SERA 2004

NuEditor: A Tool Suite for Specification and Verification of NuSCR

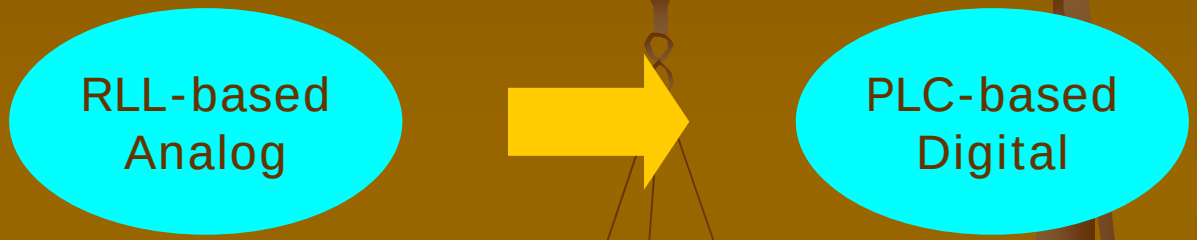
Jaemyung Cho
Junbeom Yoo
Sungdeok Cha*
KAIST, Korea

Jaemyung

Junbeom

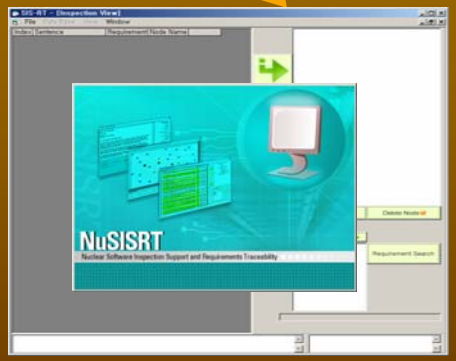
KNICKS? KNICS.

- Instrumentation and Control System for Nuclear Power Plants

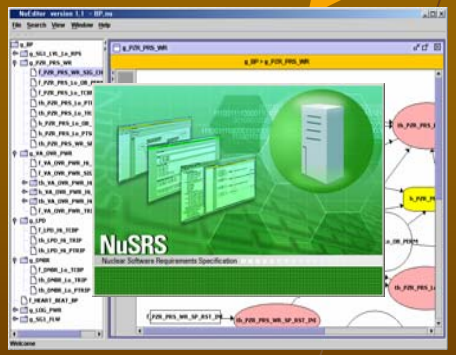


- Similar system, Wolsung SDS2, currently in service
  - Since ~1996
  - All requirements were documented in tabular notation (SCR)
- Software subject to rigorous safety analysis (and government approval)

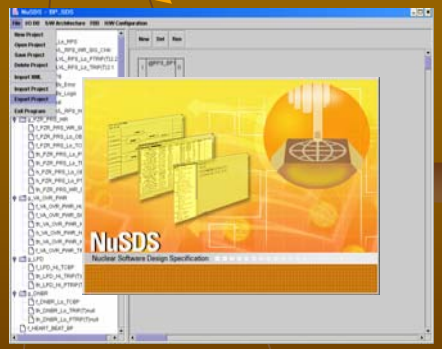
NuSEE and KNICS



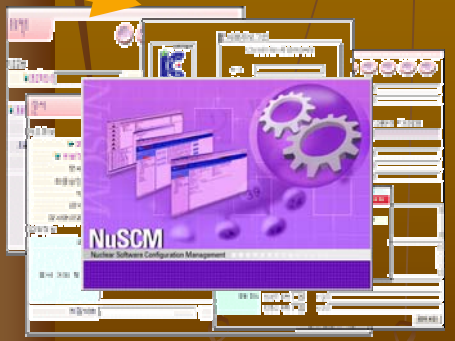
Korean/English Specification Traceability and Inspection Support



