<br>FROM_INIL_TO-s0-inabled;<br>FROM_INIL_TO-s0-inabled;<br>FROM_INIL_TO-s0-inabled;<br>FROM_INIL_TO-s0-inabled;<br>FROM_INIL_TO-s0-inabled;<br>FROM_INIL_TO-s0-inable_init_FILLOO_POWER_OB_DByp_Init= talse & (I_MOd_ErrI_Mod_Err = two<br>Save Close Execution<br>FROM_INIL_TO-s0-inabled;<br>FROM_INIL_IOO_POWER_Val_OUT_HIL_IOO_POWER_Val_OUT In_III_INIL_OO_POWER_VAL_OUT In_III_S0;<br>FROM_INIL_IOO_POWER_VAL_OUT_HIL_IOO_POWER_VAL_OUT In_III_INIL_S0;<br>FROM_INIL_TO-s0-inabled;<br>FROM_INIL_IOO_POWER_VAL_OUT_HIL_IOO_POWER_VAL_OUT In_III_INIL_S0;<br>FROM_INIL_TO-s0-inabled;<br>FROM_INIL_IOO_POWER_VAL_OUT_HIL_IOO_POWER_VAL_OUT In_IIII_INIL_S0;<br>FROM_INIL_IIIIIIIIIIIIIIIIIIIIIIIIIIIIIIIII                                                                                                                                                                                                                                                                                                                                                        | DEFINE                                                                                     |                                 |                                         |  |  |  |  |  |  |  |  |
| TWD = 1:<br>TWD = | - Constants                                                                                |                                 |                                         |  |  |  |  |  |  |  |  |
| Ames - 10;<br>- On-state_name > state = state_name;<br>in-, init = 2TATE = s1;<br>- On-state_name = and = in-state_name & enable_cond;<br>FROM_INIT_TO-30-enabled = inINIT_& & (T.H.L.CO_POWER_Opb_Perm_In = failse & (T.H.L.CO_POWER_OF<br>FROM_INIT_TO-30-enabled = in-state_(T.H.L.CO_POWER_Opb_Perm_In = failse & (T.H.L.CO_POWER_OF<br>FROM_INIT_TO-30-enabled = in-state_(T.H.L.CO_POWER_Opb_Perm_In = failse & (T.H.L.CO_POWER_OF<br>FROM_INIT_TO-30-enabled = in-state_(T.H.L.CO_POWER_Opb_Perm_In = failse & (T.H.L.CO_POWER_OP<br>FROM_INIT_TO-30-enabled = in-state_(T.H.L.CO_POWER_Opb_Perm_In = failse & (T.H.L.CO_POWER_OP<br>FROM_INIT_TO-30-enabled = in-state_(T.H.L.CO_POWER_Opb_Perm_In = failse & (T.H.L.CO_POWER_OP<br>FROM_INIT_TO-31-enabled = in-state_(T.H.L.CO_POWER_Opb_Perm_In = failse & (T.H.L.CO_POWER_OP<br>-0 enabled in- state_INIT_INIT_OF = 1-enabled;<br>FROM_INIT_TO-31-balken = FROM_INIT_TO-30-enabled;<br>FROM_INIT_TO-31-balken = FROM_INIT_TO-30-enabled;<br>FROM_INIT_TO-31-balken = FROM_INIT_TO-30-enabled;<br>FROM_INIT_TO-31-balken = FROM_INIT_TO-30-enabled;<br>FROM_INIT_TO-31-balken = FROM_INIT_TO-30-enabled;<br>FROM_INIT_TO-31-balken = FROM_INIT_TO-30-enabled;<br>FROM_INIT_TO-31-balken = FROM_INIT_TO-30-enabled;<br>FROM_INIT_TO-30-POWER_OP_Byn_INIT_HILLOO_POWER_Op_Byn_Init= tals & (I.M.D.G_EnrI_M.G_Enr = talk<br>Save Close Execution<br>PROPERTY<br>Add(T.H.LLOO_POWER_Op_Byn_INIT_HILLOO_POWER_Op_DByn_Init= tals & (I.M.D.G_EnrI_M.G_Enr = talk<br>SBEC AO(T.H.LLOO_POWER_Op_Byn_INIT_HILLOO_POWER_Op_DByn_Init= talk & (I.M.D.G_EnrI_M.G_Enr = talk<br>SBEC AO(T.H.LLOO_POWER_Op_Byn_INIT_HILLOO_POWER_Op_DByn_Init= talk & (I.M.D.G_EnrI_M.G_EnrI_M.G_ENR_OP_B)n_INIT_HILLOO_POWER_Op_DByn_Init= talk & (I.M.G_EnrI_M.G_ENR_OP_B)n_INIT_HILLOO_POWER_OP_DByn_INIT_FILE_0D_POWER_OP_DByn_INIT_FILE_0D_POWER_OP_DByn_INIT_FILE_0D_POWER_TIN_LOD_FILE_0D_POWER_OP_DByn_INIT_FILE_0D_POWER_OP_DByn_INIT_FILE_0D_POWER_OP_DByn_INIT_FILE_0D_POWER_OP_DByn_INIT_FILE_0D_POWER_OP_DByn_INIT_FILE_0D_POWER_OP_DByn_INIT_FILE_0D_POWER_OP_DD_PN_INIT_FILE_0D_POWER_OP_DByn_INIT_FILE_0D_POWER_OP_DByn_INIT_                                                                                                                                                                                                                                                                                                                                                                            | true := 1:                                                                                 |                                 |                                         |  |  |  |  |  |  |  |  |
|                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                       | false = 0                                                                                  |                                 |                                         |  |  |  |  |  |  |  |  |
| In_julSTATE = sit;<br>                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                | (in-state name := state = state name)                                                      |                                 |                                         |  |  |  |  |  |  |  |  |
| n-0.9 = STATE = sq.<br>n-0.9 = STATE = sq.<br>-dranation_name-enabled = in-istle_name & enable_cont)<br>FROM_bit_OC-0-0-enabled = in-istle_(T_H_LOO_POWER_Opb_Perm_in= failse & (T_H_LOO_POWER_Opb_Perm_in= failse & (T_H_LOO_POWER_Opb_Perm_in                                                                                                                                                                                                                                                                                                                                                                                                                  | in, init = STATE = init :                                                                  |                                 |                                         |  |  |  |  |  |  |  |  |
| n-1 = STATE = s1;<br>(                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                | in-s0 = STATE = s0:                                                                        |                                 |                                         |  |  |  |  |  |  |  |  |
| -dranstion_name-inabided = Ini-citité_name & enable_cond) FROM-Init_CT-O-Enabled = Ini-citité_name & enable, Cond) FROM-Init_CT-O-Enabled = Ini-sitité_(LH_LLOO_POWER_Ob_Perm_In= failes & & (LH_LOO_POWER_FROM=) FROM-Init_CT-O-Enabled = Ini-sitité_(LH_LLOO_POWER_Ob_Perm_In= failes & & (LH_LLOO_POWER_FROM=) FROM-Init_CT-O-Enabled = Ini-sitité_(LH_LLOO_POWER_Ob_Perm_In= failes & (LH_LLOO_POWER_FROM=) FROM-Init_CT-O-Enabled = Ini-sitité_(LH_LLOO_POWER_Ob_Perm_In= failes & (LH_LLOO_POWER_FROM=) FROM-Init_CT-O-Enabled = Ini-sitité_(LH_LLOO_POWER_Ob_Perm_In= failes & (LH_LLOO_POWER_FROM=) FROM-Init_CT-Eit-Inabled = Ini-sitité_(LH_LOO_POWER_I) Save Close Execution PROPERTY                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                      | n-s1 := STATE = s1                                                                         |                                 |                                         |  |  |  |  |  |  |  |  |
