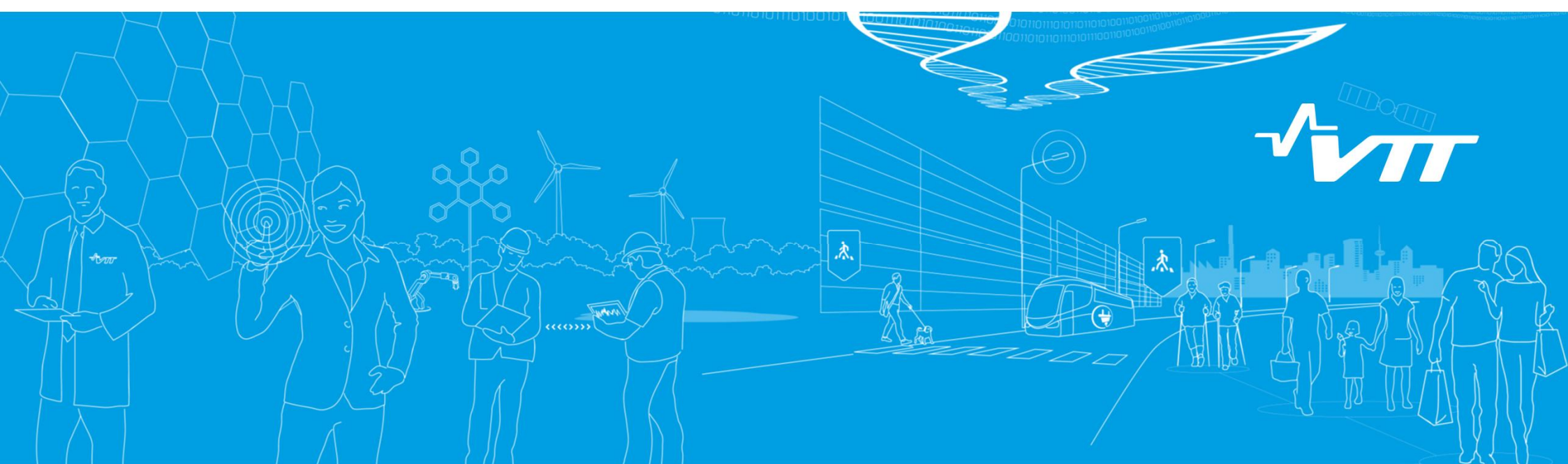
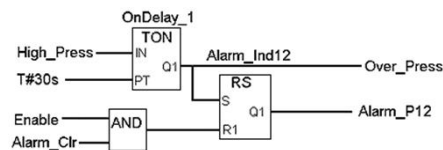
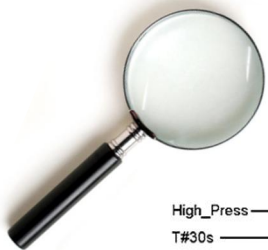




Mallintarkastus automaatio-ohjelmistojen verifiointimenetelmänä

Antti Pakonen

ASAF Ydinvoima-automaation teemapäivä
22.5.2014 Säteilyturvakeskus

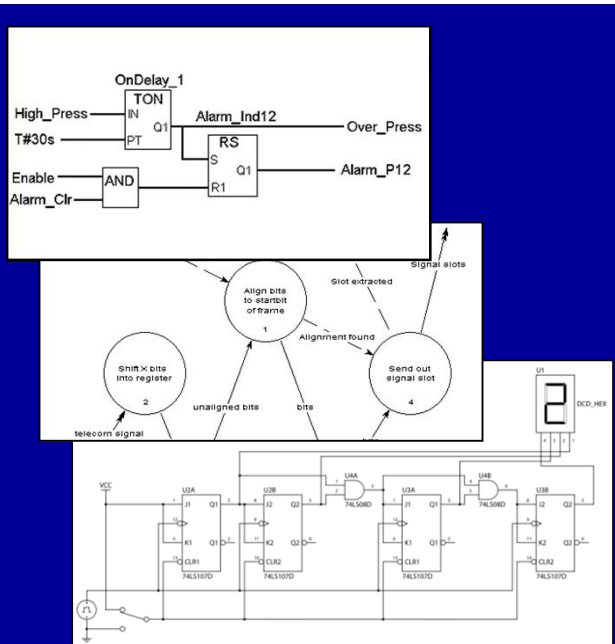


SAFIR – Kansallinen ydinvoimalaitosten turvallisuustutkimusohjelma 2011-2014

- Tutkimus alkoi aiemmassa SAFIR-ohjelmassa vuonna 2007.
- Nopeasti tuloksia tutkimuspiloteissa
- Käytännön soveltaminen STUK:n kanssa käyntiin jo 2008



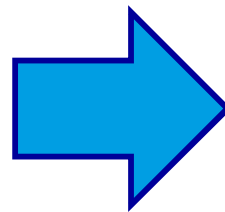
Automaation sovellusohjelmiston verifiointi



