SERA 2004

NuEditor: A Tool Suite for Specification and Verification of NuSCR

Jaemyung Cho Junbeom Yoo Sungdeok Cha* KAIST, Korea



Jaemyung



Junbeom

KNICKS? KNICS.

 Instrumentation and Control System for Nuclear Power Plants

> RLL-based Analog

PLC-based Digital

Similar system, Wolsung SDS2, currently in service

■ Since ~1996

All requirements were documented in tabular notation (SCR)

Software subject to rigorous safety analysis (and government approval)

NuSEE and KNICS





Korean/English Specification Traceability and Inspection Support



NuEditor



Function Block Diagram (FBD) Generation and Analysis

> Configuration Management

NuSCR / NuEditor

Customize SCR to effectively reflect characteristics unique to nuclear engineering domain

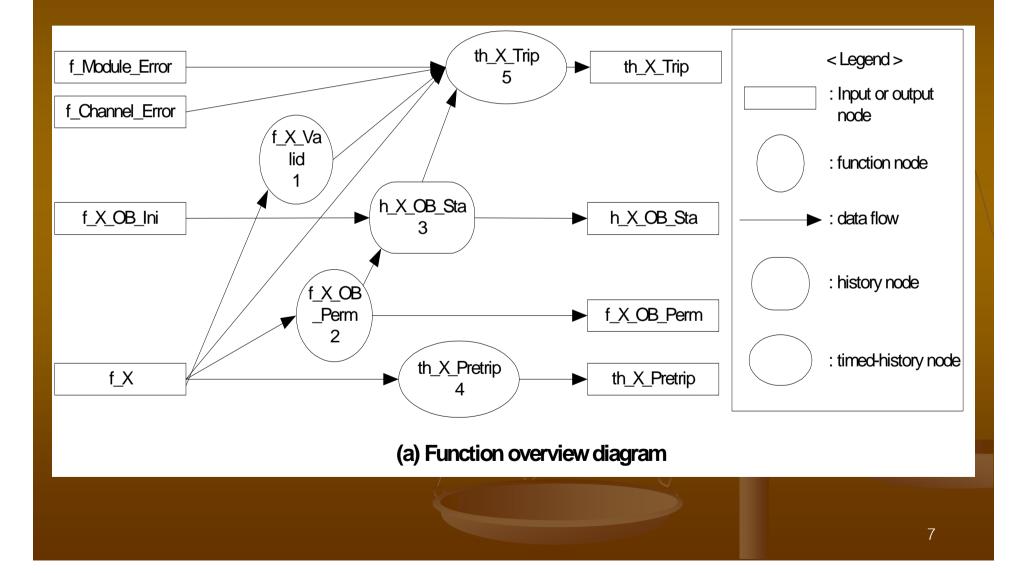
 "tables-always" notation is difficult to read (to domain experts) when documenting time- and state-dependent requirements