| FROM_INIT_O-D-D-Dabled = In:_Init_& & (C HI_LOO_POWER_Opb_Perm_In= failss & & (HI_LOO_POWER<br>FROM-IshT-O-B-Dabled = In:SI & (C HI_LOO_POWER_Obb_Perm_In= failss & & (HI_LOO_POWER_<br>FROM-IshT-O-B-Dabled = In:SI & & (C HI_LOO_POWER_Obb_Perm_In= failss & & (HI_LOO_POWER_<br>FROM-IshT-O-B-Dabled = In:SI & & (C HI_LOO_POWER_Obb_Perm_In= failss & & (HI_LOO_POWER_<br>FROM-IshT-O-B-Dabled = In:SI & & (C HI_LOO_POWER_Obb_Perm_In= failss & & (HI_LOO_POWER_<br>-0"anation_name-taken = #Tanailon_Int_O-B-Dabled;<br>FROM-IshT-O-B-Dabled = In:SI & & (C HI_LOO_POWER_Obb_Perm_In= failss & & (HI_LOO_POWER_<br>-0"anation_name-taken = #Tanailon_Int_O-B-Dabled;<br>FROM-IshT-O-B-Dabled = In:SI & U (HI_LOO_POWER_Obb_Perm_In= failss & (HI_LOO_POWER_<br>-0"anation_name-taken = #Tanailon_Int_O-B-Dabled;<br>FROM-IshT-O-B-Dabled = In:SI & U (HI_LOO_POWER_Obb_Perm_In= failss & (HI_LOO_POWER_<br>-0"anation_name-taken = #TANAILO_IN_I-TO-B-I-mabled;<br>FROM-IshT-O-B-Dabled = In:SI & U (HI_LOO_POWER_Obb_Perm_In= failss & (HI_LOO_POWER_<br>-0"anation_name-taken = #TANAILO_IN_I-TO-B-I-mabled;<br>FROM-IshT-O-B-Dabled = In:SI & U (HI_LOO_POWER_Obb_Perm_In= failss & (HI_LOO_POWER_<br>-0"anation_name-taken = #TANAILO_IN_I-TO-B-I-mabled;<br>FROM-IshT-O-B-I-Dabled = In:SI & U (HI_LOO_POWER_Obb_Perm_In= failss & (HI_LOO_POWER_Obb_Perm_In=                                                                                                                                                                                                                                                                                                                                                                                          | -(transition name-enabled := in-st                                                         | tate name & enable cond)        |                                         |  |  |  |  |  |  |  |  |
| FROM-SIT-O-B-nabled =: in=s0 <sup>®</sup> c(C)_HL_CO_POVER_Ob_Parm_In=fulse & d, H_LOO_POVER_C<br>FROM-SIT-O-B-nabled =: in=s1 <sup>®</sup> c(C)_HL_CO_POVER_Ob_Parm_In=fulse & d, H_LOO_POVER_C<br>FROM-SIT-O-B-nabled =: in=s1 <sup>®</sup> c(C)_HL_CO_POVER_Ob_POVER_In=fulse & d, H_LOO_POVER_C<br>FROM-SIT-O-B-nabled =: in=s1 <sup>®</sup> c(C)_HL_CO_POVER_Ob_POVER_In=fulse & d, H_LOO_POVER_C<br>- danation_name-stables<br>FROM-SIT-O-B-nabled =: in=s1 <sup>®</sup> c(C)_HL_CO_POVER_Ob_POVER_In=fulse & d, H_LOO_POVER_C<br>- danation_name-stables<br>FROM-SIT-O-B-nabled =: from_InITO-SI-B-nabled;<br>FROM-SIT-O-B-Intens = FROM-SIT-SIB-B-inabled;<br>FROM-SIT-O-B-Intens = FROM-SIT-SIB-B-inabled;<br>FROM-SIT-O-B-INAM = FROM-SIT-SIB-B-INBLED;<br>FROM-SIT-O-B-INAM = FROM-SIT-SIB-B-INBLED;<br>FROM-SIT-SIB-B-INBLED;<br>FROM-SIT-SIB-B-INBLED;<br>FROM-SIT-SIB-B-INBLED;<br>FROM-SIT-SIB-B-INBLED;<br>FROM-SIT-SIB-B-INBLED;<br>FROM-SIT-SIB-B-INBLED;<br>FROM-SIT-SIB-B-INBLED;<br>FROM-SIT-SIB-B-INBLED;<br>FROM-SIT-SIB-B-INBLED;<br>FROM-SIT-SIB-B-INBLED;<br>FROM-SIT-SIB-B-INBLED;<br>FROM-SIT-SIB-B-INBLED;<br>FRO                                                                                                                                                                                                                                                                           | FROMinitTO-s0-enabled := in-                                                               | _init_ & ((f_HI_LOG_POWER_Opb_F | Perm_In = false & (f_HI_LOG_POW         |  |  |  |  |  |  |  |  |
| FROM-s11-TO-s10-anabled s: In-s1 & (CL+LLOO_POWER_Ob_Perm_In- failes & (L+LLOO_POWER_Ob_Perm_In- failes & (L+LLOO_POWER_                                                                                                                                                                                                                                                                                                                                                                                                                         | FROM-s0-TO-s0-enabled := in-s0                                                             | & ((f_HI_LOG_POWER_Opb_Perm_    | In = false & (f_HI_LOG_POWER_C          |  |  |  |  |  |  |  |  |
| FROM-UIL, TO-51-enabled = In:_Int_& & (f(H_LLOO_POWER_Opb_Perm_In = failse & (H_LLOO_POWER_FROM=517-51-enabled = Init & (ICH_LLOO_POWER_Opb_Perm_In = failse & (H_LLOO_POWER_) FROM=517-51-enabled = Init & (ICH_LLOO_POWER_Opb_Perm_In = failse & (H_LLOO_POWER_) FROM=517-51-enabled = FROM=Int_TO-50-enabled; FROM=517-51-enabled = FROM=Int_TO-50-enabled; FROM=517-51-enabled = FROM=517-51-enabled; FROM=517-51-enabled = FROM=517-51-enabled; FROM=517-51-51-enabled; FROM=517-51-51-enabled; FROM=517-51-51-51-51-51-51-51-51-51-51-51-51-51-                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                        | FROM-s1-TO-s0-enabled := in-s1                                                             | & ((f_HI_LOG_POWER_Opb_Perm_    | In = false & (f_HI_LOG_POWER_C          |  |  |  |  |  |  |  |  |
| FROM-ShT-O-1-mabled = In-10 & (I'(_HL_LO_0_COVER_Ob_Perm_In = failes & (I_HL_LOPOVER (Tanation_name-taken = transition_name-enabled) FROM-shT-O-1-batken = FROM-shT-O-2-0-mabled, FROM-shT-O-3-batken = FROM-shT-O-3-0-mabled, FROM-shT-O-3-1-aken = FROM-shT-O-3-0-mabled, FROM-shT-                                                                                                                                                                                                                                                                                                                                                                                                                               | FROMinitTO-s1-enabled := ininit_ & (I(f_HI_LOG_POWER_Opb_Perm_In = false & (f_HI_LOG_POW   |                                 |                                         |  |  |  |  |  |  |  |  |
| FROM-51T-C-51-enabled_init-51 & (f(_1H_LOO_POWER_OpE_Perru_In = failse & (t_1H_LOO_POWER_I)           Granstion_name-states           FROM_51T-C-51-enabled,           FROM_51T                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                         | FROM-s0-TO-s1-enabled := in-s0                                                             | & (I(f_HI_LOG_POWER_Opb_Perm    | _in = faise & (f_HI_LOG_POWER_(         |  |  |  |  |  |  |  |  |
| - dranation_name-taken = transition_name-enabled; - frook_init_To-50-tabled; - Frook_init_To-50-tabled; - Frook_init_To-50-tabled; - Frook_init_To-51-taken = FROM_init_To-50-tabled; - Frook_init_To-51-taken = FROM_init_To-51-tanabled; - Frook_init_To-51-taken = Frook_init_To-51-tanabled; - Frook_init_To-51-taken = Frook_init_To-51-taken; - Frook_init_To-                                                                                                                                                                                                                                                                                                                                                                                                                         | FROM-s1-TO-s1-enabled := in-s1 & (I(f_HI_LOG_POWER_Opb_Perm_In = false & (f_HI_LOG_POWER_0 |                                 |                                         |  |  |  |  |  |  |  |  |
| FROM_III_TO-60-taken = FROM_III_TO-60-enabled; FROM =01-06-taken = FROM_SINC_06-enabled; FROM =01-06-taken = FROM-sinC-06-enabled; FROM_III_TO-61-taken = FROM-sinC-61-enabled; FROM =10-06-taken = FROM-sinC-61-enabled; FROM =10-06-taken = FROM-sinC-61-enabled; Save Close Execution PROPERTY N0(f_HI_LO0_POWER_Op_Byp_Init_HI_LO6_POWER_Op_Byp_Init= frue & (f_Mod_Err L Mod_Err = true SPEC Ad(f_HI_LO0_POWER_Val_Out_HI_LO0_POWER_Val_Out = th_II_LO0_POWER_Top_Dyp_Init= frue & (f_Mod_Err I_Mod_Err = true)                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                  | (transition_name-taken := transiti                                                         | on_name-enabled)                |                                         |  |  |  |  |  |  |  |  |
| FROM-5D70-5D1aken = FROM-5D70-5D-enabled;<br>FROM-5170-6b1aken = FROM-5D70-6D-enabled;<br>FROM-5U1420-5D1-2D-enabled;<br>FROM-5D10-51-54-5D2-51-enabled;<br>FROM-5170-51-54-5D2-51-enabled;<br>FROM-5170-51-54-50-51-51-enabled;<br>FROM-5170-51-54-54-50-51-70-51-enabled;<br>FROM-5170-51-54-54-52-52-54-54-54-54-54-54-54-54-54-54-54-54-54-                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                       | ROMinitTO-s0-taken := FROM                                                                 | initTO-s0-enabled;              |                                         |  |  |  |  |  |  |  |  |