NuEditor



Function Block Diagram (FBD) Generation and Analysis



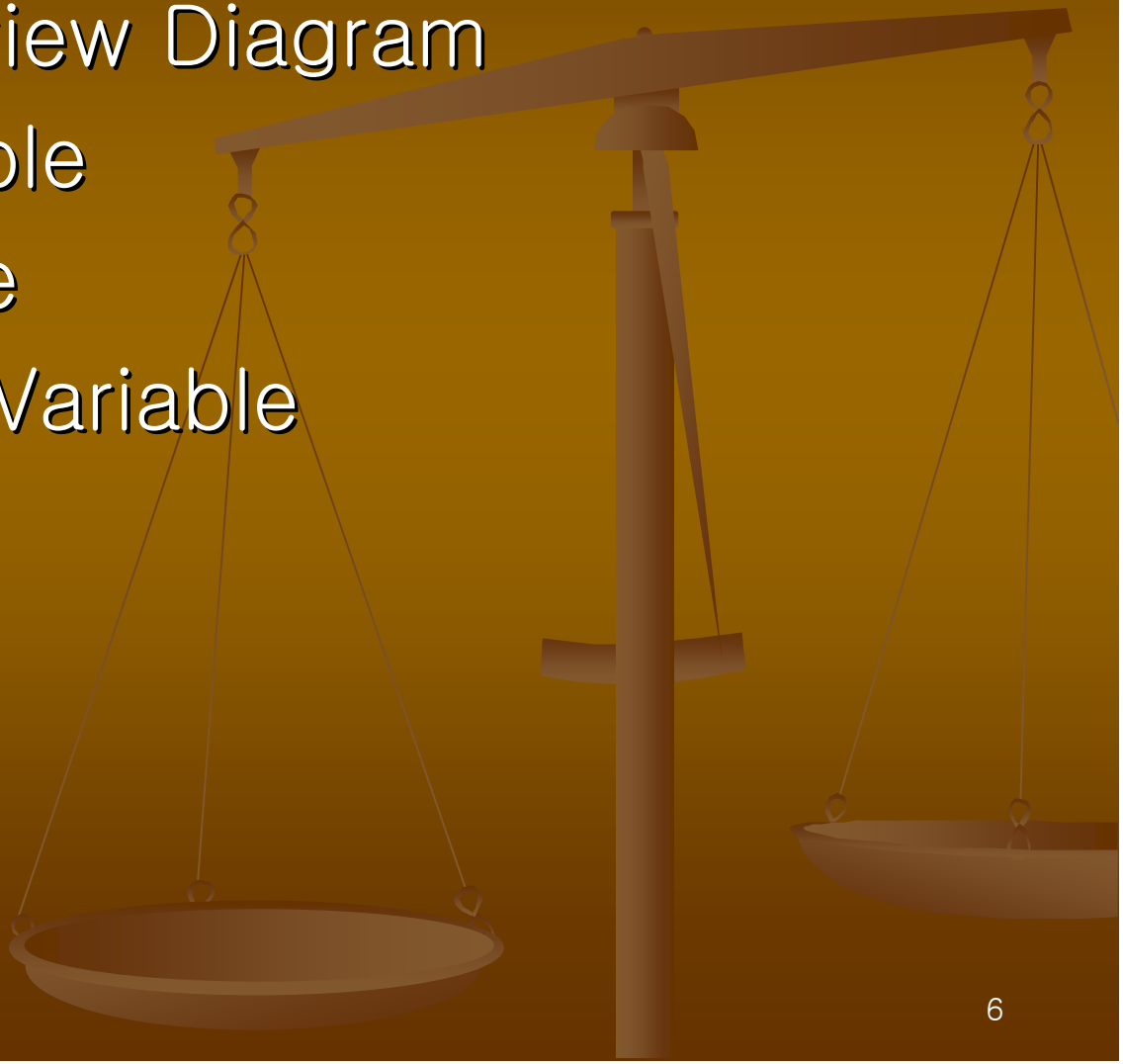
Configuration Management

NuSCR / NuEditor

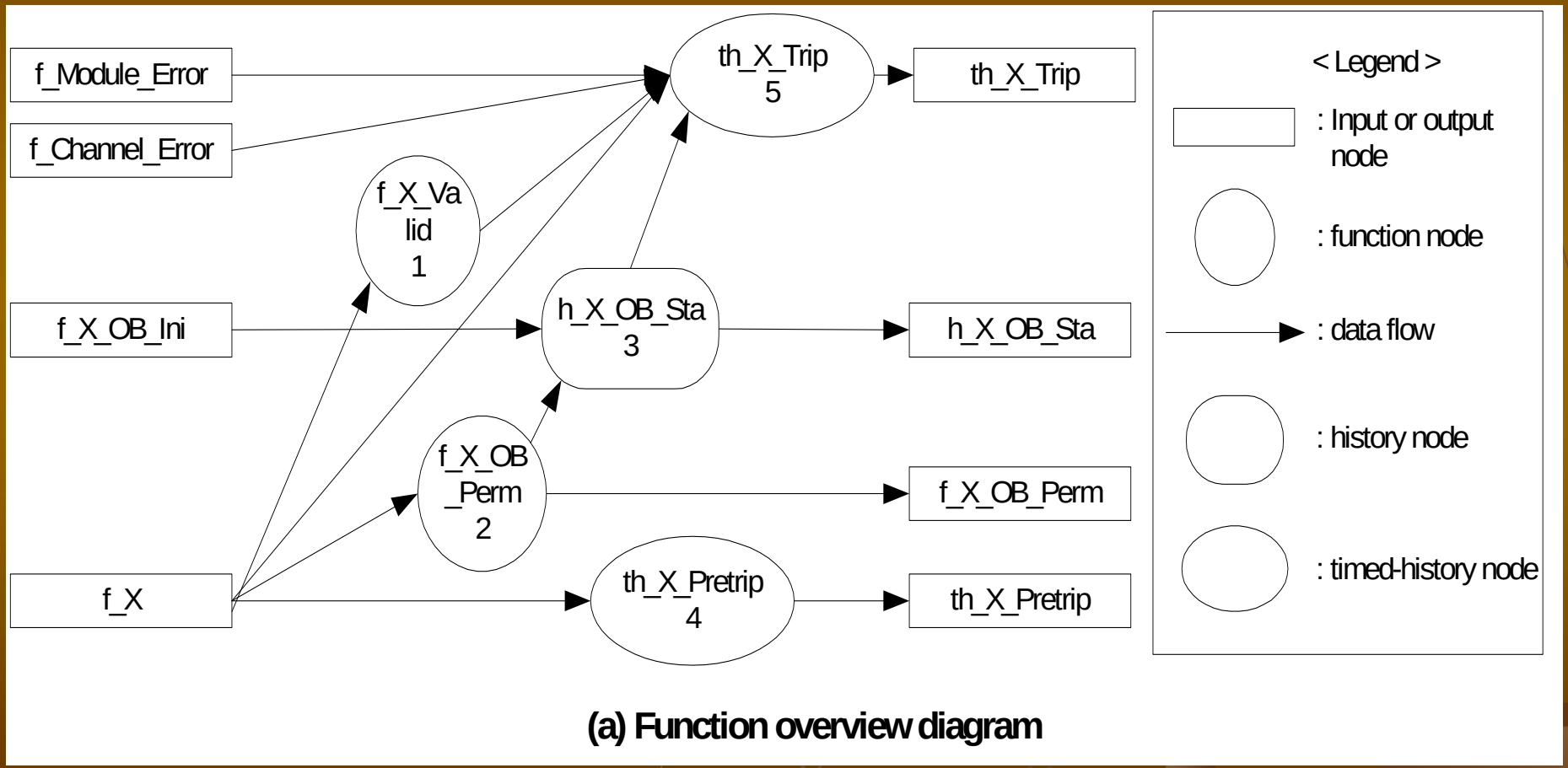
- Customize SCR to effectively reflect characteristics unique to nuclear engineering domain
  - "tables-always" notation is difficult to read (to domain experts) when documenting time- and state-dependent requirements
- NuEditor supports graphical editing and formal verification of NuSCR