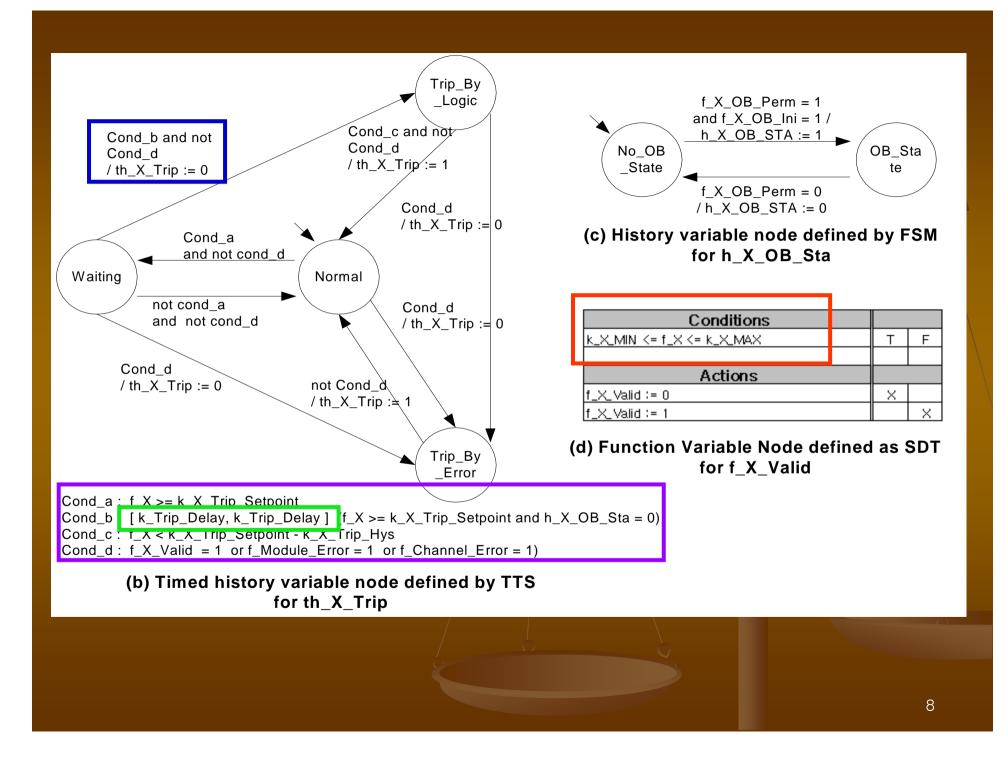
NuEditor supports graphical editing and formal verification of NuSCR

NuSCR

Function Overview Diagram
Function Variable
History Variable
Timed-history Variable