| FROM =17-0-90-taken = FROM-s1-T0-90-enabled;       FROM =17-0-51-taken = FROM-s0-T0-91-enabled;       FROM =10-51-taken = FROM-s0-T0-91-enabled;       FROM =10-51-taken = FROM-s0-T0-91-enabled;       Save     Close       Execution       PROPERTY       Soft_H1_L00_POWER_Op_Byp_Init_H1_L00_POWER_Op_Byp_Init= true & (f_Mod_Err End_Lerr = true<br>spec Ao(f_H1_L00_POWER_Val_out_H1_L00_POWER_Val_out_m_H1_L00_POWER_T0_p_Byp_Init= failes & if_Mod_Errf_Mod_Err       Sec Ao(f_H1_L00_POWER_Op_Byp_Init_H1_L00_POWER_Val_out_m_H1_L00_POWER_T0_p_Dyp_Init= failes & if_Mod_Errf_Mod_Errf_Mod_Errf_Mod_Errf_Mod_Errf_Mod_Errf_Mod_Errf_Mod_Errf_Mod_Errf_Mod_Errf_Mod_Errf_Mod_Errf_Mod_Errf_Mod_Errf_Mod_Errf_Mod_Errf_Mod_Errf_Mod_Errf_Mod_Errf_Mod_Errf_Mod_Errf_Mod_Errf_Mod_Errf_Mod_Errf_Mod_Errf_Mod_Errf_Mod_Errf_Mod_Errf_Mod_Errf_Mod_Errf_Mod_Errf_Mod_Errf_Mod_Errf_Mod_Errf_Mod_Errf_Mod_Errf_Mod_Errf_Mod_Errf_Mod_Errf_Mod_Errf_Mod_Errf_Mod_Errf_Mod_Errf_Mod_Errf_Mod_Errf_Mod_Errf_Mod_Errf_Mod_Errf_Mod_Errf_Mod_Errf_Mod_Errf_Mod_Errf_Mod_Errf_Mod_Errf_Mod_Errf_Mod_Errf_Mod_Errf_Mod_Errf_Mod_Errf_Mod_Errf_Mod_Errf_Mod_Errf_Mod_Errf_Mod_Errf_Mod_Errf_Mod_Errf_Mod_Errf_Mod_Errf_Mod_Errf_Mod_Errf_Mod_Errf_Mod_Errf_Mod_Errf_Mod_Errf_Mod_Errf_Mod_Errf_Mod_Errf_Mod_Errf_Mod_Errf_Mod_Errf_Mod_Errf_Mod_Errf_Mod_Errf_Mod_Errf_Mod_Errf_Mod_Errf_Mod_Errf_Mod_Errf_Mod_Errf_Mod_Errf_Mod_Errf_Mod_Errf_Mod_Errf_Mod_Errf_Mod_Errf_Mod_Errf_Mod_Errf_Mod_Errf_Mod_Errf_Mod_Errf_Mod_Errf_Mod_Errf_Mod_Errf_Mod_Errf_Mod_Errf_Mod_Errf_Mod_Errf_Mod_Errf_Mod_Errf_Mod_Errf_Mod_Errf_Mod_Errf_Mod_Errf_Mod_Errf_Mod_Errf_Mod_Errf_Mod_Errf_Mod_Errf_Mod_Errf_Mod_Errf_Mod_Errf_Mod_Errf_Mod_Errf_Mod_Errf_Mod_Errf_Mod_Errf_Mod_Errf_Mod_Errf_Mod_Errf_Mod_Errf_Mod_Errf_Mod_Errf_Mod_Errf_Mod_Errf_Mod_Errf_Mod_Errf_Mod_Errf_Mod_Errf_Mod_Errf_Mod_Errf_Mod_Errf_Mod_Errf_Mod_Errf_M                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                               | ROM-s0-T0-s0-taken := FROM-s0                                                              | J-TO-s0-enabled;                |                                         |  |  |  |  |  |  |  |  |
| FROM_Init_TO-s1-laken = FROM_Init_TO-s1-enabled;       FROM =0.70-s1-laken = FROM_s1-TO-s1-enabled;       FROM =1.70-s1-laken = FROM_s1-TO-s1-enabled;       Image: Save                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                              | FROM-s1-TO-s0-taken := FROM-s1                                                             | -TO-s0-enabled;                 |                                         |  |  |  |  |  |  |  |  |
| ROWEDTO-S1-taken = RFOM-b0Tc-S1-enabled;<br>ROWETO-S1-taken = RFOM-b1TC-S1-enabled;<br>Save Close Execution<br>PROPERTY<br>NG(LHILLOG_POWER_Op_Byp_InitLHILLOG_POWER_Op_Byp_Init= true & (C_Mod_ErrLMod_Err = true<br>STORE Val_ULOG_POWER_Op_Byp_InitLHILLOG_POWER_Op_Byp_Init= failes & (M_Mod_ErrLMod_Err<br>Store = Store = St                                                                                                                                                                                                                                                                                                                                                                                                            | FROMinitTO-s1-taken := FROM                                                                | initTO-s1-enabled;              | E                                       |  |  |  |  |  |  |  |  |
| FROM 51 TO-51 taken = FROM-51 TO-51-enabled;       Save     Close       Execution       PROPERTY       Sec As(f_LLOG_POWER_Op_Byp_Init[HIL_LOG_POWER_Op_Byp_Init] = flue & (f_Mod_Err f_Mod_Err = flue Bec As(f_HL_LOG_POWER_Val_Out + m_HL_LOG_POWER_Tinp_Logic k, SPEC As(f_HL_LOG_POWER_Op_Byp_Init] = failse & (f_Mod_Errf_Mod_Errf_Mod_Errf_Mod_Errf_Mod_Errf_Mod_Errf_Mod_Errf_Mod_Errf_Mod_Errf_Mod_Errf_Mod_Errf_Mod_Errf_Mod_Errf_Mod_Errf_Mod_Errf_Mod_Errf_Mod_Errf_Mod_Errf_Mod_Errf_Mod_Errf_Mod_Errf_Mod_Errf_Mod_Errf_Mod_Errf_Mod_Errf_Mod_Errf_Mod_Errf_Mod_Errf_Mod_Errf_Mod_Errf_Mod_Errf_Mod_Errf_Mod_Errf_Mod_Errf_Mod_Errf_Mod_Errf_Mod_Errf_Mod_Errf_Mod_Errf_Mod_Errf_Mod_Errf_Mod_Errf_Mod_Errf_Mod_Errf_Mod_Errf_Mod_Errf_Mod_Errf_Mod_Errf_Mod_Errf_Mod_Errf_Mod_Errf_Mod_Errf_Mod_Errf_Mod_Errf_Mod_Errf_Mod_Errf_Mod_Errf_Mod_Errf_Mod_Errf_Mod_Errf_Mod_Errf_Mod_Errf_Mod_Errf_Mod_Errf_Mod_Errf_Mod_Errf_Mod_Errf_Mod_Errf_Mod_Errf_Mod_Errf_Mod_Errf_Mod_Errf_Mod_Errf_Mod_Errf_Mod_Errf_Mod_Errf_Mod_Errf_Mod_Errf_Mod_Errf_Mod_Errf_Mod_Errf_Mod_Errf_Mod_Errf_Mod_Errf_Mod_Errf_Mod_Errf_Mod_Errf_Mod_Errf_Mod_Errf_Mod_Errf_Mod_Errf_Mod_Errf_Mod_Errf_Mod_Errf_Mod_Errf_Mod_Errf_Mod_Errf_Mod_Errf_Mod_Errf_Mod_Errf_Mod_Errf_Mod_Errf_Mod_Errf_Mod_Errf_Mod_Errf_Mod_Errf_Mod_Errf_Mod_Errf_Mod_Errf_Mod_Errf_Mod_Errf_Mod_Errf_Mod_Errf_Mod_Errf_Mod_Errf_Mod_Errf_Mod_Errf_Mod_Errf_Mod_Errf_Mod_Errf_Mod_Errf_Mod_Errf_Mod_Errf_Mod_Errf_Mod_Errf_Mod_Errf_Mod_Errf_Mod_Errf_Mod_Errf_Mod_Errf_Mod_Errf_Mod_Errf_Mod_Errf_Mod_Errf_Mod_Errf_Mod_Errf_Mod_Errf_Mod_Errf_Mod_Errf_Mod_Errf_Mod_Errf_Mod_Errf_Mod_Errf_Mod_Errf_Mod_Errf_Mod_Errf_Mod_Errf_Mod_Errf_Mod_Errf_Mod_Errf_Mod_Errf_Mod_Errf_Mod_Errf_Mod_Errf_Mod_Errf_Mod_Errf_Mod_Errf_Mod_Errf_Mod_Errf_Mod_Errf_Mod_Errf_Mod_Errf_Mod_Errf_Mod_Errf_Mod_Errf_Mod_Errf_Mod_Errf_Mod_Errf_Mod_Errf_Mod_Errf_Mod_Errf_Mod_Errf_Mod_Errf_Mod_Errf_Mod_Errf_Mod_Errf_Mod_Errf_Mod_Errf_Mod_Errf_Mod_Errf_Mo                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                          | FROM-s0-TO-s1-taken := FROM-s0                                                             | J-TO-s1-enabled;                |                                         |  |  |  |  |  |  |  |  |
| Save     Close     Execution     PROPERTY     Nod_Enr_Log_POWER_Op_Byp_Init_HILLOG_POWER_Op_Byp_Init=true & (f_Mod_Enr_LMod_Enr=true     Acd(_HI_LOG_POWER_Val_Out_HILLOG_POWER_Val_Out_HILLOG_POWER_Val_Out_HILLOG_POWER_Val_Out_HILLOG_POWER_Val_Out_HILLOG_POWER_Val_Out_HILLOG_POWER_Val_Out_HILLOG_POWER_Val_Out_HILLOG_POWER_Val_Out_HILLOG_POWER_Val_Out_HILLOG_POWER_Val_Out_HILLOG_POWER_Val_Out_HILLOG_POWER_Val_Out_HILLOG_POWER_Val_Out_HILLOG_POWER_Val_Out_HILLOG_POWER_Val_Out_HILLOG_POWER_Val_Out_HILLOG_POWER_Val_Out_HILLOG_POWER_Val_Out_HILLOG_POWER_Val_Out_HILLOG_POWER_Val_Out_HILLOG_POWER_Val_Out_HILLOG_POWER_Val_Out_HILLOG_POWER_Val_Out_HILLOG_POWER_Val_Out_HILLOG_POWER_Val_OUt_HILLOG_POWER_Val_OUt_HILLOG_POWER_Val_OUt_HILLOG_POWER_Val_OUt_HILLOG_POWER_Val_OUt_HILLOG_POWER_Val_OUt_HILLOG_POWER_Val_OUt_HILLOG_POWER_Val_OUt_HILLOG_POWER_Val_OUt_HILLOG_POWER_Val_OUt_HILLOG_POWER_Val_OUt_HILLOG_POWER_Val_OUt_HILLOG_POWER_Val_OUt_HILLOG_POWER_Val_OUt_HILLOG_POWER_Val_OUt_HILLOG_POWER_Val_OUt_HILLOG_POWER_Val_OUt_HILLOG_POWER_Val_OUt_HILLOG_POWER_Val_OUt_HILLOG_POWER_Val_OUt_HILLOG_POWER_Val_OUt_HILLOG_POWER_Val_OUt_HILLOG_POWER_VAL_OUT_HILLOG_POWER_VAL_OUT_HILLOG_POWER_VAL_OUT_HILLOG_POWER_VAL_OUT_HILLOG_POWER_VAL_OUT_HILLOG_POWER_VAL_OUT_HILLOG_POWER_VAL_OUT_HILLOG_POWER_VAL_OUT_HILLOG_POWER_VAL_OUT_HILLOG_POWER_VAL_OUT_HILLOG_POWER_VAL_OUT_HILLOG_POWER_VAL_OUT_HILLOG_POWER_VAL_OUT_HILLOG_POWER_VAL_OUT_HILLOG_POWER_VAL_OUT_HILLOG_POWER_VAL_OUT_HILLOG_POWER_VAL_OUT_HILLOG_POWER_VAL_OUT_HILLOG_POWER_VAL_OUT_HILLOG_POWER_VAL_OUT_HILLOG_POWER_VAL_OUT_HILLOG_POWER_VAL_OUT_HILLOG_POWER_VAL_OUT_HILLOG_POWER_VAL_OUT_HILLOG_POWER_VAL_OUT_HILLOG_POWER_VAL_OUT_HILLOG_POWER_VAL_OUT_HILLOG_POWER_VAL_OUT_HILLOG_POWER_VAL_OUT_HILLOG_POWER_VAL_OUT_HILLOG_POWER_VAL_OUT_HILLOG_POWER_VAL_OUT_HILLOG_POWER_VAL_OUT_HILLOG_POWER_VAL_OUT_HILLOG_POWER_VAL_OUT_HILLOG_POWER_VAL_OUT_HILLOG_POWER_VAL_OUT_HILLOG_POWER_VAL_OUT_HILLOG_POWER_VAL_OUT_HILLOG_POWER_VAL_OUT_HILLOG_POWER_VAL_OUT_HILLOG_POWER_VAL_OUT_HILLOG_POWER_VAL_OUT_HILLOG_PO                                                                                                                                                                                                                                                                                                                                                                                                                             | FROM-s1-TO-s1-taken := FROM-s1                                                             | -TO-s1-enabled;                 | -                                       |  |  |  |  |  |  |  |  |