NuSCR

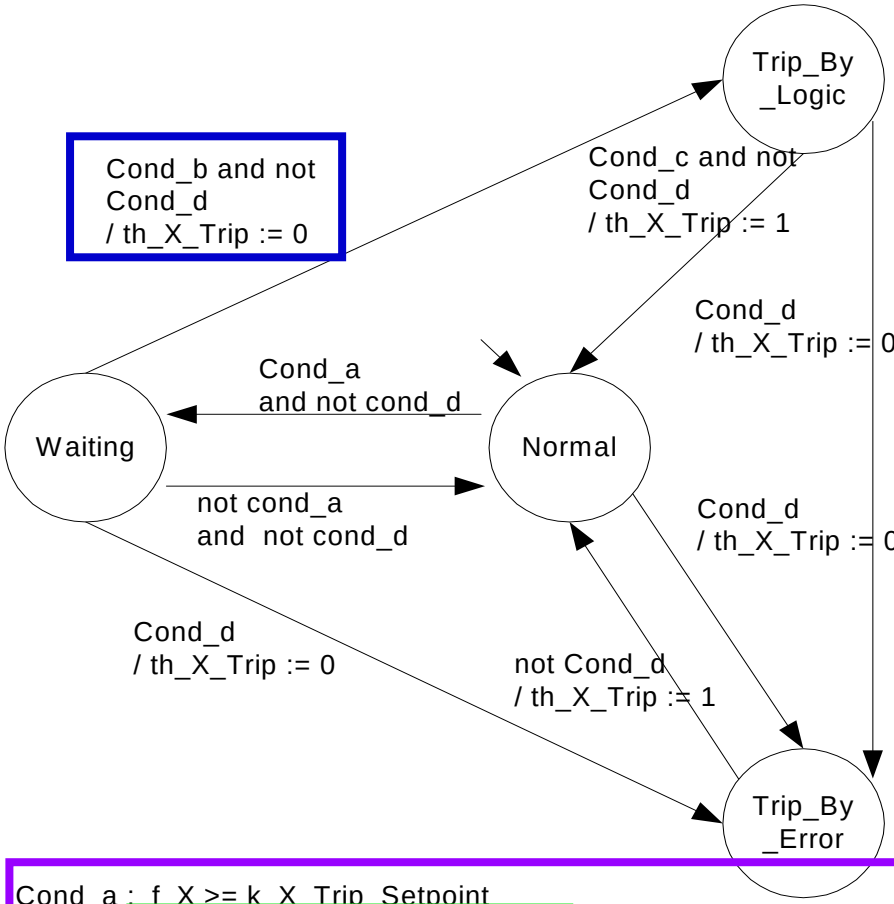
- Function Overview Diagram
- Function Variable
- History Variable
- Timed-history Variable



Function Overview Diagram

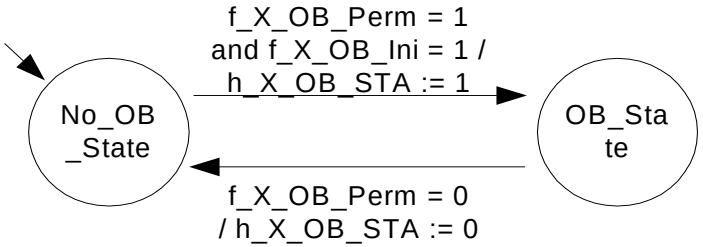


(a) Function overview diagram



Cond_a : f_X >= k_X_Trip_Setpoint
Cond_b : [k_Trip_Delay, k_Trip_Delay] (f_X >= k_X_Trip_Setpoint and h_X_OB_Sta = 0)
Cond_c : f_X < k_X_Trip_Setpoint - k_X_Trip_Hys
Cond_d : f_X_Valid = 1 or f_Module_Error = 1 or f_Channel_Error = 1)