Program

Function Block Diagram
State Chart Diagram
FPGA schematic

Generate
code



```
#include <stdio.h>
#include <stdlib.h>
#include <sys/types.h>
#include <arpa/inet.h>

void server1(portServ ports)
{
    int sockServ1, sockServ2, sockClient;
    struct sockaddr_in monAddr, addrClient, addrServ2;
    socklen_t lenAddrClient;

    if ((sockServ1 = socket(AF_INET, SOCK_STREAM, 0)) == -1) {
        perror("Error socket");
        exit(1);
    }
    if ((sockServ2 = socket(AF_INET, SOCK_STREAM, 0)) == -1) {
        perror("Error socket");
        exit(1);
    }

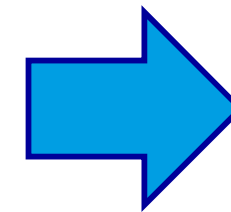
    bzero(monAddr, sizeof(monAddr));
    monAddr.sin_family = AF_INET;
    monAddr.sin_port = htons(ports.port1);
    monAddr.sin_addr.s_addr = INADDR_ANY;
    bzero(addrServ2, sizeof(addrServ2));

    private void doGet(HttpRequest req, String user, String password) {
        // ... (omitted code) ...
    }
}
```

Code

C, Java...
Assembly
FPGA netlist

Compile
& upload
binary

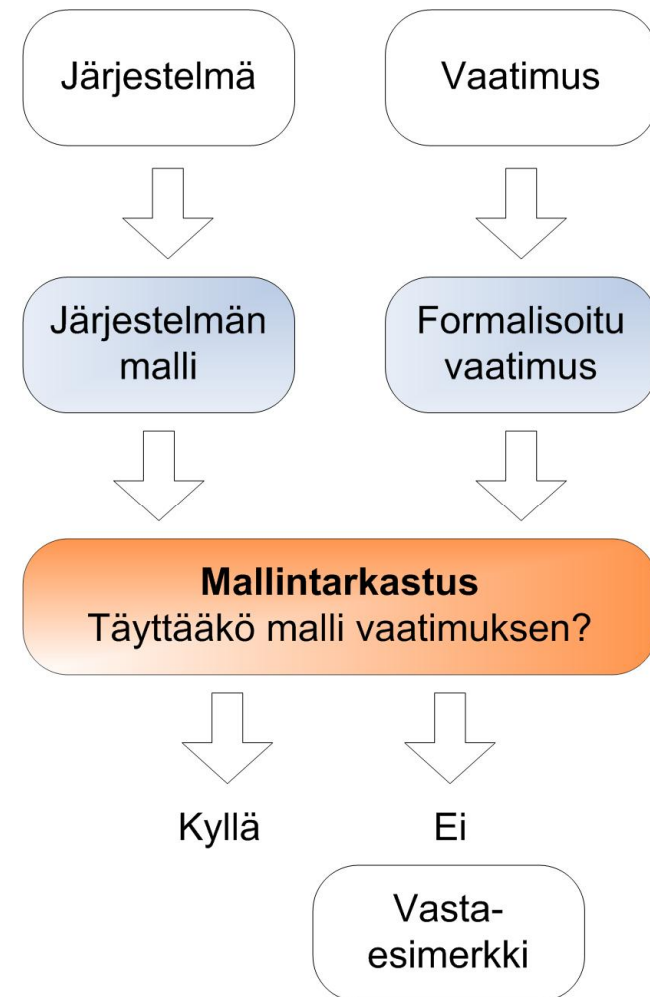


Embedded System

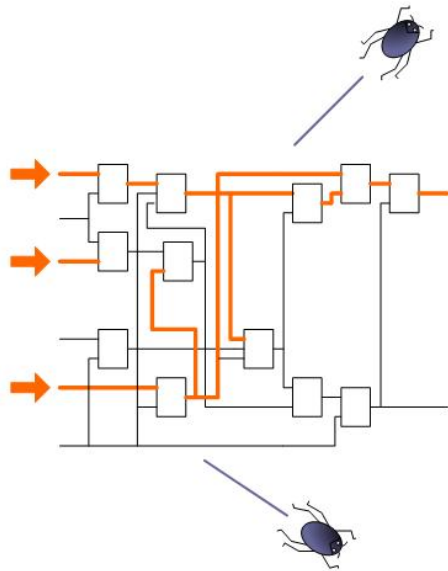
PLC, FPGA,
PC, μ C...

Mallintarkastus

- Mallintarkastus on tehokas menetelmä kriittisten järjestelmien verifiointiin.
- Mallintarkastin on työkalu, joka testaa kattavasti, että tarkasteltavasta järjestelmästä tehty malli täyttää määritellyt vaatimukset.
 - Vastaus on joko **KYLLÄ**...
 - ...tai **EI**, missä tapauksessa mallintarkastin palauttaa vastaesimerkin, josta näkyy vaatimuksen rikkova suorituspolk.