| Save         Close         Execution           PROPERTY                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                               | < II.                                                                                      |                                 |                                         |  |  |  |  |  |  |  |  |
| PROPERTY<br>AGY_HLLOG_POWER_Op_Byn_Init[HL_LOG_POWER_Op_Byn_Init= brus & (fMod_Err f_Mod_Err = brus<br>BREC AGY_HL_DOG_POWER_Val_Out FH_LOG_POWER_Val_Out = bru_HL_LOG_POWER_Titip_Lopic k;<br>BREC AGY_HL_DOG_POWER_Op_Byn_Init[HL_LOG_POWER_Op_Byn_Init= failes & (fMod_Errf_Mod_E                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                  | Save                                                                                       | Close                           | Execution                               |  |  |  |  |  |  |  |  |
| AG(",HI_LOG_POWER_OP_BYp_Init("HI_LOG_POWER_OP_BYp_Init="bue & ("_Mod_Err", Mod_Err="bue<br>SPEC.AG((",HI_LOG_POWER_Val_out[",HI_LOG_POWER_Val_out > m_HI_LOG_POWER_Tho_Logic k,<br>SPEC.AG(",HI_LOG_POWER_OP_BYp_Init_HI_LOG_POWER_OP_BYp_Init="failes & d"_Mod_Err", Mod_E                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                          | PROPERTY                                                                                   |                                 |                                         |  |  |  |  |  |  |  |  |
| AGC/H_LOG_POWER_Op_Bp_Init[H_LOG_POWER_Op_Bpy_Init=twa & d[Mod_Err_Mod_Err_Mod_Err_Mod_Err_Mod_Err_Mod_Err_Mod_Err_Mod_Err_Mod_Err_Mod_Err_Mod_Err_Mod_Err_Mod_Err_Mod_Err_Mod_Err_Mod_Err_Mod_Err_Mod_Err_Mod_Err_Mod_Err_Mod_Err_Mod_Err_Mod_Err_Mod_Err_Mod_Err_Mod_Err_Mod_Err_Mod_Err_Mod_Err_Mod_Err_Mod_Err_Mod_Err_Mod_Err_Mod_Err_Mod_Err_Mod_Err_Mod_Err_Mod_Err_Mod_Err_Mod_Err_Mod_Err_Mod_Err_Mod_Err_Mod_Err_Mod_Err_Mod_Err_Mod_Err_Mod_Err_Mod_Err_Mod_Err_Mod_Err_Mod_Err_Mod_Err_Mod_Err_Mod_Err_Mod_Err_Mod_Err_Mod_Err_Mod_Err_Mod_Err_Mod_Err_Mod_Err_Mod_Err_Mod_Err_Mod_Err_Mod_Err_Mod_Err_Mod_Err_Mod_Err_Mod_Err_Mod_Err_Mod_Err_Mod_Err_Mod_Err_Mod_Err_Mod_Err_Mod_Err_Mod_Err_Mod_Err_Mod_Err_Mod_Err_Mod_Err_Mod_Err_Mod_Err_Mod_Err_Mod_Err_Mod_Err_Mod_Err_Mod_Err_Mod_Err_Mod_Err_Mod_Err_Mod_Err_Mod_Err_Mod_Err_Mod_Err_Mod_Err_Mod_Err_Mod_Err_Mod_Err_Mod_Err_Mod_Err_Mod_Err_Mod_Err_Mod_Err_Mod_Err_Mod_Err_Mod_Err_Mod_Err_Mod_Err_Mod_Err_Mod_Err_Mod_Err_Mod_Err_Mod_Err_Mod_Err_Mod_Err_Mod_Err_Mod_Err_Mod_Err_MOd_Err_Mod_Err_Mod_Err_Mod_Err_Mod_Err_Mod_Err_Mod_Err_Mod_Err_Mod_Err_Mod_Err_Mod_Err_Mod_Err_Mod_Err_Mod_Err_Mod_Err_Mod_Err_Mod_Err_Mod_Err_Mod_Err_Mod_Err_Mod_Err_Mod_Err_Mod_Err_Mod_Err_Mod_Err_Mod_Err_Mod_Err_Mod_Err_Mod_Err_Mod_Err_Mod_Err_Mod_Err_Mod_Err_Mod_Err_Mod_Err_Mod_Err_Mod_Err_Mod_Err_Mod_Err_Mod_Err_Mod_Err_Mod_Err_Mod_Err_Mod_Err_Mod_Err_Mod_Err_Mod_Err_Mod_Err_Mod_Err_Mod_Err_Mod_Err_Mod_Err_Mod_Err_Mod_Err_Mod_Err_Mod_Err_Mod_Err_Mod_Err_Mod_Err_Mod_Err_Mod_Err_Mod_Err_Mod_Err_Mod_Err_MOD_Err_Mod_Err_Mod_Err_Mod_Err_Mod_Err_Mod_Err_Mod_Err_Mod_Err_Mod_Err_Mod_Err_Mod_Err_Mod_Err_Mod_Err_Mod_Err_Mod_Err_Mod_Err_Mod_Err_Mod_Err_Mod_Err_Mod_Err_Mod_Err_Mod_Err_Mod_Err_Mod_Err_Mod_Err_Mod_Err_Mod_Err_MOD_Err_MOD_Err_MOD_Err_MOD_Err_MOD_Err_MOD_Err_MOD_Err_MOD_Err_MOD_Err_MOD_Err_MOD_Err_MOD_Err_MOD_Err_MOD_Err_MOD_Err_MOD_Err_MOD_Err_MOD_Err_MOD_Err_MOD_Err_MOD_Err_MOD_Err_MOD_Err_MOD_Err_MOD_Err_MOD_Err_MOD_Err_MOD_Err_MOD_Err_MOD_Err_MOD_Err_MOD_Err_MOD_Err_MOD_Err_MOD_Err_MOD_Err_MOD_Err_MO                                                                                                                                                                                                                                                                                                                                                                                                                         |                                                                                            |                                 |                                         |  |  |  |  |  |  |  |  |
| SPEC.AG((T,HI_LOG_POWER_Val_out_HI_LOG_POWER_Val_out > m_HI_LOG_POWER_Thip_Logic k,<br>SPEC.AG((,HI_LOG_POWER_Op_Byp_Init_HI_LOG_POWER_Op_Byp_Init=failse & (f_Mod_Errf_Mod_E                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                         | AG(f_HI_LOG_POWER_Op_Byp_Ir                                                                | nitf_HI_LOG_POWER_Op_Byp_Init=  | true & (f_Mod_Err.f_Mod_Err = true   f_ |  |  |  |  |  |  |  |  |
| SPEC AG((_HI_LOG_POWER_Op_Byp_Init_HI_LOG_POWER_Op_Byp_Init=failse & ((_Mod_Errf_Mod_E                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                | SPEC AG((f_HI_LOG_POWER_Val                                                                | _Outf_HI_LOG_POWER_Val_Out > ti | h_HI_LOG_POWER_Trip_Logic.k_HI          |  |  |  |  |  |  |  |  |
| < III                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                 | SPEC AG(f_HI_LOG_POWER_Op_                                                                 | _Byp_Init.f_HI_LOG_POWER_Op_Byp | _Init = false & (f_Mod_Err.f_Mod_Err =  |  |  |  |  |  |  |  |  |
| <   II   1   1   1   1   1   1   1   1                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                |                                                                                            |                                 |                                         |  |  |  |  |  |  |  |  |
| <                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                     |                                                                                            |                                 |                                         |  |  |  |  |  |  |  |  |
| IIIIIIIIIIIIIIIIIIIIIIIIIIIIIIIIIIII                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                  |                                                                                            |                                 |                                         |  |  |  |  |  |  |  |  |
|                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                       | • II                                                                                       |                                 | •                                       |  |  |  |  |  |  |  |  |
| Apply                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                 |                                                                                            | Apply                           |                                         |  |  |  |  |  |  |  |  |