Function Overview Diagram





NuSCR Semantics

ARTICLE IN PRESS



Available at

www.ElsevierComputerScience.com

The Journal of Systems and Software xxx (2003) xxx-xxx

The Journal of Systems and Software

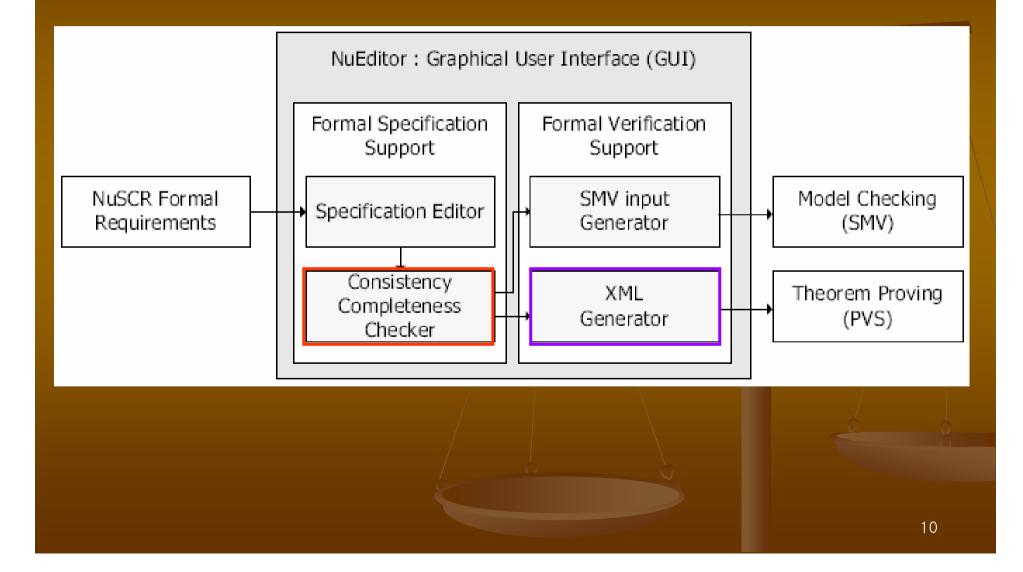
www.elsevier.com/locate/jss

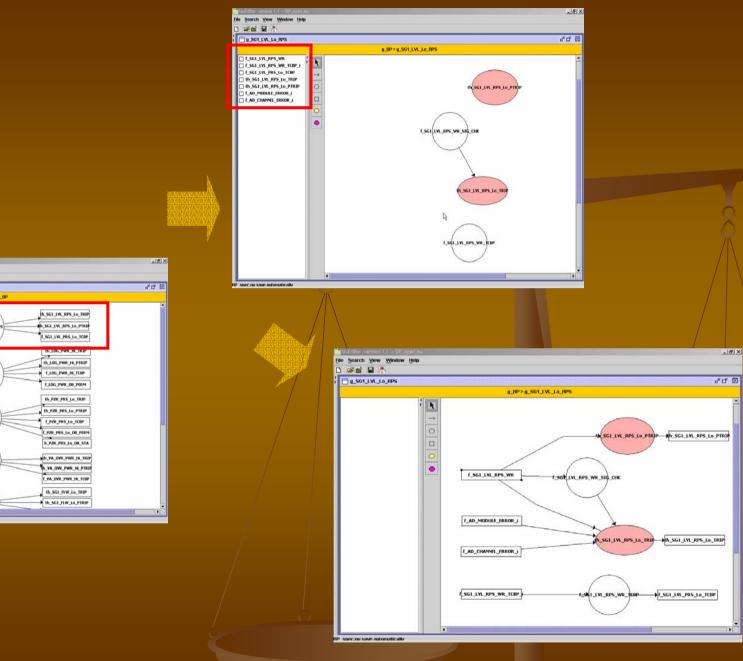
A formal software requirements specification method for digital nuclear plant protection systems

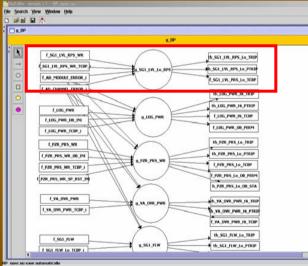
Junbeom Yoo^{a,*}, Taihyo Kim^a, Sungdeok Cha^a, Jang-Soo Lee^b, Han Seong Son^b

 ^a 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
 ^b 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

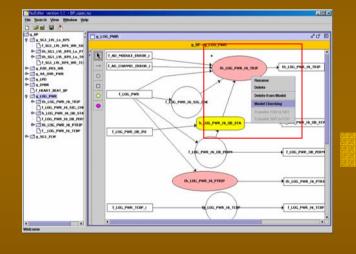
NuEditor







Formal Verification Support



(SMV Input Generation)