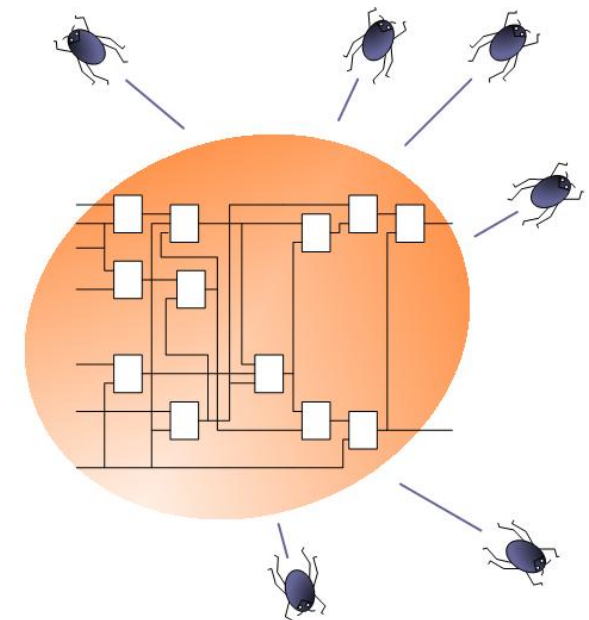


Mallintarkastus vs. testaus ja simulointi



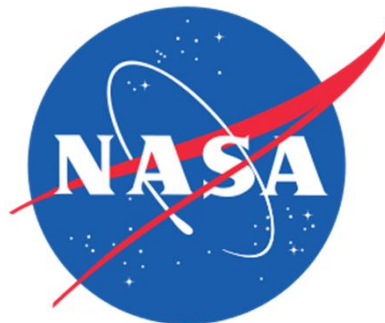
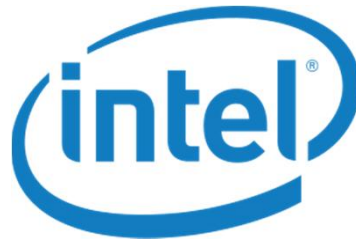
- Testaus ja simulointi perustuvat aina siihen, että käydään läpi rajallinen määrä testitapauksia tai ajoja.
- Jo verraten yksinkertaisille binääripiireille 100% testikattavuus on käytännössä mahdotonta saavuttaa.

- Mallintarkastus ei perustu siihen, että kaikki tilat lasketaan läpi, vaan kattavuus saavutetaan huomioimalla kaikki vaatimusten kannalta oleelliset tilat.
- Käytännössä haku puumaisesta tietorakenteesta

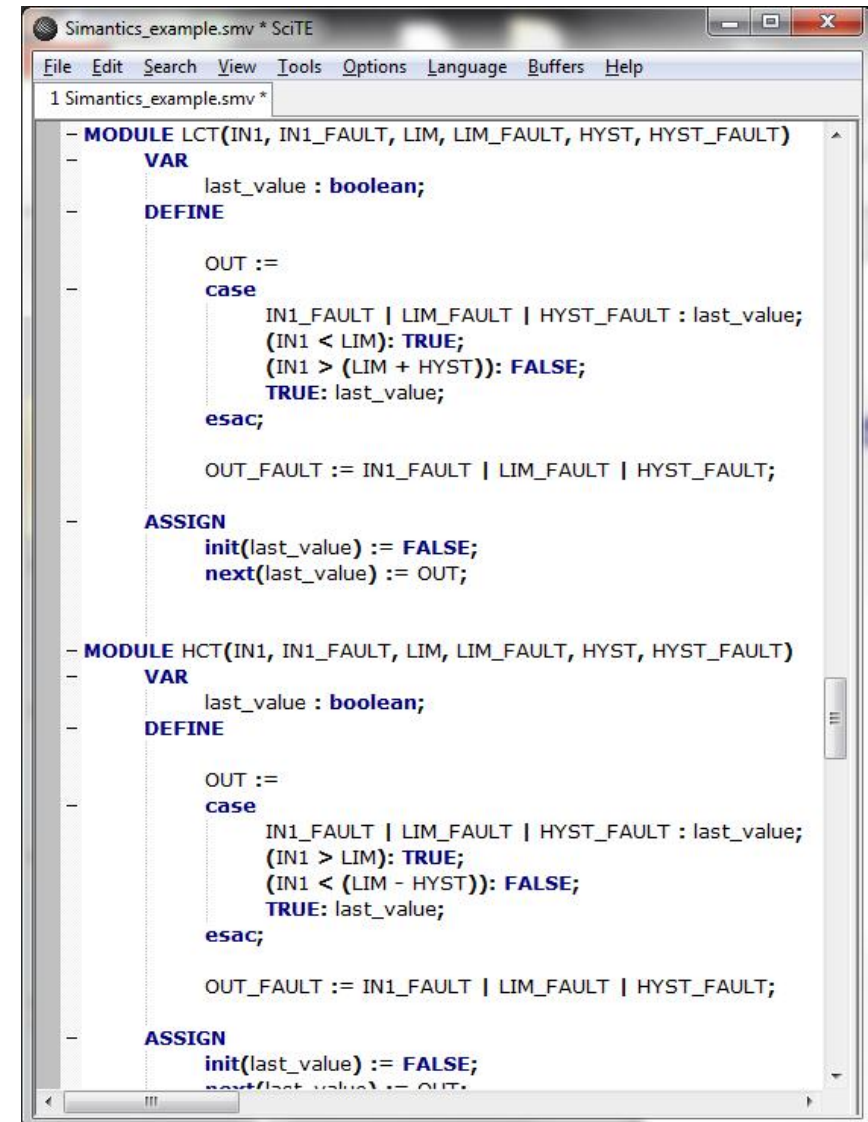
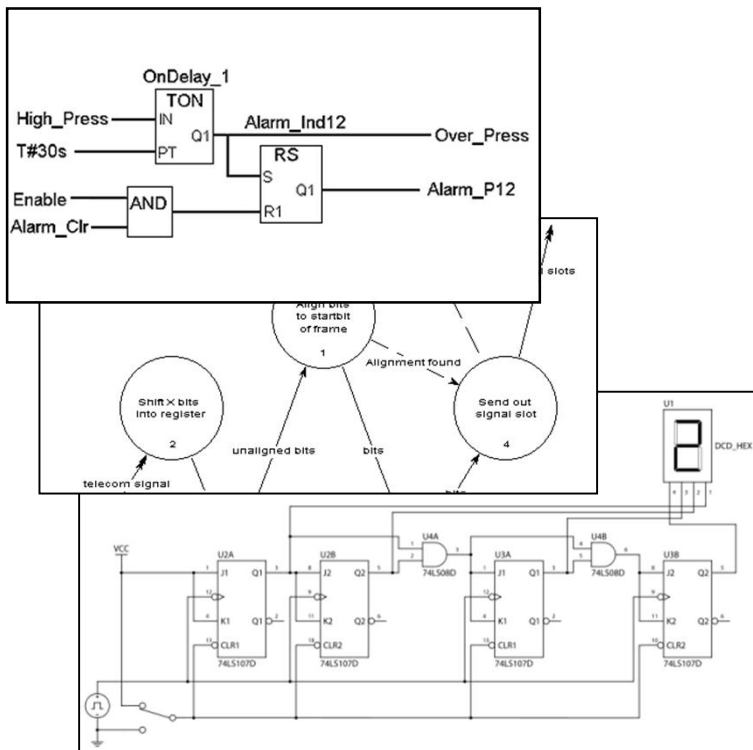