#### $\uparrow @$ Insert properties

| 74 default.smv 📃 🗆 🔀                                                                                                                                               |  |  |  |  |  |  |  |  |  |  |
|--------------------------------------------------------------------------------------------------------------------------------------------------------------------|--|--|--|--|--|--|--|--|--|--|
| <u>File Prop View Goto History Abstraction</u>                                                                                                                     |  |  |  |  |  |  |  |  |  |  |
| Browser Properties Results Cone Using Groups                                                                                                                       |  |  |  |  |  |  |  |  |  |  |
| All results                                                                                                                                                        |  |  |  |  |  |  |  |  |  |  |
| Property Result                                                                                                                                                    |  |  |  |  |  |  |  |  |  |  |
| (AG ((([HI_LOG_POWER_Op_Byp_Init.f_HI_LOG_POWER_Op_Byp_Init=1)&((([M failse Wed Jan 04 15:1                                                                        |  |  |  |  |  |  |  |  |  |  |
| I                                                                                                                                                                  |  |  |  |  |  |  |  |  |  |  |
| Source Trace Log                                                                                                                                                   |  |  |  |  |  |  |  |  |  |  |
| Fil <u>e</u>                                                                                                                                                       |  |  |  |  |  |  |  |  |  |  |
| [Optimized conjunctive relation: comps = 1, size = 1955]         []           [optimized transition relation size: 1955]         .0.171875 s           system time |  |  |  |  |  |  |  |  |  |  |
| <pre>luser time</pre>                                                                                                                                              |  |  |  |  |  |  |  |  |  |  |
| See file "default.warh" for warhings.<br>user time                                                                                                                 |  |  |  |  |  |  |  |  |  |  |

←③Model checking using SMV

#### $\downarrow$ ④Verification Result Analysis

Model checking results

(AG (((f\_HI\_LOG\_POWER\_Op\_Byp\_Init.f\_HI\_LOG\_POWER\_Op\_Byp\_Init=1) &(((f\_M... false



### **FBD Synthesis**

# • Was feasible due to relatively small (and intended) semantic gap





# Synthesized FBD was NOT Optimized

#### state- and history-dependent nodes posed challenge

#### Table 1

Comparison of the number of FBD blocks included in the fixed set-point rising trip logic

|                                           | f_X_Valid | th_X_Trip | th_X_Pretrip | F_X_OB_Perm | h_X_OB_Sta | Total |
|-------------------------------------------|-----------|-----------|--------------|-------------|------------|-------|
| System atically gen-<br>erated from NuSCR | 3         | 39        | 16           | 2           | 11         | 71    |
| Manually generated<br>by experts          | 3         | 12        | 8            | 9           |            | 32    |

Number of function blocks used.

#### Table 2

Comparison of the number of function blocks used for the representative trip logics in BP

| Trip logic for BP                                                           | Mechanically gener-<br>ated from NuSCR | Manually generated by experts |
|-----------------------------------------------------------------------------|----------------------------------------|-------------------------------|
| Fixed set-point rising<br>trip with operating<br>bypass                     | 71                                     | 32                            |
| Fixed set-point rising<br>trip without operating<br>bypass                  | 53                                     | 24                            |
| Auto-limited rate<br>variable set point trip<br>without operating<br>bypass | 95                                     | 40                            |
| Manual reset variable<br>set point trip with<br>operating bypass            | 117                                    | 67                            |
| Total                                                                       | 336<br>2.06:1                          | 163                           |



#### 

RELIABILITY ENGINEERING & SYSTEM SAFETY

Reliability Engineering and System Safety 87 (2005) 287-294

www.elsevier.com/locate/ress

#### Synthesis of FBD-based PLC design from NuSCR formal specification

Junbeom Yoo<sup>a,\*</sup>, Sungdeok Cha<sup>a</sup>, Chang Hwoi Kim<sup>b</sup>, Duck Yong Song<sup>c</sup>

<sup>a</sup>Department of Electrical Engineering and Computer Science, Korea Advanced Institute of Science and Technology (KAIST) and AITrc/SPIC/IIRTRC, 373-1, Kusong-dong, Yusong-gu, Taejon, South Korea
<sup>b</sup>I&C-HMI team, Korea Atomic Energy Research Institute (KAERI), 150, Deokjin-dong, Yusong-gu, Taejon, South Korea °Nuclear Research Division, Atomic Creative Technology Ltd, 1688-5, Sinil-dong, Daedeok-gu, Taejon, South Korea

Received 15 August 2003; accepted 21 May 2004

Number of function blocks used.