| NUPUT VARIALE | | | r |
|--|---------------------|---|-------|
| m 105 PM /R THP (Solitery | | 1 | - N M |
| , LOG, Freit, H., 201, CHE: Inclusion , AD, MODARE, EMICIEL J.: Inclusion | | | |
| 1.00, Perf. 6. 1001 3.00, Perf. 4. 08, 318 (collect) | | | |
| AD_ONWEL_DEED_1 holes; mt_1 = 0.4; | | | |
| | | | |
| | | | |
| | | | |
| | | | |
| PROPERTY | | | |
| 940C 446 (K) | | | |
| | | | |
| SPECIAL (PROMINACIONE-TO-TREP) IN LOCE ADAM & PROMINACIONE TO-TREP BY EXECUTIVATION SPECIAL (PROMINACIONE-TO-ROTRING ADAM & PROMINACIONE TO-TREP BY EXECUTIVATION | | | |
| $\begin{array}{l} \label{eq:constraints} \left(p_{1}^{2} \left(p_{2}^{2} \left(p_{1}^{2} \left(p_{2}^{2} \left$ | | | |
| | | | |
| PEC 44(17,25exed,0100 = 11(1,36684,0100 = 1) → 47(6,3(250 = 0) | | | |
| 94C A007_X > 3_0_74_54patri 6.0xe_1 > 40 -> AF 0_0_754p = 0 | | | |
| 990 All(07_Darrel_Droc = 111_Piolais_Droc = 111_U_Dial(=1) & (7_2 == k_U_Dro_Dispon)) -> 4976_U_Dro | | | |
| 94C 64(b,),(0,)(a + 1.6.1),(barrel,Drot + 1)),(b6(a,)(brot + 1)),(b(a) + 1).6.67 6(10),(b(a + 1) + 8 | 4 Al 10, 3, 74 + 1) | | |
| | Circe | | |
| | | | |
| renormonomenomen | | | |
| | | | |
| Sector Sector Sector | | | |
| 21.22.21.21.2 | | | |
| | | | |
| Statistics and statistics | | | |
| | | | |
| | | | |
| Generate SMU Innut the | | | |
| €, Generate SMV input file | | | |
| Generate SMV input file Ormenated by NuEditor 1, 1 | | | _ |
| | | | |
| Generated by NuEditor 1.1 | | | |
| - Generated by NuEditor 1.1 - SMV Input for NuSCR | | | |
| - Generated by NuEdbor 1.1 - SMV Inputfor NuSCR - SE Lab. KAIST. | | | |
| – SMV Inputfor NuSCR → SE Lab. KAIST. MODULE main | | | |
| - Generated by NuEddor 1.1 - SMV Input for NuSCR - SE Lab. KAIST. MODULE main | | | |
| - Orenerated by NuEdsor 1.1 - SWI hourdor hugCR - SE Lab. KARST. MODULE main MAR Th_LOO_PVMR_H_TTIP: boolean; (1,LOO_PVMR_H_SIG)_CHK: boolean; | | | |
| - Overenzied by Nulldfor I.1 - SMU Inguitor HugOR - SE Lab Awast. MODULE main UAR h_LOO_PVRL_HL_TRIP: boolean, (LOO_PVRL_HL_TRIP: boolean, (LOO_PVRL_HL_SO_CH4: boolean, (LOO_PVRL_HL_SO_CH2): boolean, | | | |
| - Orenersited by NuEditor 1.1 - SWI hourd for NuECR - SE Lab. KARST. MODULE main MR Th_LOO_PVRF_H_TRIP: bootean; (LAO_MODULE_ERROR_J: notean; (LAO_MODULE_COM) | | | |
| - Overenzied by Nulldfor 1.1 - SMN leguthor HuSCR - SE Lak KNST. | | | |
| - Orientated by NuEditor 1.1 - SWI hourd for NuECR - SE Lab. KARST. MODULE main MR Th_LOO_PVMR_HI_TRIP: boolean; (LAO_MODULE_ERROR_J: boolean; (LAO_MODULE_CORT), toolean; (LAO_MODULE_ERROR_J: boolean; N_LOO_PVMR_HI_COR_STA: boolean; (LAO_MODULE_ERROR_J: boolean; N_LOO_PVMR_HI_COR_STA: | | | |