Historiaa

- Teoria kehitetty 1980-luvun alussa
- 1990-luvulla laitteet, esim. prosessorit
- 2000-luvulla myös ohjelmistot



Haasteet: Mallinnus



Haasteet: Vastaesimerkkien tulkinta

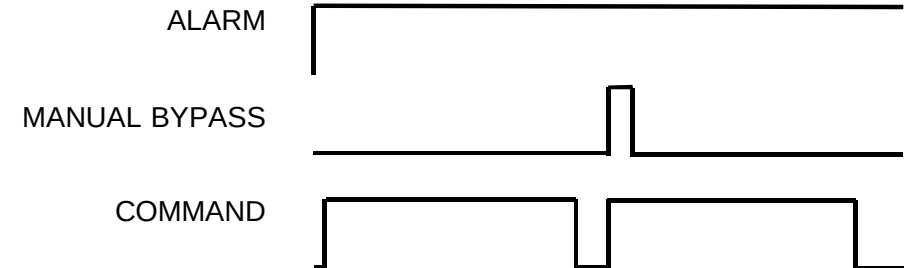
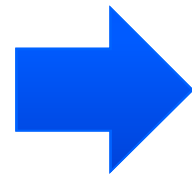
```

Simantics_example.smv - SciTE
File Edit Search View Tools Options Language Buffers Help
1 Simantics_example.smv

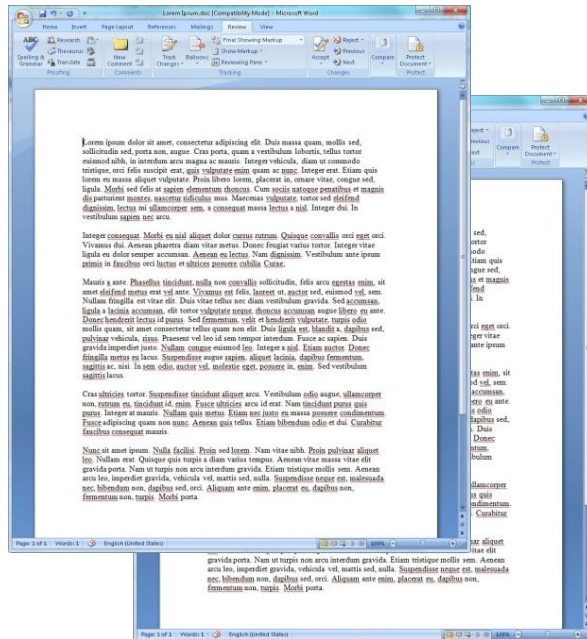
elapsed: 0.00 seconds, total: 0.00 seconds
-- specification EF BLOCK_301_0.PUL001.previousGoodInput = TRUE is true
-- specification G ITANK01_REFILL_FAULT is false
-- as demonstrated by the following execution sequence
Trace Description: LTL Counterexample
Trace Type: Counterexample
-> State: 1.1 <-
TANK01_L_S_1 = 0
TANK01_L_S_1_FAULT = FALSE
TANK01_L_S_2 = 0
TANK01_L_S_2_FAULT = FALSE
TANK01_L_S_3 = 0
TANK01_L_S_3_FAULT = FALSE
MAN_S_RESET = FALSE
MAN_S_RESET_FAULT = TRUE
BLOCK_201_0.LCT001.last_value = FALSE
BLOCK_201_0.LCT002.last_value = FALSE
BLOCK_201_0.LCT003.last_value = FALSE
BLOCK_201_0.HCT001.last_value = FALSE
BLOCK_201_0.HCT002.last_value = FALSE
BLOCK_201_0.HCT003.last_value = FALSE
BLOCK_201_0.TOF001.clock = 10
BLOCK_201_0.TOF001.previousGoodInput = FALSE
BLOCK_201_0.TOF002.clock = 10
BLOCK_201_0.TOF002.previousGoodInput = FALSE
BLOCK_301_0.PUL001.clock = 0
BLOCK_301_0.PUL001.previousGoodInput = FALSE
BLOCK_301_0.SR001.memory = FALSE
BLOCK_301_0.SR002.memory = FALSE
TANK01_FLUSH_FAULT = TRUE
TANK01_FLUSH = FALSE
TANK01_REFILL_FAULT = TRUE
TANK01_REFILL = FALSE
BLOCK_101_0.LEVEL_3_FAULT = TRUE
BLOCK_101_0.LEVEL_3 = 0
BLOCK_101_0.LEVEL_2_FAULT = TRUE
BLOCK_101_0.LEVEL_2 = 0
BLOCK_101_0.LEVEL_1_FAULT = TRUE
BLOCK_101_0.LEVEL_1 = 0
BLOCK_101_0.LCL001.OUT_FAULT = TRUE
BLOCK_101_0.LCL001.OUT = 0
BLOCK_101_0.LCL002.OUT_FAULT = TRUE
BLOCK_101_0.LCL002.OUT = 0
BLOCK_101_0.LCL003.OUT_FAULT = TRUE
BLOCK_101_0.LCL003.OUT = 0
BLOCK_201_0.ALARM_HI_FAULT = FALSE
BLOCK_201_0.ALARM_HI = TRUE
BLOCK_201_0.ALARM_LO_FAULT = FALSE
BLOCK_201_0.ALARM_LO = TRUE
BLOCK_201_0.LCT001.OUT_FAULT = TRUE
BLOCK_201_0.LCT001.OUT = FALSE
BLOCK_201_0.LCT002.OUT_FAULT = TRUE
BLOCK_201_0.LCT002.OUT = FALSE
BLOCK_201_0.LCT003.OUT_FAULT = TRUE
BLOCK_201_0.LCT003.OUT = FALSE
BLOCK_201_0.HCT001.OUT_FAULT = TRUE
BLOCK_201_0.HCT001.OUT = FALSE
BLOCK_201_0.HCT002.OUT_FAULT = TRUE
BLOCK_201_0.HCT002.OUT = FALSE
BLOCK_201_0.HCT003.OUT_FAULT = TRUE
BLOCK_201_0.HCT003.OUT = FALSE

BLOCK_301_0.SR002.memory = TRUE
-> State: 2.4 <-
-- specification G (MAN_S_RESET_FAULT -> ITANK01_REFILL_FAULT) is true
-- specification G (MAN_S_RESET_FAULT -> ITANK01_FLUSH_FAULT) is true
elapsed: 0.14 seconds, total: 0.32 seconds
>Exit code: 0