# **FBD Verification and VIS**

- Manual optimization of FBD code was inevitable
- Used VIS (Verification Interacting with Synthesis) to support subsequent behavioral equivalence
  - Defined FBD translation rules into Verilog



#### KOREA UNIVERSITY College of Informatics

## **Intuitive and Visual Analysis**

# To help domain experts better understand results

| e salle vis cujevanence Chather                            |                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                |                                      |                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                | a, 6, 13                 |     | Automatic Vis Equiva              | alence Che | icker                           | - C 🖸     |
|------------------------------------------------------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|--------------------------------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|--------------------------|-----|-----------------------------------|------------|---------------------------------|-----------|
|                                                            |                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                |                                      |                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                |                          |     | Eile Bun Help                     |            |                                 |           |
| ering scences Sesult Hersell Table                         |                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                |                                      |                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                | 0                        |     |                                   | Barrutt    |                                 |           |
| Verling 1                                                  |                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                | Verilog 2                            |                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                |                          |     | Verilog sources                   | PRESUR     | tesult Table                    |           |
| 007/TeXthemet/Holes 2 Revanueles/PP/0F80.                  | Verterth_X_Pretto_Mana                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                         | CXC300756/travel/68                  | vis-2 literamples/RP8/F80.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                     | Veillerth X.Pretio_Mech. |     |                                   |            |                                 |           |
| def enum (80, #1) th_Z_Protei                              | ip_state;                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                      | typedef enum (2                      | , 81, 82) th_Z_Pr                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                              | eteip_state:             |     |                                   |            |                                 |           |
| def enum (TO, V1, V2, V2, V4, V9, V10, V11, V12, V13, V14, | 215, 26, 27,                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                   | Typedef enum [71<br>78, 79, 710, 711 | , w1, w2, w3, w4,<br>. w12, w13, w14,                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                          | #5, #6, #7,<br>#15, #16, |     | Goes to state                     |            |                                 |           |
| 119, 119, 120) times_state;                                |                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                | W17, W18, W19, 1                     | 20) timer_state;                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                               |                          |     | timerCHTP2:01                     |            |                                 |           |
| ine & Pretrip Setpoint 30                                  |                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                | 'define k Pretri                     | p Setpoint 30                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                  |                          |     | timer. Tl                         |            |                                 |           |
| ine k % Pretrip Hys 10                                     |                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                | 'define k_E_Fret                     | rip Nys 10                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                     |                          |     | On innut:                         |            |                                 |           |
| efine k_Trip_Delay 20                                      | -                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                              | //'define k_7ri                      | _Delay 20                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                      |                          |     | f x<0>:0                          |            |                                 |           |
|                                                            |                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                |                                      |                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                |                          |     | f X<1>:1                          |            |                                 |           |
| h_N_Pretrip module<br>le th N Pretrip(clk, f N, th         | I Pretrip):                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                    | // th_X_Pretrip                      | module<br>rip(clk, f E, th                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                     | I Pretrix):              |     | f_X<2>:1                          |            |                                 |           |
|                                                            |                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                |                                      | and the state of t |                          |     | f_X<3>:1                          |            |                                 |           |
| e clk;                                                     |                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                | input clk;                           |                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                |                          |     | f_X<4>:1                          |            |                                 |           |
| ut th_X_Pretrip;                                           | H                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                              | output th_E_Pret                     | eip;                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                           |                          |     | £_X<5>:0                          |            |                                 |           |
| Anner wire # X-                                            |                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                | (linterer wire )                     | x.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                             |                          |     | f_X<6>:1                          |            |                                 |           |
| teper f_R:                                                 |                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                | //integer f_Es                       |                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                |                          |     |                                   |            |                                 |           |
| th_X_Pretrip;                                              |                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                | Mare th_X_Preter                     | apu -                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                          |                          |     | Goes to state                     | 21         |                                 |           |
| Pretrip_state reg state;                                   |                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                | th_I_Fretrip_et                      | te reg states                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                  |                          |     | timer\$NTK2:T2                    |            |                                 |           |
| th_Frev_X_Fretrips                                         |                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                | teg th_Frev_7_F                      | timer                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                          |                          |     | Cimer: T2                         |            |                                 | 11        |
|                                                            |                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                |                                      |                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                |                          |     | On input:                         |            |                                 |           |
| isl state = Zij<br>isl th Fray 7 Fratrin = 1;              |                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                | initial state =                      | zů;<br>z Fretrie = 1:                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                          |                          |     | <ul> <li>unonanged&gt;</li> </ul> |            |                                 | =         |
| isl timer = 70;                                            |                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                | initial timer -                      | 201                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                            |                          |     | Goes to state                     | 3.         |                                 |           |
| on th V Dratnin = /statami                                 | 20 44 1 V cm                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                   |                                      |                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                |                          |     | timerSNTK2:93                     |            |                                 |           |
| retrip Setpaint - 'k X Pretri                              | ip_Hys) 71:                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                    | wire Cond_s_1;                       |                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                |                          |     | timer:T3                          |            |                                 |           |
| (state===================================                  | 00 44 1_X >                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                    | wire Cond b 1;                       |                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                |                          |     | On input:                         |            |                                 |           |
| r - 05)20:                                                 | at a start and a start at at a start at a st |                                      |                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                |                          |     | <unchanged></unchanged>           |            |                                 |           |
| (state===================================                  | 00 46 f_X ≻<br>in Hen 46                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                       | assign Cond a 1                      | = (f X >= 'k_Pret<br>= ((f X >=                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                | trip_Setpoint);          |     |                                   |            |                                 |           |
| r 1= 25)71:                                                | -P                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                             | 'k_Pretrip_Setp                      | int) 66 (timer ==                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                              | 25));                    |     | Goes to state                     | 4:         |                                 |           |
| (state==)                                                  | 01 46 f_X <                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                    | //assign Cond_c                      | 1 = (f_N < 'k_Pre                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                              | strip_Setpoint           |     | timer\$NTK2: T4                   |            |                                 |           |
| -                                                          |                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                |                                      | -                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                              |                          |     | timer: T4                         |            |                                 |           |
|                                                            |                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                |                                      |                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                |                          |     | On input:                         |            |                                 |           |
|                                                            |                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                |                                      |                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                |                          |     | <unchanged></unchanged>           |            |                                 |           |
|                                                            |                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                |                                      |                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                |                          |     |                                   | 5.         |                                 |           |
|                                                            |                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                |                                      |                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                |                          |     | timerSNTK2.05                     |            |                                 |           |
|                                                            |                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                |                                      |                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                |                          |     | timer . TS                        |            |                                 |           |
|                                                            |                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                |                                      |                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                |                          |     | On input:                         |            |                                 |           |
|                                                            |                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                |                                      |                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                |                          |     | <unchanged></unchanged>           |            |                                 |           |
| fomatic Vis Eculwience Checker                             |                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                |                                      |                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                | ್ ಶ ಡ                    |     |                                   |            |                                 |           |
| Run Holm                                                   |                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                |                                      |                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                |                          |     | Goes to state                     | 6:         |                                 |           |
|                                                            | -                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                              |                                      |                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                |                          |     | state\$NTK2:80                    |            |                                 |           |
| Verilog sources Result Result Ta                           | able                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                           |                                      |                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                |                          |     | state: 82                         |            |                                 |           |
| 2 of play                                                  | Eletownut                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                      | Electrone a                          | Edu 101ato                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                     | Edu 201919               |     | th Prev X Pretr                   | 1.DANAK    | 210                             |           |
| Initial                                                    | Indial                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                         | Initial                              | 61 1 TO                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                        | SD 1 TD                  |     | th prev A pretr                   | rip:u      |                                 |           |
| 61                                                         | 1                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                              | 1                                    | S1 1 T1                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                        | 81 1 T1                  |     | (linghanged)                      |            |                                 |           |
| 61                                                         | 1                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                              | 1                                    | S11T2<br>S11T3                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                 | S11T2<br>S11T3           |     | <ul> <li>unchanged&gt;</li> </ul> |            |                                 |           |
| 61                                                         | 1                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                              | 1                                    | S1 1 T4                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                        | 811T4                    |     | Goes to state                     | 7:         |                                 |           |
| 61                                                         | 1                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                              | 1                                    | S1 1 T5                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                        | S1 1 T5                  |     | timer\$NTK2:20                    |            |                                 |           |
| 52                                                         | 0                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                              | 0                                    | 50 0 TO                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                        | 820T0                    |     | timer:T0                          |            |                                 |           |
| 52                                                         | 1                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                              | 0                                    | Nul                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                            | Nul                      |     | On input:                         |            |                                 |           |
|                                                            |                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                |                                      |                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                |                          |     | f_X<3>:0                          |            |                                 |           |
|                                                            |                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                |                                      |                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                |                          |     | f_X<6>:0                          |            |                                 |           |
|                                                            |                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                |                                      |                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                |                          |     | Networks are NO                   | T sequ     | entially equivalent.            |           |
|                                                            |                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                |                                      |                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                |                          |     | vis> vis releas                   | e 2.0      | (compiled Sat Jun 14 12:02:36   | 2008)     |
|                                                            |                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                |                                      |                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                |                          |     | vis> vis> vis>                    | vis> v     | is> # vis release 2.0 (compiled | Sat Jun - |
|                                                            |                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                |                                      |                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                |                          | (h) | Ready                             |            |                                 |           |
|                                                            |                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                |                                      |                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                |                          | (u) |                                   |            |                                 |           |