| - Orenerated by NullEdor 1.1 - SMF logut for NuGCR - SE Lab KNST. MODULE main NAR DLOG_PVR_H_TRIP: boolean; 1_LOG_PVR_H_B_SO_CH4: Societan; 1_LOG_PVR_H00; _ boolean; 1_LOG_PVR_100; _ STA: boolean; (_AD_CH4NNEL_ERROR_J: boolean; (_AD_CH4NNEL_ERROR_J: boolean; 1_MO_F_NT_6; _ STA: boolean; (_AD_CH4NNEL_ERROR_J: boolean; 1_MO_F_NT_6; _ STA: boolean; 1_MO_F_NT_6; _ STA: boolean; (_AD_CH4NNEL_ERROR_J: boolean; 1_MO_F_NT_6; _ STA: boolean; _ STA: _ S | | | |
| - Orientated by NuEditor 1.1 - SWI hourd for NuECR - SE Lab. KARST. MODULE main MR Th_LOO_PVMR_HI_TRIP: boolean; (LAO_MODULE_ERROR_J: boolean; (LAO_MODULE_CORT), toolean; (LAO_MODULE_ERROR_J: boolean; N_LOO_PVMR_HI_COR_STA: boolean; (LAO_MODULE_ERROR_J: boolean; N_LOO_PVMR_HI_COR_STA: | x | | |
| - Ormerated by NulliBitor 1.1 - SMM loyal for NuBCR - SE Lab KNST. MODULE main VAR LLOD_PVR_H_B_0_CHK: Societan; LLOD_PVR_H_B_0_CHK: Societan; LLOD_PVR: B_0_0_3; Societan; LLOD_PVR: B_0_0_3; Societan; LLOD_PVR: B_0_0_3; Societan; LLOD_PVR: B_0_0_3; Societan; LLOD_PVR: B_0_0_3; Societan; STATE (NOFMME_RROR): boolean; STATE (NOFMME_WAITNO, TRIP_BY_ERROR; | x | | |
| - Orenerated by NullEdor 1.1 - SMF logut for NuGCR - SE Lab KNST. MODULE main NAR DLOG_PVR_H_TRIP: boolean; 1_LOG_PVR_H_B_SO_CH4: Societan; 1_LOG_PVR_H00; _ boolean; 1_LOG_PVR_100; _ STA: boolean; (_AD_CH4NNEL_ERROR_J: boolean; (_AD_CH4NNEL_ERROR_J: boolean; 1_MO_F_NT_6; _ STA: boolean; (_AD_CH4NNEL_ERROR_J: boolean; 1_MO_F_NT_6; _ STA: boolean; 1_MO_F_NT_6; _ STA: boolean; (_AD_CH4NNEL_ERROR_J: boolean; 1_MO_F_NT_6; _ STA: boolean; _ STA: _ S | X | | |
| - Ormersited by NuEditor 1.1 - SW Input for HuBCR - SE Lab. KARST. MODULE main WR m_LOO_PWR_H_E00_CHK: boolean; (LAD_MODULE_ERROR_J: boolean; (LAD_MODULE_ERROR_J: boolean; (LAD_MODULE_ERROR_J: boolean; h_LOO_PWR_H_E00_STA: boolean; h_LOO_PWR_H_ERROR_J: boolean; time_1: 0.4; STATE: (NORMML, WATINO, TRIP_BY_ERROR; ASSION | x | | |
| - Ormerated by NullBorr 1.1 - SWI Joyaffor HugCR - SE Lab KMST. MODULE main VAR 0_ JPMR_H_BIO_CHK: boolean; LL00_FMR_H_BIO_CHK: boolean; LL00_FMR_H_BIO_CHK: boolean; LL00_FMR_B_BRORG : boolean; LL00_FMR_B_BRORG : boolean; STATE: INOTMAL_WAITNO, TRP_BY_LOOKC, TRIP_BY_ERROR; SSIGN: MIGSTATE) = TRIP_BY_ERROR; SSIGN: | x | | |
| - Ormersited by NuEditor 1.1 - SWI hop/tor HuBCR - SE Lab. KARST. MODULE main WR m_LOO_PWR_H_E00_CHK: toolean; (LAD_MODULE_ERROR_1: toolean; (LAD_MODULE_ERROR_1: toolean; (LAD_MODULE_ERROR_1: toolean; (LAD_MODULE_ERROR_1: toolean; 1.0.0_PWR_H_E00_STA: toolean; 1.0.0_PWR_H_E00_STA: toolean; time_1: 0.4; STATE (HORMML, WATINO; THP_BY_ERROR; MRISTATD > THP_BY_ERROR; MRISTATD > THP_BY_ERROR; MRISTATD > THP_BY_ERROR; | x | | |