```

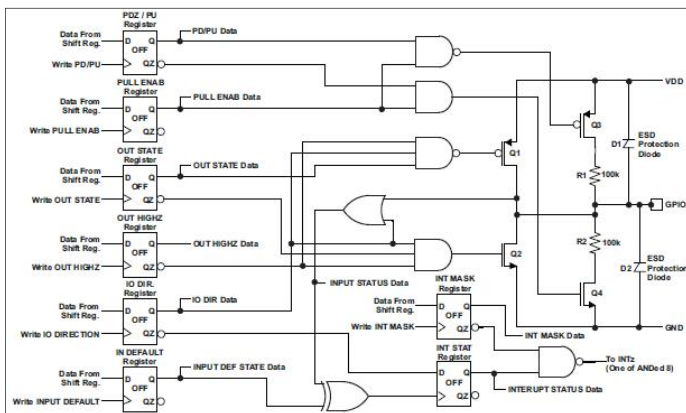


Haasteet: Vaatimukset



$(G \text{ !Alarm}) \mid (!\text{Alarm} \cup (\text{Alarm} \& F$
 Shutdown $\rightarrow (!\text{Shutdown} \cup ((\text{Temperature} < 55) \& !\text{Shutdown} \& X (!\text{Shutdown} \cup$
 Feedback_pump = OFF)))

$G((\text{Shutdown} \& !((T4_Level_M < 230)))$
 $\rightarrow (G(V15_Open) \mid !V15_Open$
 $\cup (T4_Level_M < 230)))$



Referenssit

- Automaatio-ohjelmistojen verifiointi mallintarkastuksella on vakiintunut osaksi Suomen ydinvoimateollisuuden käytäntöjä.