## **FBD Testing**

• FBD, based on its data-flow model, posed particular challenge

KOREA UNIVERSIT

Any test case would satisfy 100% coverage with simplistic definition

### • Had to define a customized coverage criteria to satisfy regulatory requirements

...The two aspects of test coverage that are particularly important for the unit testing of safety system software are *coverage of requirements* and *coverage of the internal structure of the code*. ... For safety system software, the unit test coverage criteria to be employed should be identified and justified. ... [USNRC Regulation Guide 1.171] [4]





# **Obama co-author?;)**

Information and Software Technology 51 (2009) 1131-1139



#### A data flow-based structural testing technique for FBD programs

#### Eunkyoung Jee<sup>a</sup>, Junbeom Yoo<sup>b</sup>, Sungdeok Cha<sup>c,\*</sup>, Doohwan Bae<sup>a</sup>

<sup>a</sup> Div. of Computer Science, EECS Department, KAIST, 335 Gwahangno, Yuseong-gu, Daejeon 305-701, Republic of Korea <sup>b</sup> Div. of Computer Science and Engineering, Konkuk University, 1 Hwayang-dong, Gwangjin-gu, Seoul 143-701, Republic of Korea <sup>c</sup> Dept. of Computer Science and Engineering, Korea University, Anam-dong, Seongbuk-Gu, Seoul 136-701, Republic of Korea

#### ARTICLE INFO

Article history: Received 4 August 2008 Received in revised form 22 January 2009 Accepted 24 January 2009 Available online 10 March 2009

Keywords: Software testing Structural testing Test coverage criteria Programmable logic controller Function block diagram

#### ABSTRACT

With increased use of programmable ld assurance became an important issue. Re ical systems by identifying coverage crit erage criteria, based on control flow g function block diagram (FBD) which is a three structural coverage criteria for FBI their effectiveness using a real-world rea prepared by FBD testing professionals, o tested sufficiently. Domain experts, ha effective.





## **FBD-customized coverage criteria**

- Defined conditions under which specific input played direct role in determining the output
  - d-path condition
- Defined various coverage criteria under which various FBD unit testing could be performed
  - Basic coverage, input condition coverage, complex condition coverage
  - Similar to statement coverage, branch coverage, condition coverage in traditional (procedural) software testing



Fig. 5. A simplified FBD program for calculating th\_X\_Trip.

(a) Coverage Result for Basic Coverage Criterion

| Test |                       | _                     | Te                    | est Requirement       | 5                     |                       |                       | #Test Reqs            | Coverage |
|------|-----------------------|-----------------------|-----------------------|-----------------------|-----------------------|-----------------------|-----------------------|-----------------------|----------|
| Set  | DPC(p <sub>31</sub> ) | DPC(p <sub>32</sub> ) | DPC(p <sub>33</sub> ) | DPC(p <sub>51</sub> ) | DPC(p <sub>52</sub> ) | DPC(p <sub>53</sub> ) | DPC(p <sub>54</sub> ) | (Satisfied/<br>Total) | (%)      |
| TS1  | 0                     | 0                     | 0                     | 0                     | 0                     | 0                     | 0                     | 7/7                   | 100%     |

(b) Coverage Result for Input Condition Coverage Criterion

| Test<br>Set |      | Test Requirements |          |          |          |                       |          |                    |                    |                    |                    |             |                 |
|-------------|------|-------------------|----------|----------|----------|-----------------------|----------|--------------------|--------------------|--------------------|--------------------|-------------|-----------------|
|             | Test | DPC(p31)          | DPC(p31) | DPC(p32) | DPC(p32) | DPC(p <sub>33</sub> ) | DPC(p33) | DPC                | DPC                | DPC                | DPC                | (Satisfied/ | Coverage<br>(%) |
|             | 301  | ∧ ME              | ∧ ¬ME    | ∧ CE     | ∧ ¬CE    | ^ LT                  | ∧ ¬LT    | (p <sub>51</sub> ) | (p <sub>52</sub> ) | (p <sub>53</sub> ) | (p <sub>54</sub> ) | Total)      | (~)             |
|             | TS1  | х                 | 0        | х        | 0        | х                     | 0        | 0                  | 0                  | 0                  | 0                  | 7/10        | 70%             |
|             | TS2  | 0                 | 0        | 0        | 0        | 0                     | 0        | 0                  | 0                  | 0                  | 0                  | 10/10       | 100%            |

(c) Coverage Result for Complex Condition Coverage Criterion

| Tart | Test Requirements     |          |                       |                       |                       |                       |     |  |  |  |
|------|-----------------------|----------|-----------------------|-----------------------|-----------------------|-----------------------|-----|--|--|--|
| Set  | DPC(p <sub>31</sub> ) | DPC(p31) | DPC(p <sub>31</sub> ) | DPC(p <sub>31</sub> ) | DPC(p <sub>31</sub> ) | DPC(p <sub>31</sub> ) |     |  |  |  |
|      | ∧ ME                  | ∧ ¬ME    | ^ OR6                 | ∧ ¬OR6                | ∧ TR                  | ∧ ¬TR                 |     |  |  |  |
| TS1  | х                     | 0        | х                     | 0                     | х                     | 0                     | ••• |  |  |  |
| TS2  | 0                     | 0        | 0                     | 0                     | 0                     | 0                     |     |  |  |  |
| TS3  | 0                     | 0        | 0                     | 0                     | 0                     | 0                     |     |  |  |  |

| _ |                                | #Test Regs                      | 0                               |                                  |                                |                                 |                               |                                |                       |      |
|---|--------------------------------|---------------------------------|---------------------------------|----------------------------------|--------------------------------|---------------------------------|-------------------------------|--------------------------------|-----------------------|------|
|   | DPC(p <sub>54</sub> )<br>^ LE4 | DPC(p <sub>54</sub> )<br>^ ¬LE4 | DPC(p <sub>54</sub> )<br>^ AND5 | DPC(p <sub>54</sub> )<br>∧ ¬AND5 | DPC(p <sub>54</sub> )<br>^ OR6 | DPC(p <sub>54</sub> )<br>^ –OR6 | DPC(p <sub>54</sub> )<br>^ TR | DPC(p <sub>54</sub> )<br>^ ¬TR | (Satisfied/<br>Total) | (%)  |
|   | 0                              | х                               | х                               | 0                                | х                              | 0                               | х                             | 0                              | 25/50                 | 50%  |
|   | 0                              | х                               | х                               | 0                                | Х                              | 0                               | х                             | 0                              | 34/50                 | 68%  |
|   | 0                              | 0                               | 0                               | 0                                | 0                              | 0                               | 0                             | 0                              | 50/50                 | 100% |

For the input vector (f\_X, f\_Module\_Error, f\_Channel\_Error, f\_X\_Logic\_Trip),

 $TS1 = \{ (2, 0, 0, 0) \}$   $TS2 = \{ (2, 0, 0, 0), (2, 1, 1, 1) \}$  $TS3 = \{ (2, 0, 0, 0), (2, 1, 1, 1), (0, 0, 1, 1), (99, 0, 1, 1) \}$  ME: f\_Module\_Error CE: f\_Channel\_Error LT: th\_X\_Logic\_Trip TR: th\_X\_Trip

Fig. 6. Coverage assessment result for the FBD program in Fig. 5.



# • Developed a tool to automate test case generation (Jee et at., STVR, 2014)

- Used Yices, an SMT solver developed by SRI International



#### KOREA UNIVERSITY College of Informatics

## **KNICS Lessons**

### • Be flexible and attentive to stakeholders' needs

- Including regulatory personnel when relevant
- "Let them do the work";)
  - Extremely important that SE professionals communicate and work well with domain experts
  - It is NEVER as easy as it seems
- Do not reinvent wheels. SMV, VIS, Yices, ...
- Provide data visualization/interpretation tools
- Domain-specific problems can become interesting SE challenges (e.g., FBD testing criteria)



### **Hybrid Ventricular Assist Device**

- Korea Artificial Organ Center (KAOC) project
- Animal-tested for 183 days on a calf, exceeding the FDA regulations on long-term experiment
  - No anomaly was detected



#### 📩 뉴스홈 > **의료** 👘

동록날짜 2007년08월13일 00시00분

글자크기 🗗 🗖 🛛 🛱 🖉

#### 국산 인공심장 이식 송아지, 국내 최장 70일 생존 高大 한국인공장기센터 연구팀, 인공장기상용화 전기마련





고려대 한국인공장기센터(소장 선 경, 안암병원 흉부외과)가 인공심장 을 이식한 송아지가 국내 최장 생존 기록 70일을 세워, 의학계의 관심이 쏠리고 있다. 종전 45일보다 25일 이상 오래 생존 한 기록이다.