| - Orientated by NuEditor 1.1 - SMI hourd by | x | | |
| - Ormersited by NuEditor 1.1 - SM/ Input for HuBCR - SE Lab. KARST. MODULE main MR Th_LOO_PWR_H_EB0_CHK: boolean; (LAD_MODULE_ERROR_1: boolean; (LAD_MODULE_ERROR_1: boolean; (LAD_MODULE_ERROR_1: boolean; (LAD_MODULE_ERROR_1: boolean; (LAD_MODULE_ERROR_1: boolean; (LAD_MODULE_ERROR_1: boolean; time_1: 0.4; STATE (INOFINAL, WATINO, TRIP_BY_ERROR; MGISTATE) > TRIP_BY_ERROR; MGISTATE) > TRIP_BY_ERROR; MGISTATE) > TRIP_BY_ERROR; FROM TRIP_MOLOTO-TO-NORMAL_Isken: NORMAL; FROM TRIP_BY_COLOTO-TO-NORMAL_Isken: NORMAL; FROM TRIP_BY_COLOTO-NORMAL_Isken: NORMAL; FROM TRIP_BY_COLOTO-NORMAL_Isken: NORMAL; FROM TRIP_BY_COLOTO-NORMAL_Isken: NORMAL; FROM TRIP_BY_COLOTO-NORMAL_Isken: NORMAL; | x | | |
| Orenerated by NuEdator 1.1 = SM/ Input for NuEdator 1.1 = SM/ Input for NuEdator 1.1 = SM/ Input for NuEdator 1.1 MODULE main VMR MDULE main VMR In_LOO_PMR_H_BOO_CHA: Isoolean; (LOO_PMR_H_BOO_CHA: Isoolean; (ILOO_PMR_H_BOO_CHA: Isoolean; (ILOO_PMR_H_BOO, ISOOlean; (ILOO, ISOOlean; (ILOO_PMR_H_BOO, ISOOlean; (ILOO, ISOOlean; (ILOO) (ILOO | x | | |
| - Generated by NuEdbort 1 - SM/ Input for HuSCR - SE Lab. KARST. MOULE main MR Th_LOO_PMR_H_TRIP: Iboolean; (LAD_MOULE_ERROR_J: boolean; (LAD_MOULE_ERROR_J: boolean; (LAD_MOULE_ERROR_J: boolean; (LAD_MOULE_ERROR_J: boolean; (LAD_MOULE_ERROR_J: boolean; Itma_1:0.4; STATE: (NORMAL, WATNO, TRIP_BY_ERROR; MRISTATE) = TRIP_BY_ERROR; MRISTATE) = TRIP_BY_ERROR; MRISTATE) = TRIP_BY_ERROR; MRISTATE: NORMAL; KROM TRIP_SY_LOGIC-To-NORMAL_Isken: NORMAL; FROM WATNO-TO-NORMAL-Isken: NORMAL; FROM WATNO-TO-TRIP_SY_LOGIC-Isken: TRIP_BY_LOGIC; FROM WATNO-TO-TRIP_SY_LOGIC-ISKEN: TWIPTNO; FROM WATNO-TO-TRIP_SY_LOGIC-ISKEN: TRIP_BY_LEROG; FROM WATNO-TO-TRIP_SY_LOGIC-ISKEN: TRIP_SY_LOGIC; FROM WATNO-TO-TRIP_SY_LOGIC-ISKEN: TRIP_SY_LOGIC; FROM WATNO-TO-TRIP_SY_LOGIC-ISKEN: TRIP_SY_LEROG; FROM WATNO-TO-TRIP_SY_LOGIC-ISKEN: TRIP_SY_LEROG; FROM WATNO-TO-TRIP_SY_LOGIC-ISKEN: TRIP_SY_LEROG; FROM WATNO-TO-TRIP_SY_LEROGIC-ISKEN: TRIP_SY_LEROG; FROM WA | x | | |
| Orientated by NuEdator 1.1 = SM / Input for NuEdator 1.1 MOULE main MAR MOULE main MAR MULO / PWR / H_ (SR) (-FK): Isociean; (L/O, O'HWR - H_ (SR) (-FK): Isociean; (Thu, O'HWR - HK) (-FK) (-FK) (Thu (FK) (-FK) (-FK)) (SR) (SR) (-FK) (-FK) (-FK) (-FK) (SR) (-FK) (-FK) (-FK) (-FK) (-FK) (FK) (-FK) | | | |
| - Orientated by NuEditor 1.1 - SMI hourd by | | | |