(b) Timed history variable node defined by TTS for th_X_Trip



(c) History variable node defined by FSM for h_X_OB_Sta

Conditions		
k_X_MIN <= f_X <= k_X_MAX	T	F
Actions		
f_X_Valid := 0	X	
f_X_Valid := 1		X

(d) Function Variable Node defined as SDT for f_X_Valid

NuSCR Semantics

ARTICLE IN PRESS

Available at
www.ElsevierComputerScience.com
POWERED BY SCIENCE DIRECT®

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

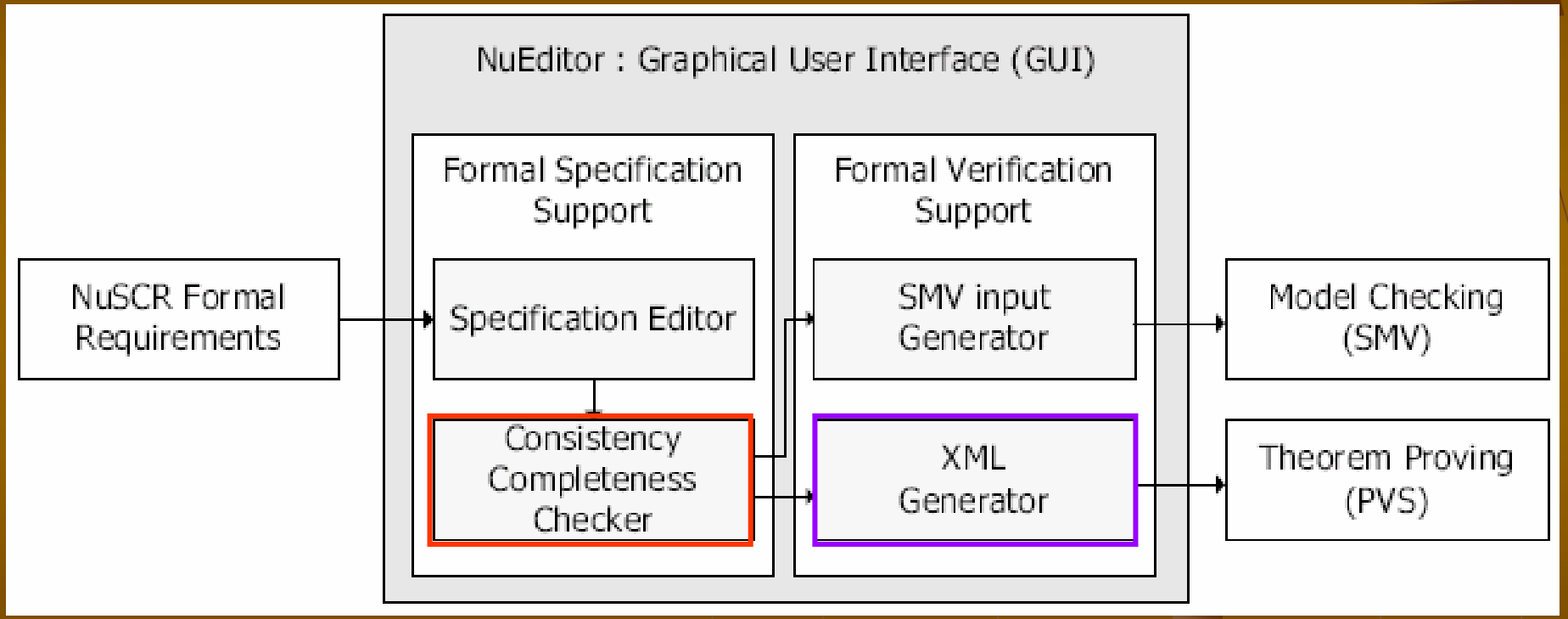
Junbeom Yoo [a,*], Taihyo Kim [a], Sungdeok Cha [a], Jang-Soo Lee [b], Han Seong Son [b]

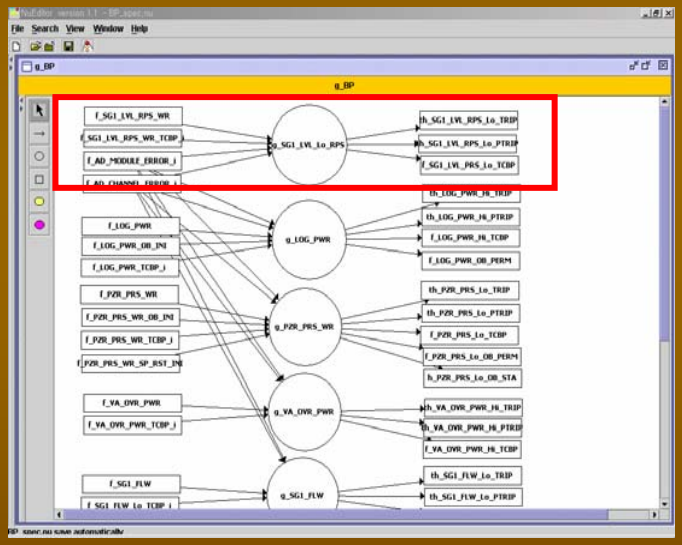
[a] *Department of Electrical Engineering and Computer Science, Korea Advanced Institute of Science and Technology (KAIST) and AITrc/SPIC, 373-1, Kusong-dong, Yusong-gu, Taejon 305701, South Korea*