이번에 이식한 인공심장 H-VAD는 고려대 한국인공장기센터가 자체개 발한 것이다.이로써 국내기술로 만 든 인공심장으로는 최장 생존기록을 달성했다는 점이 의미가 깊다.



## **H-VAD Software**

#### • Event-driven architecture

- Pumping Rate (PR), Stroke Length (SL), Start / Stop button
- 211 probing statements were added

### • Control logic in ~3,800 LoC in C

- Relatively simple branch conditions



## **In-Vitro Testing**

• Each button was pressed at least once

KOREA UNIVERSIT

- All permitted parameter values were covered (e.g., SL 30~90, default 60)
- Stop button was pressed at arbitrary and random moments





## **In-Vitro Testing**

- Tried to force the system to engage in predefined emergency modes
- Achieved 80.6%, 170 out of 211 probes, coverage

|      |                            |     |     |              | Preconditi   | on            |                | Related    | Provide Kar                                                                                     |
|------|----------------------------|-----|-----|--------------|--------------|---------------|----------------|------------|-------------------------------------------------------------------------------------------------|
| ID   | Test inputs                | PR  | SL  | Control mode | Running mode | Pump position | Pump direction | Guide line | Description                                                                                     |
| TC1  | START                      | 50  | 60  | PR           | STOP         | Center        | N/A            | 1          | Baseline                                                                                        |
| TC2  | Plus (10 times)            | 50  | 60  | PR           | RUNNING      | N/A           | N/A            | 2          | Increasing pump rate                                                                            |
| TC3  | Plus                       | 150 | 60  | PR           | RUNNING      | N/A           | N/A            | 3          | Upper boundary checking for pump rate                                                           |
| TC4  | Minus (10 times)           | 50  | 60  | PR           | RUNNING      | N/A           | N/A            | 2          | Decreasing pump rate                                                                            |
| TC5  | Minus                      | 5   | 60  | PR           | RUNNING      | N/A           | N/A            | 3          | Lower boundary checking for pump rate                                                           |
| TC6  | SL                         | 50  | 60  | PR           | RUNNING      | N/A           | N/A            | 1          | Changing the control mode                                                                       |
| TC7  | Plus (10 times)            | 50  | 60  | SL           | RUNNING      | N/A           | N/A            | 2          | Increasing stroke length                                                                        |
| TC8  | Plus                       | 50  | 80  | SL           | RUNNING      | N/A           | N/A            | 3          | Upper boundary checking for stroke length                                                       |
| TC9  | Minus (10 times)           | 50  | 60  | SL           | RUNNING      | N/A           | N/A            | 2          | Decreasing stroke length                                                                        |
| TC10 | Minus                      | 50  | 30  | SL           | RUNNING      | N/A           | N/A            | 3          | Lower boundary checking for stroke length                                                       |
| TC11 | PR                         | 50  | 60  | SL           | RUNNING      | N/A           | N/A            | 1          | Changing the control mode                                                                       |
| TC12 | Plus (10 times)            | 50  | 60  | PR           | STOP         | N/A           | N/A            | 2          | Same with TC2 but in stopped mode                                                               |
| TC13 | Plus                       | 150 | 60  | PR           | STOP         | N/A           | N/A            | 3          | Same with TC3 but in stopped mode                                                               |
| TC14 | Minus (10 times)           | 50  | 60  | PR           | STOP         | N/A           | N/A            | 2          | Same with TC4 but in stopped mode                                                               |
| TC15 | Minus                      | 5   | 60  | PR           | STOP         | N/A           | N/A            | 3          | Same with TC5 but in stopped mode                                                               |
| TC16 | SL                         | 50  | 60  | PR           | STOP         | N/A           | N/A            | 1          | Same with TC6 but in stopped mode                                                               |
| TC17 | Plus (10 times)            | 50  | 60  | SL           | STOP         | N/A           | N/A            | 2          | Same with TC7 but in stopped mode                                                               |
| TC18 | Plus                       | 50  | 80  | SL           | STOP         | N/A           | N/A            | 3          | Same with TC8 but in stopped mode                                                               |
| TC19 | Minus (10 times)           | 50  | 60  | SL           | STOP         | N/A           | N/A            | 2          | Same with TC9 but in stopped mode                                                               |
| TC20 | Minus                      | 50  | 30  | SL           | STOP         | N/A           | N/A            | 3          | Same with TC10 but in stopped mode                                                              |
| TC21 | PR                         | 50  | 60  | SL           | STOP         | N/A           | N/A            | 1          | Same with TC11 but in stopped mode                                                              |
| TC22 | STOP                       | N/A | N/A | N/A          | RUNNING      | Тор           | Up             | 4          | Pressing STOP button when the pump is<br>going up from the center position                      |
| TC23 | STOP                       | N/A | N/A | N/A          | RUNNING      | Center        | Up             | 4          | Pressing STOP button when the pump is passing<br>the center position and the direction is up.   |
| TC24 | STOP                       | N/A | N/A | N/A          | RUNNING      | Bottom        | Up             | 4          | Pressing STOP button when the pump is going<br>up from the bottom                               |
| TC25 | STOP                       | N/A | N/A | N/A          | RUNNING      | Тор           | Down           | 4          | Pressing STOP button when the pump is going<br>down from the top                                |
| TC26 | STOP                       | N/A | N/A | N/A          | RUNNING      | Center        | Down           | 4          | Pressing STOP button when the pump is passing<br>the center position and the direction is down. |
| TC27 | STOP                       | N/A | N/A | N/A          | RUNNING      | Bottom        | Down           | 4          | Pressing STOP button when the pump is going<br>down from the center position                    |
| TC28 | Disable center hall sensor | N/A | N/A | N/A          | RUNNING      | N/A           | N/A            | 5          | Triggering emergency mode 1                                                                     |
| TC29 | Block air valve            | N/A | N/A | N/A          | RUNNING      | N/A           | N/A            | 5          | Triggering emergency mode 2                                                                     |



# **In-Vitro Testing: Results**

 Found two behavior patterns, previously unknown to KAOC staff, that appeared abnormal





# Animal Testing and H-VAD Software

- Used two 3-months old piglets
- 78.7% code coverage (cf 80.6%)
  - Due to our inability to force/repeat certain test cases without endangering the test animal's life





# **Animal Testing: Results**

#### Could NOT recreate in-vitro testing result



# **Animal Testing: Results**

### Abnormal pumping pattern, off by 7, repeated

KOREA UNIVERSIT





### **H-VAD Lessons**

- SE techniques, although common sense and trivial to us, are not always applied in practice
- "Live" testing is expensive, difficult, timeconsuming, ...
  - It is extremely difficult to make credible claims on software quality in safety-critical setting

### • "All NEW H-VAD" project could not be launched

- Guide hardware design so as to simplify software design and enhance software safety assurance
- Dedicated and continuous involvement of domain experts are crucial to the success



#### • Safety-Critical Systems Symposium, Feb 2011, Southampton, UK

#### **Testing of Safety-Critical Software Embedded in an Artificial Heart**

Sungdeok Cha<sup>1</sup>, Sehun Jeong<sup>1</sup>, Junbeom Yoo<sup>2</sup> and Young-Gab Kim<sup>1</sup>

<sup>1</sup>Korea University, Seoul, Korea

<sup>2</sup>Konkuk University, Seoul, Korea

**Abstract** Software is being used more frequently to control medical devices such as artificial heart or robotic surgery system. While much of software safety issues in such systems are similar to other safety-critical systems (e.g., nuclear power plants), domain-specific properties may warrant development of customized techniques to demonstrate fitness of the system on patients. In this paper, we report results of a preliminary analysis done on software controlling a Hybrid Ventricular Assist Device (H-VAD) developed by Korea Artificial Organ Centre (KAOC). It is a state-of-the-art artificial heart which completed animal testing phase. We performed software testing in in-vitro experiments and animal experiments. An abnormal behaviour, never detected during extensive in-vitro analysis and animal testing, was found.

## Conclusions

- Interdisciplinary research is important and doable, but difficult
- Software engineering can and should play important roles in software-driven and software-intensive society
- Support domain experts to do their work well
  - We must learn to work with domain experts