- Evaluation of NPP I&C system designs 2008-2011



- Verification of nuclear automation 2009
- Verification of nuclear I&C by model checking 2012-



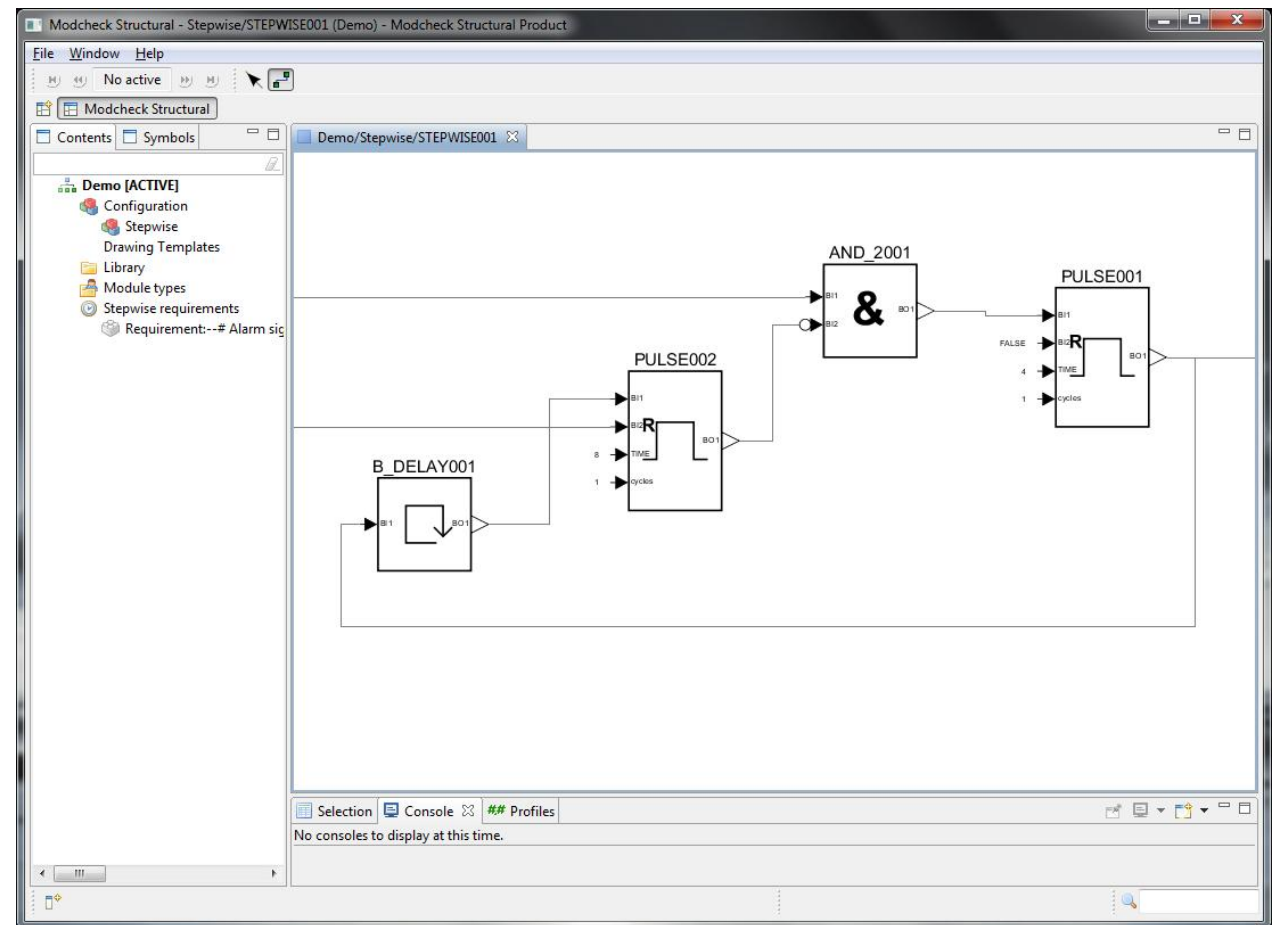
Mallintarkastus ydinvoimahankkeessa



- Jos piilevät virheet löytyvät vasta viranomaisen syynissä, toimintamalli ei ole järin tehokas.
- Parasta olisi soveltaa menetelmää jo suunnittelun yhteydessä.
- Olemassa olevia järjestelmiä uusittaessa paras asiantuntemus vaatimuksista voi kuitenkin olla luvanhaltijalla.