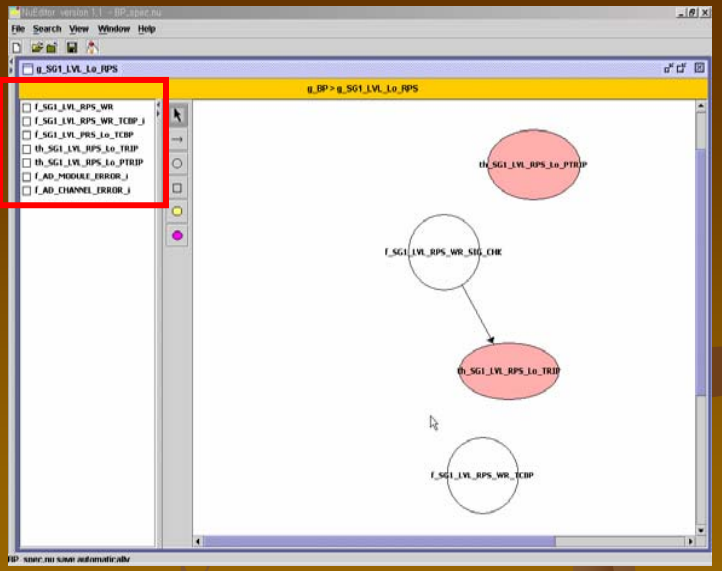
[b] *Korea Atomic Energy Research Institute (KAERI), MMIS team, 150, Deokjin-dong, Yusong-gu, Taejon, South Korea*

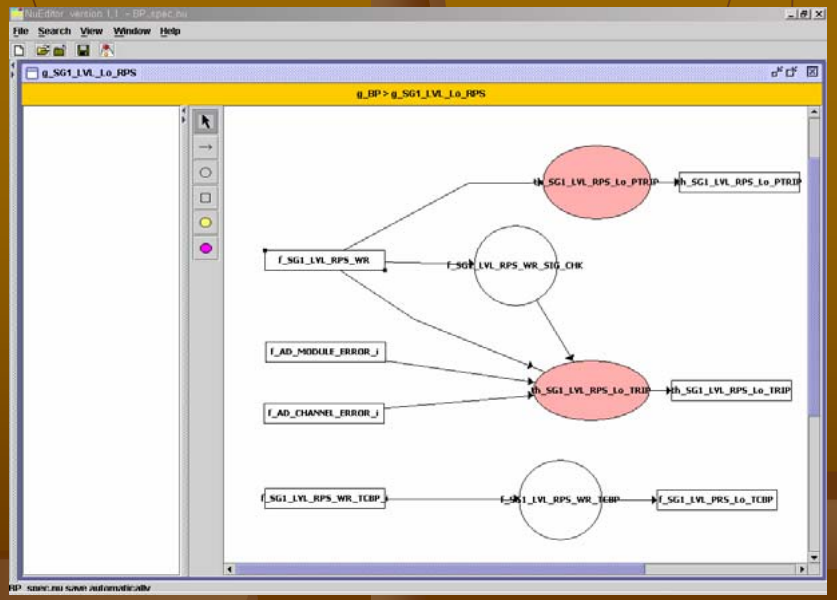
Received 18 March 2003; received in revised form 29 September 2003; accepted 5 October 2003

NuEditor

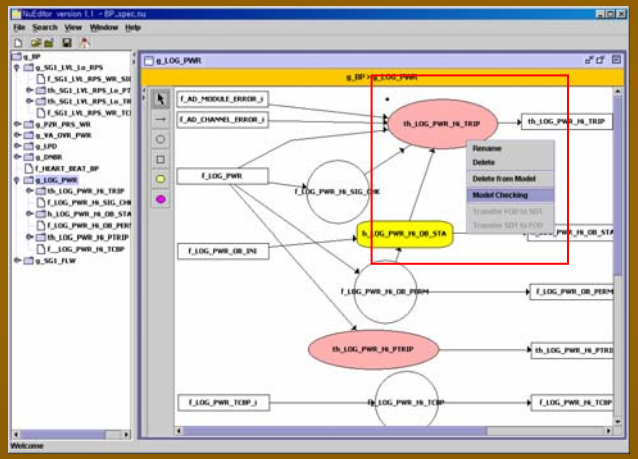

NuEditor : Graphical User Interface (GUI)
Formal Specification Support
Formal Verification Support
NuSCR Formal Requirements
Specification Editor
Consistency Completeness Checker
SMV input Generator
XML Generator
Model Checking (SMV)
Theorem Proving (PVS)