Execution

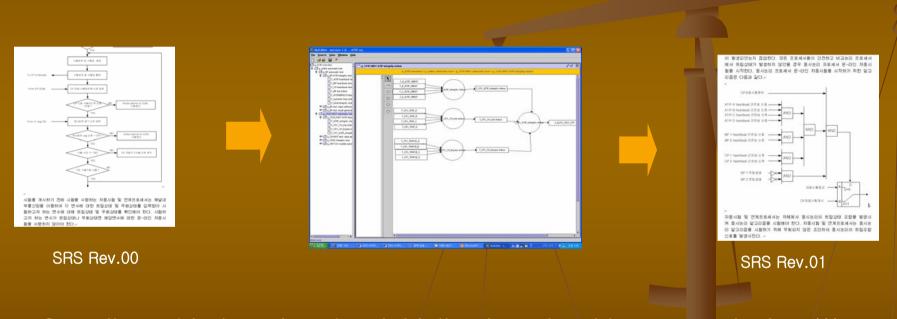
Close

(property)

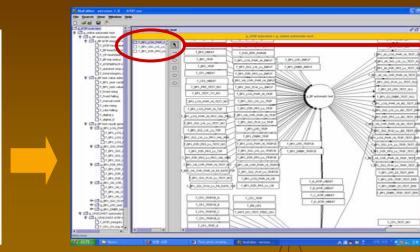
| | | | Property | | | Result | |
|---|--|--|---|--|---|--|--|
| (AG (EX 1 |)) | | | | | true | Mon Apr 26 2 |
| (AG (~()F | ROM-WAITING | TO-TRIP_BY | LOGIC-taken &\F | ROM-WAITING-1 | O-NORMAL-t | true | Mon Apr 26 2 |
| (AG (~(\F | ROM-WAITING | -TO-TRIP_BY_ | LOGIC-taken &\F | ROM-WAITING-1 | O-TRIP_BY_ | true | Mon Apr 26 2 |
| | | | taken &/FROM-W | | | true | Mon Apr 26 2 |
| | | | taken &VFROM-V | | | true | Mon Apr 26 2 |
| | | | P_BY_ERROR-1 | | | true | Mon Apr 26 2 |
| (AG (~(\F | ROM-NORMAL | -TO-TRIP_BY_ | ERROR-taken &\ | FROM-NORMAL | -TO-WAITING-ta | true | Mon Apr 26 2 |
| ×[| | | | | | | |
| Nodel ci | ecking res | | | | | 0.020 | 0288 2 |
| Model cl (AG (EX (AG (~() (AG (~() (AG (~() (AG (~() (AG (~() (AG (~() | 1)) FROM-WAITID FROM-WAITID FROM-WAITID FROM-WAITID FROM-WAITID FROM-TRIP_1 FROM-NORMAN | NG-TO-TRIP_ NG-TO-TRIP_ NG-TO-NORMA NG-TO-NORMA BY_LOGIC-TO | BY_LOGIC-take BY_LOGIC-take L-taken (/FK L-taken (/FK L-taken (/FK ZERDR-taker S. | en £\FROM-WAN DM-WAITING-TO DM-WAITING-TO DR-taken £\FF | TING-TO-NORM TING-TO-TRIP TRIP_BY_ERD TRIP_BY_ERD NOM-TRIP_BY_1 | IAL-t BY OR-t OGIC | true true true true true |
| ayatem (Hodel c2 (AG (EX (AG (~()) (AG (~()) (AG (~()) (AG (~()) (AG (~()) (AG (~()) See file user tim | 1)) FROM-WAITID FROM-WAITID FROM-WAITID FROM-WAITID FROM-WAITID FROM-NORMAN "a.warn" : | NG-TO-TRIP NG-TO-TRIP NG-TO-NORMA NG-TO-NORMA BY_LOGIC-TO L-TO-TRIP_B | BY_LOGIC-take L-taken &\FR L-taken &\FR -TRIP_BY_ERR Y_ERROR-taker | en £\FROM-WAN DM-WAITING-TO DM-WAITING-TO DR-taken £\FF | TING-TO-NORM TING-TO-TRIP TRIP_BY_ERD TRIP_BY_ERD NOM-TRIP_BY_1 | IAL-t. BY OR-t. OGIC. IG-ta. 0.22 | true true true true true true |
| Model cl (AG (EX (AG (~() (AG (~() (AG (~() (AG (~() (AG (~() (AG (~() | 1)) FROM-WAITID FROM-WAITID FROM-WAITID FROM-WAITID FROM-WAITID FROM-NORMAN "a.warn" : | NG-TO-TRIP NG-TO-TRIP NG-TO-NORMA NG-TO-NORMA BY_LOGIC-TO L-TO-TRIP_B | BY_LOGIC-take L-taken &\FR L-taken &\FR -TRIP_BY_ERR Y_ERROR-taker | en £\FROM-WAN DM-WAITING-TO DM-WAITING-TO DR-taken £\FF | TING-TO-NORM TING-TO-TRIP TRIP_BY_ERD TRIP_BY_ERD NOM-TRIP_BY_1 | IAL-t. BY OR-t. OGIC. IG-ta. 0.22 | true true true true true true |