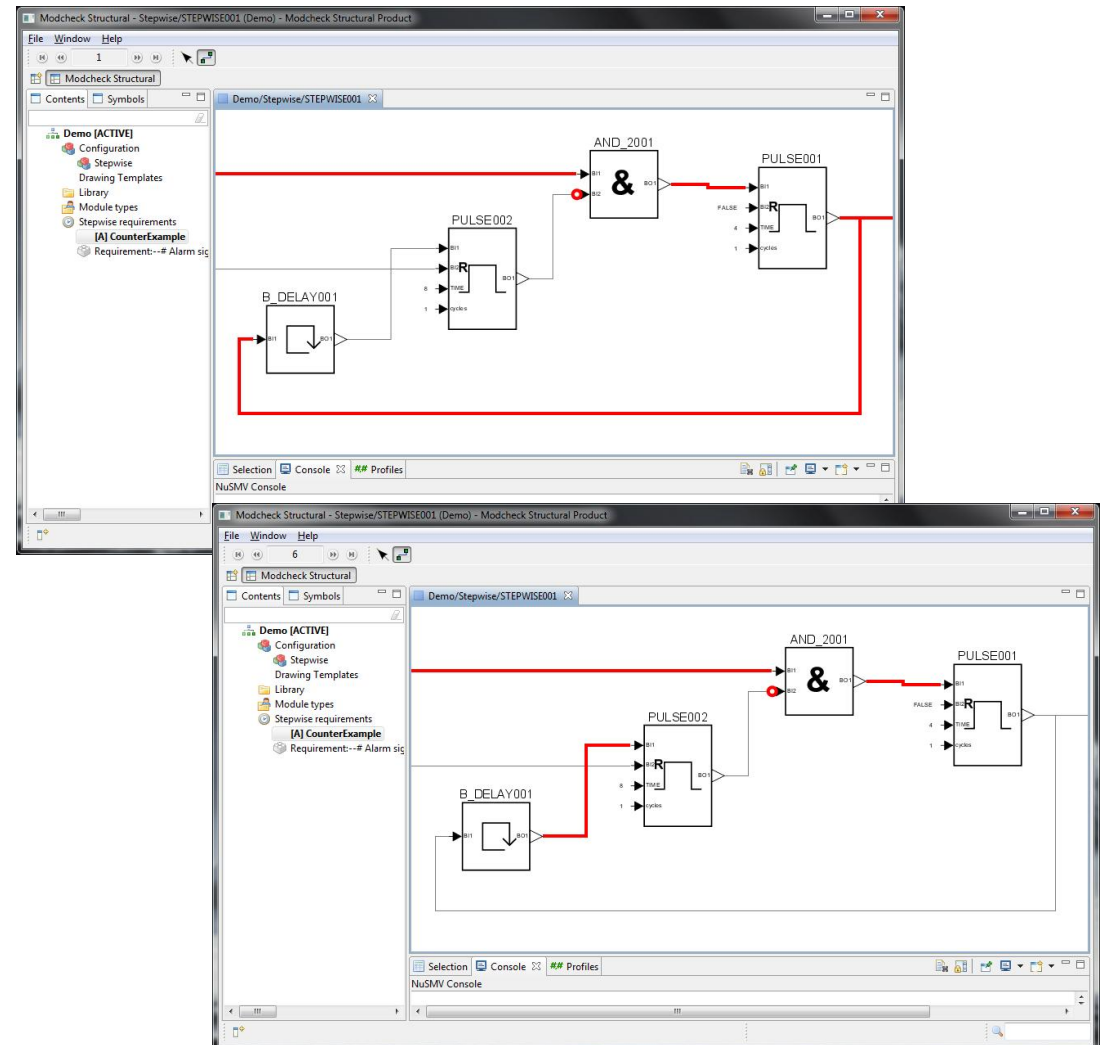
Demo: VTT:n mallintarkastustyökalu

- Simantics – open-source platform for modelling and simulation
- <https://www.simantics.org/>
- Mallin määrittely 2D-piirtotyökalulla.



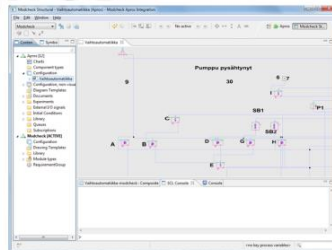
Demo: VTT:n mallintarkastustyökalu

- Vastaesimerkkien visualisointi animaatioina.
- Jatkossa: kaavioiden automaattinen muunnos eri järjestelmistä.



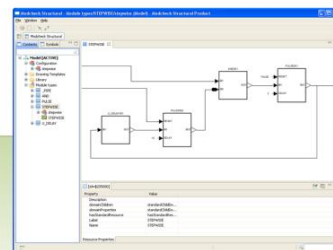
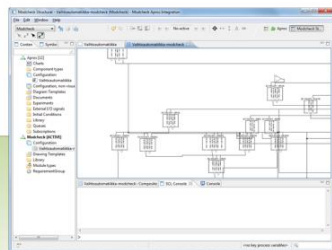
Mallimuunnokset