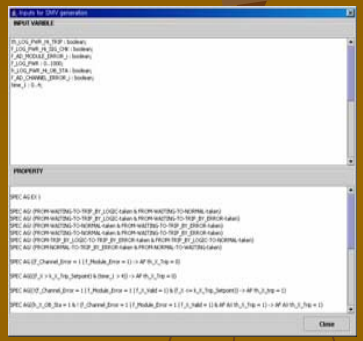

NuEditor version 1.1 - BP.spec.nu
File Search View Window Help
g_BP
g_BP
f_SG1_LVL_RPS_WR
f_SG1_LVL_RPS_WR_TCBP_I
f_AD_MODULE_ERROR_I
g_SG1_LVL_1o_RPS
th_SG1_LVL_RPS_1o_TRIP
th_SG1_LVL_RPS_1o_PTRIP
f_SG1_LVL_PRS_1o_TCBP
f_LOG_PWR
f_LOG_PWR_OB_INI
f_LOG_PWR_TCBP_I
g_LOG_PWR
th_LOG_PWR_Hi_TRIP
th_LOG_PWR_Hi_PTRIP
f_LOG_PWR_Hi_TCBP
f_LOG_PWR_OB_PERM
f_PZR_PRS_WR
f_PZR_PRS_WR_OB_INI
f_PZR_PRS_WR_TCBP_I
f_PZR_PRS_WR_SP_RST_INI
g_PZR_PRS_WR
th_PZR_PRS_1o_TRIP
th_PZR_PRS_1o_PTRIP
f_PZR_PRS_1o_TCBP
f_PZR_PRS_1o_OB_PERM
h_PZR_PRS_1o_OB_STA
f_VA_OVR_PWR
f_VA_OVR_PWR_TCBP_I
g_VA_OVR_PWR
th_VA_OVR_PWR_Hi_TRIP
th_VA_OVR_PWR_Hi_PTRIP
f_VA_OVR_PWR_Hi_TCBP
f_SG1_FLW
f_SG1_FLW_1o_TCBP_I
g_SG1_FLW
th_SG1_FLW_1o_TRIP
th_SG1_FLW_1o_PTRIP


NuEditor version 1.1 - BP.spec.nu
File Search View Window Help
g_SG1_LVL_1o_RPS
g_BP > g_SG1_LVL_1o_RPS
f_SG1_LVL_RPS_WR
f_SG1_LVL_RPS_WR_TCBP_I
f_SG1_LVL_PRS_1o_TCBP
th_SG1_LVL_RPS_1o_TRIP
th_SG1_LVL_RPS_1o_PTRIP
f_AD_MODULE_ERROR_I
f_AD_CHANNEL_ERROR_I
th_SG1_LVL_RPS_1o_PTRIP
f_SG1_LVL_RPS_WR_SIG_CHK
th_SG1_LVL_RPS_1o_TRIP
f_SG1_LVL_RPS_WR_TCBP

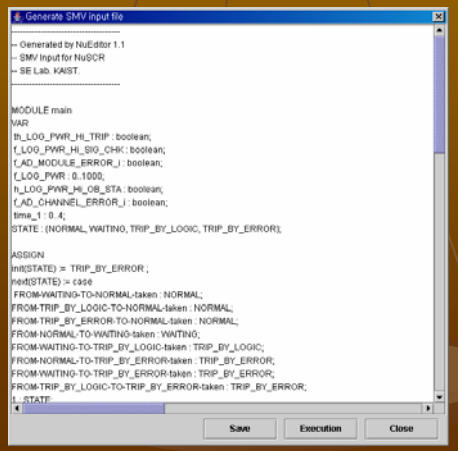

NuEditor version 1.1 - BP.spec.nu
File Search View Window Help
g_SG1_LVL_1o_RPS
g_BP > g_SG1_LVL_1o_RPS
th_SG1_LVL_RPS_1o_PTRIP
th_SG1_LVL_RPS_1o_PTRIP
f_SG1_LVL_RPS_WR
f_SG1_LVL_RPS_WR_SIG_CHK
f_AD_MODULE_ERROR_I
th_SG1_LVL_RPS_1o_TRIP
th_SG1_LVL_RPS_1o_TRIP
f_AD_CHANNEL_ERROR_I
f_SG1_LVL_RPS_WR_TCBP
f_SG1_LVL_RPS_WR_TCBP
f_SG1_LVL_PRS_1o_TCBP

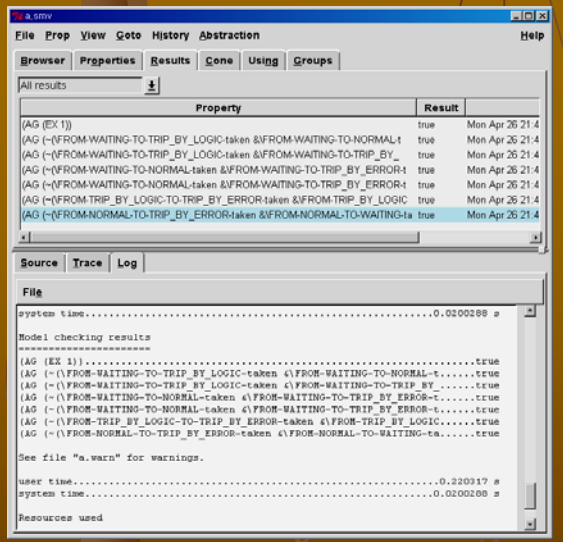
Formal Verification Support





(property)



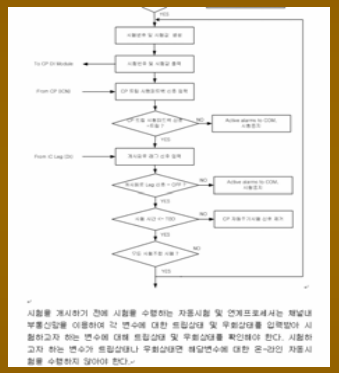


(SMV Model Checking)