Tool Demonstration...

NuEditor "In Action"



Contributed in learning that initialization algorithm was missing !!!



Found inconsistent use of variables

를 선택하는 자동시험 및 연계프로세서 알고리즘은 다음과 같다.~

4) 비교논리 A/D 변환 자동시험 오류~

6) 비교논리 드립 자동시험 오류~
 6) 비교논리 더 입력 자동시험 오류~

5,3,4,2,1 비교논리 프로세서 자동주기시험·

2) 채널 A ATIP 건정성 신호.

3) 채널 B ATIP 건전성 신호~

4) 채널 C ATIP 건전성 신호~

5) 채널 D ATIP 건전성 신호+

1) 채널 자동시험 시작..

6) BP 1 건전성 신호+

7) BP 2 건전성 신호~

8) CP 1 건전성 신호+

9) CP 2 건전성 신호·

12) 트립채널우회상태~

15)예비트립 설정치+

10)BP 1 트립상태~

11)BP 2 트립상태+

13) 무정우립산태...

14)트립 설정치~

16)공정변수값+ 17)비율설정치+

. 1) 시험중지~ 2) 비교논리 시험변수~ 3) 비교논리 시험값~

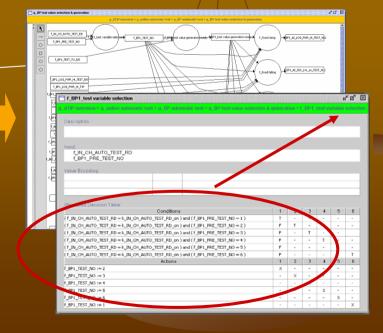
2. 출력 -

1. 입력 -



자동시험 및 연계프로세셔는 비교논리 프로세셔 자동주기시험을 위해 면저 각 공정변수에 대해 트림을 발생시키는 시험값을 생성해야 한다. 이를 위해 자동시험 및 연계프로세셔는 비교논리프로세셔로부터 채널대부통신답(CRV) 문 이용하여 각 시험변수의 현재값 및 성정치를 입력받는다. 자동시험 및 연 계프로세셔는 입력받은 현재값 및 성정치를 입용하여 그 변수가 트립상대를 유발하는 시험값을 진담하게 생성한다. ~

상승트립 고정실전치 비교논리를 시험하기 위해 입력되는 변수 시험값은 트 립설전치보다 큰 값이 되어야 한다. 상승트립 고정설전치를 시험하기 위해 시험값을 생성하는 알고리즘은 다음과 같다."



Detected ambiguities in Algorithms (incomplete specification)

Features and Future Extensions

Me too...

Grapghical Editing "Sensible" static checks Model Checking Support Reasonable PM support Simulation Code Generation Reports Generation

I know... Not yet...

Test Case Generation Fault Tree Analysis FBD Refinement Verification

Stay tuned...

Function Block Diagram Synthesis

Can you do that, huh?

* Comparison of features against Statemate MAGNUM

Conclusions

Nuclear engineers like NuSCR and NuEditor
Obvious. They are partners.
Applicable to other domains with similar characteristics
Real-time, embedded, process-control, reactive

"One investor at a time."