Apros



Vendor-specific
FB language

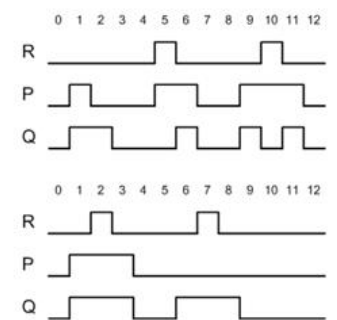
MC-APROS



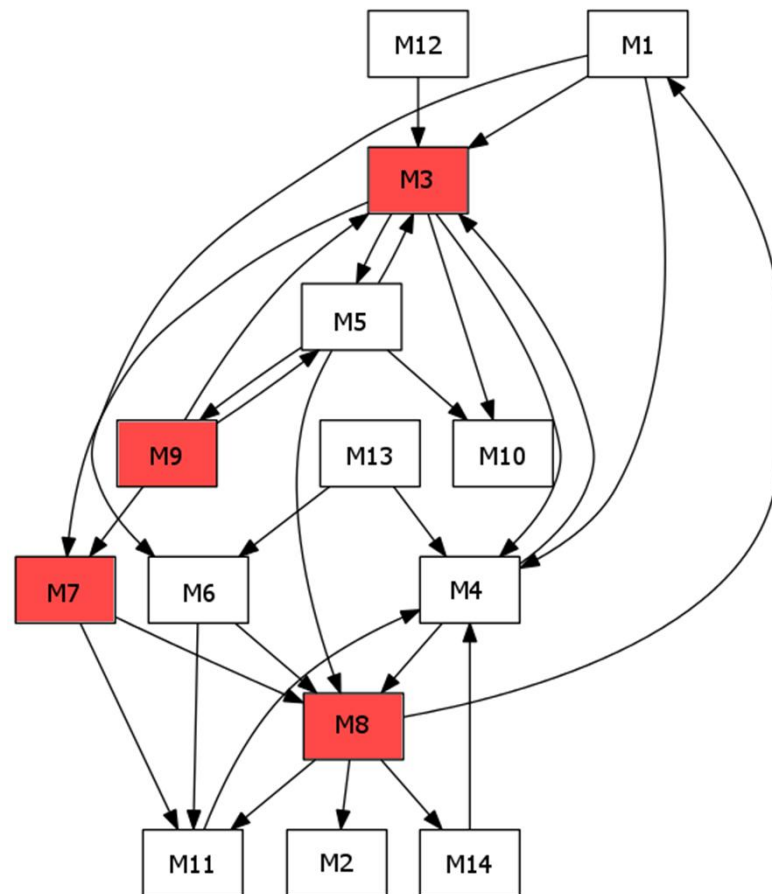
MODCHK

NuSMV

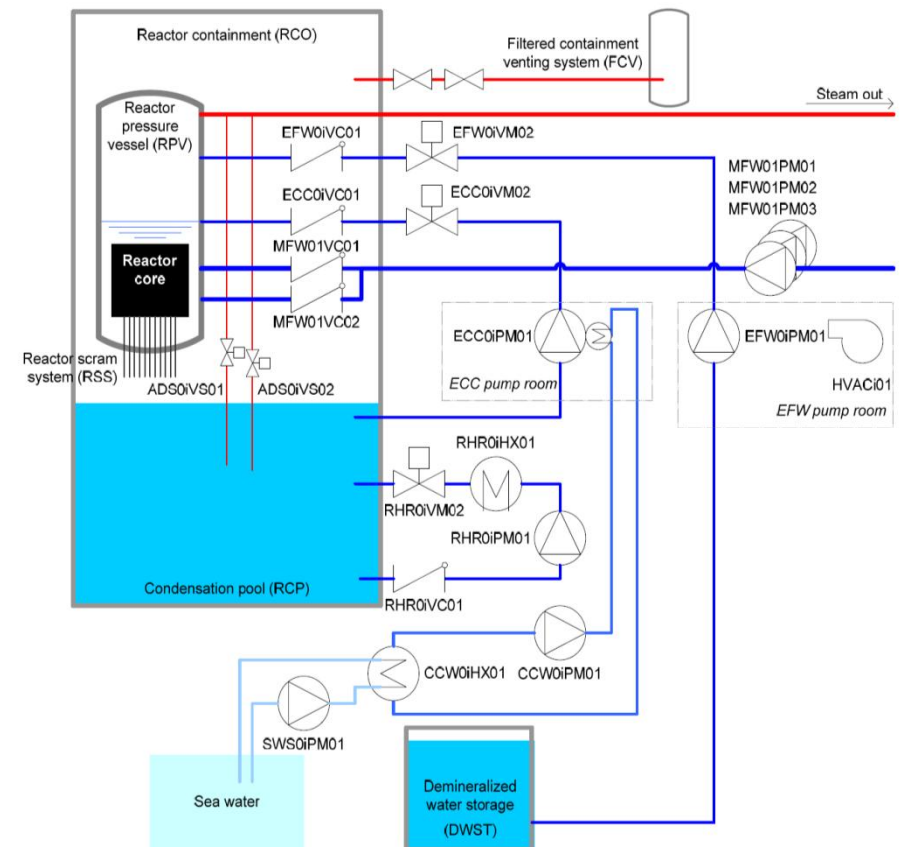
Vaatimukset

Title:	Conditional leads to	
Sentence:	While R is not true, P leads to Q	
Formulas:	LTL	$G (!R \rightarrow G (P \rightarrow Q)) ;$
	PSL	$\text{always} (!R \rightarrow \text{always} (P \rightarrow Q)) ;$
Guidance:	A cause-and-effect relationship of certain model states or signals might not be true at all cycles due to, e.g., an overriding signal with higher priority, or a periodic test sequence or a manual user action temporarily inhibiting normal signal flow. This template allows for the specification of a state or signal R which will (temporarily) break the cause-and-effect relationship between P and Q. That is, if R is not true, P will lead to Q at all cycles. Note that "P leads to Q" (or Q) <i>may</i> still be true regardless of the value of R, it is just that "P leads to Q" <i>has</i> to be true <i>only</i> when R is false.  <i>Examples of traces where the requirement holds</i> Notes on formulas: - The Boolean proposition $(P \rightarrow Q)$ can be replaced with other logic to achieve other "Conditional" formulas. - The LTL formula $G !R \rightarrow G (P \rightarrow Q)$; without the surrounding parenthesis means that scenarios where R has been active at some point will not be considered in verification. That is, the verification tool will assume that R can never be true.	
Keywords:	conditional, protection, interlock, leads to	
Related templates:	Conditional response	

Laajojen mallien modulaarinen analyysi



Laitteiston vikaantumismekanismit



Lopuksi

- 100% kattavuus
- Soveltuu erityisen hyvin turvalogiikoiden arviointiin
- Suomessa ydinvoima-alalla jo vakiintuneessa käytössä



- <http://www.vtt.fi/mallintarkastus/>