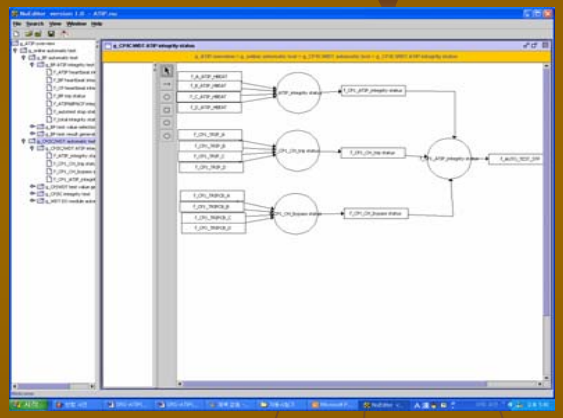
(SMV Input Generation)

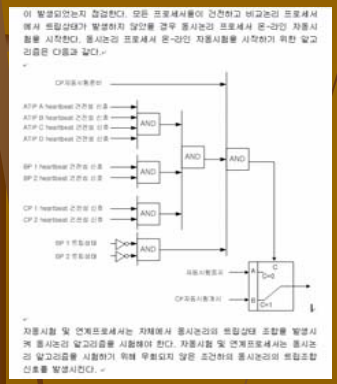
Tool Demonstration…

NuEditor “In Action”



SRS Rev.00



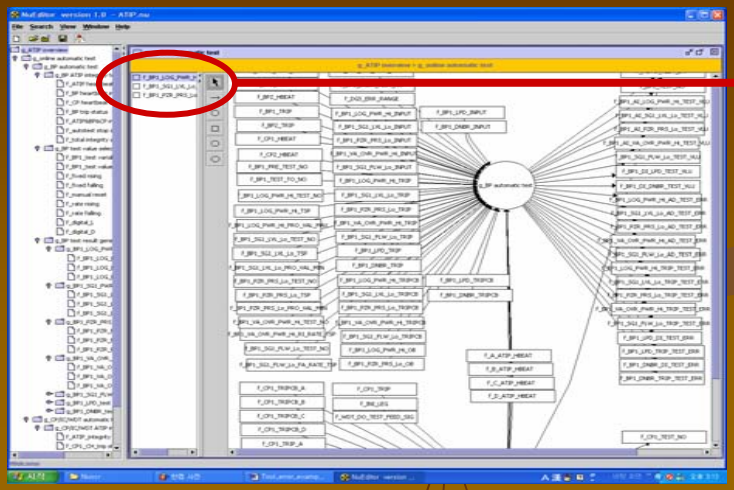


SRS Rev.01

Contributed in learning that initialization algorithm was missing !!!

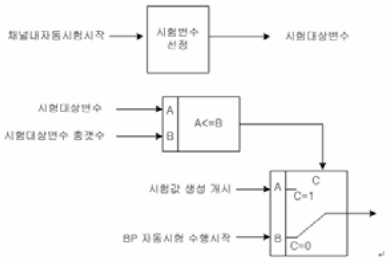
5.3.4.2.1 비교논리 프로세서 자동주기시험

1. 입력
   1) 채널 자동시험 시작
   2) 채널 A ATIP 건전성 신호
   3) 채널 B ATIP 건전성 신호
   4) 채널 C ATIP 건전성 신호
   5) 채널 D ATIP 건전성 신호
   6) BP 1 건전성 신호
   7) BP 2 건전성 신호
   8) CP 1 건전성 신호
   9) CP 2 건전성 신호
   10) BP 1 트립상태
   11) BP 2 트립상태
   12) 트립채널우회상태
   13) 운전우회상태
   14) 트립 설정치
   15) 예비트립 설정치
   16) 공정변수값
   17) 비율설정치
2. 출력
   1) 시험중지
   2) 비교논리 시험변수
   3) 비교논리 시험값
   4) 비교논리 A/D 변환 자동시험 오류
   5) 비교논리 트립 자동시험 오류
   6) 비교논리 DI 입력 자동시험 오류



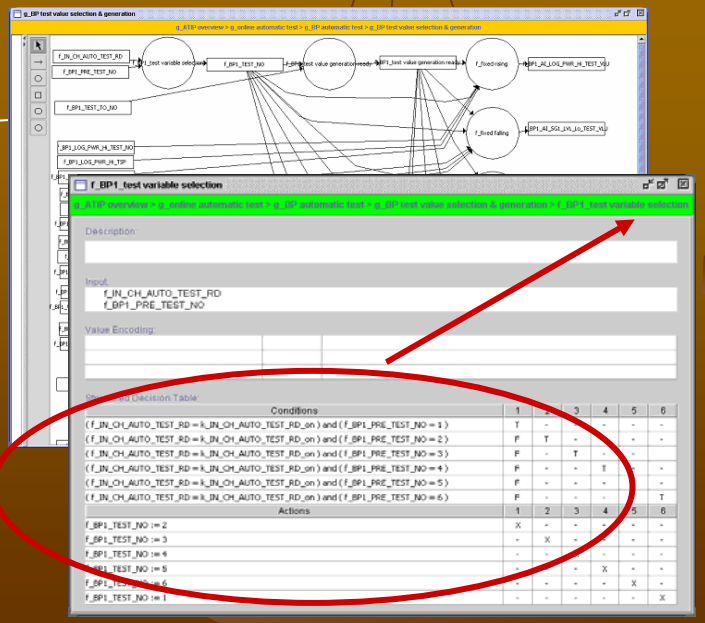
Found inconsistent use of variables

를 선택하는 자동시험 및 연계프로세서 알고리즘은 다음과 같다.



자동시험 및 연계프로세서는 비교논리 프로세서 자동주기시험을 위해 먼저 각 공정변수에 대해 트립을 발생시키는 시험값을 생성해야 한다. 이를 위해 자동시험 및 연계프로세서는 비교논리프로세서로부터 채널내부통신망(ICN)을 이용하여 각 시험변수의 현재값 및 설정치를 입력받는다. 자동시험 및 연계프로세서는 입력받은 현재값 및 설정치를 이용하여 그 변수가 트립상태를 유발하는 시험값을 랜덤하게 생성한다.

상승트립 고정설정치 비교논리를 시험하기 위해 입력되는 변수 시험값은 트립설정치보다 큰 값이 되어야 한다. 상승트립 고정설정치를 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

Function Block Diagram
Synthesis

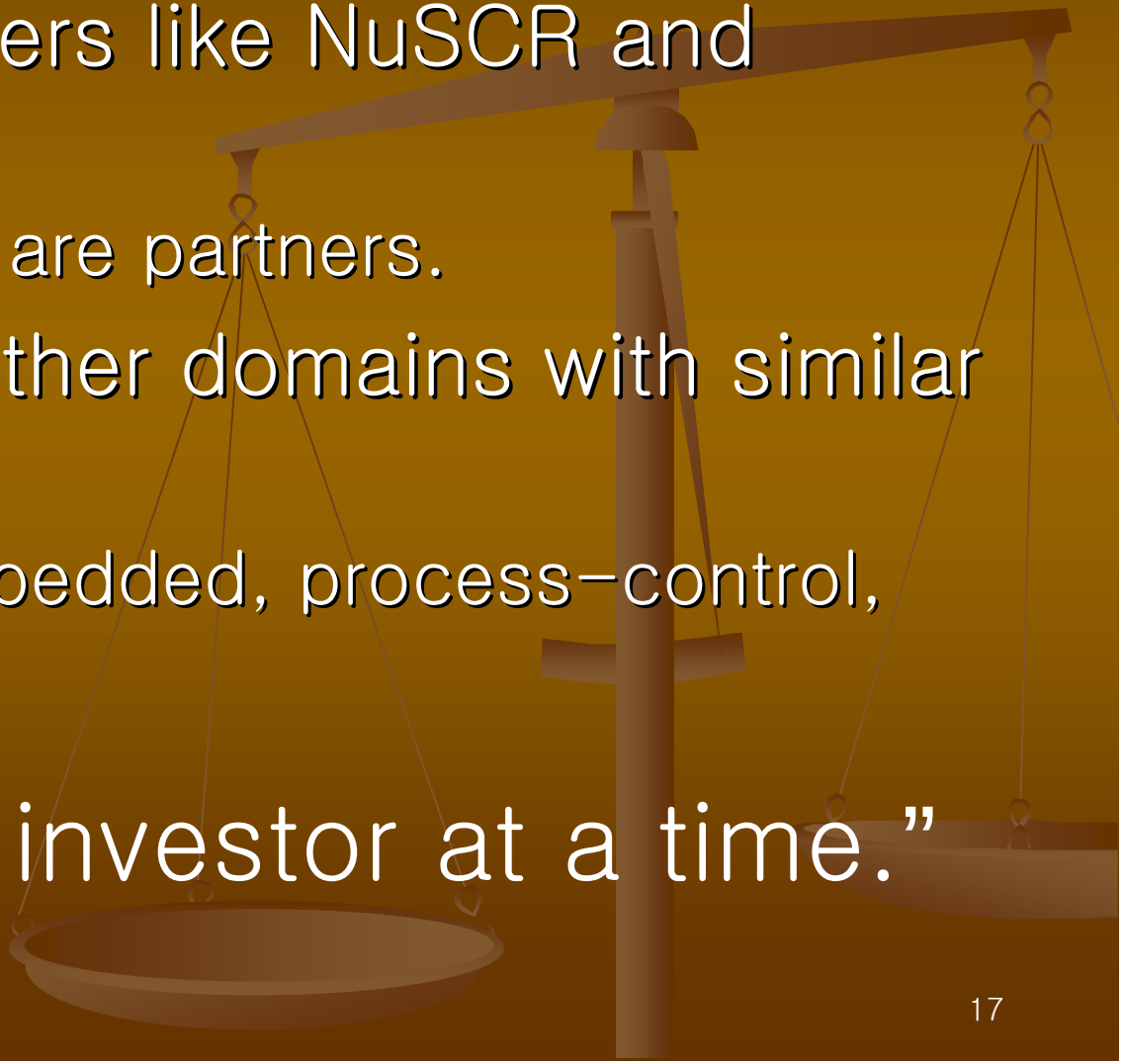
Stay tuned...

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."