Reliability of New Plant Automation of Loviisa NPP

Kalle Jänkälä

NKS/DIGREL seminar, VTT Sept. 14, 2010

PRA in automation renewal

Space and planning solutions

- PRA evaluations related to new buildings/rooms (fire, weather, flood...)
  - Check operability in different situations, e.g. when air conditioning is lost

Identification of risks related to works

  - In general the role of PRA is small (taken care of by administrative rules, training,..)
  - PRA study of lifting risks of construction works:
    - affected in selection of the cranes,
    - the positions of the used cranes and the used load paths were determined based on the recognised hazards

Changes into protection criteria

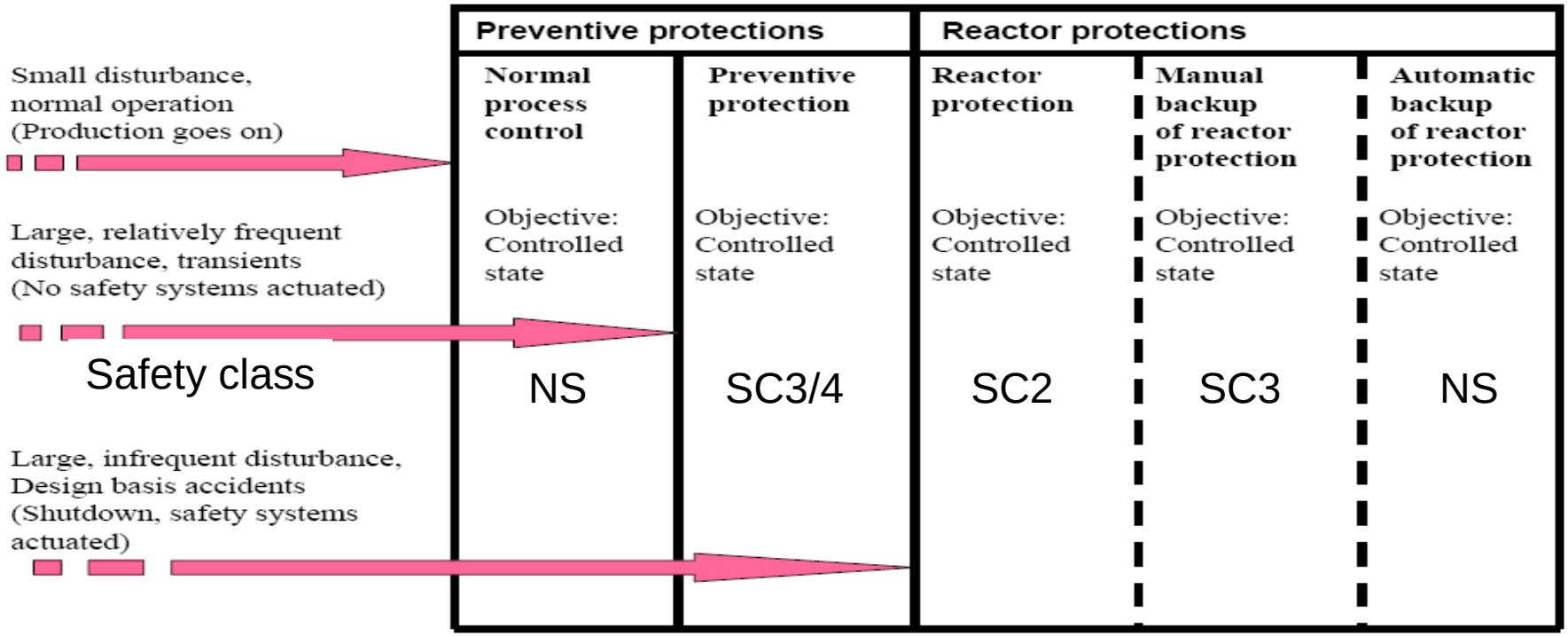
Risk-informed safety classification

Redundancy/diversity solution: adequacy

Automation renewal

- I&C systems and control room man-machine interfaces of the plant units will be replaced in several phases
- All I&C systems including safety related protection systems will be implemented with digital platforms
- Accident management principles are designed by using task categories which perform required safety functions
- Short-term accident management, which is considered in the PRA, consists of five different task categories
  - Normal process control NPC (SPPA-T2000, OM690, FUM)
  - Preventive protection PREV (TXS, QDS, AV42)
    - Preliminary inpection document has been submitted to STUK
  - Reactor protection RPS (TXS, QDS, AV42)
  - Manual Backup of Reactor protection RPSMBU (non-programmable TXS, hard-wired)
  - Automatic Backup of Reactor protection ABU (SPPA-T2000, OM690, AV42)

Defence-in-depth principle in short-term accident management



To be done by the supplier

- Failure mode and effect analyses (FMEA)
- Fault tree analyses
  - These yield inputs to the PRA of Lo
- not yet on a proper level (e.g. failure modes as defined in FMEA, CCF)
- Purpose is to utilise both analyses effectively as a way to demonstrate the fulfillment of the functional and performance requirements. Together these analyses can be used to identify failure modes that are most important for the system reliability and safety, evaluate their influences on system behaviour and propose proper countermeasures.
- shall include both the hardware and software failure modes and their effects on the final system function
- shall include common cause failures of hardware and software (errors)

- PRA is done by the utility

PRA including the new automation

- is developed as the design goes on and new information is obtained
- rough PRA estimate with new plant automation has been done to see
  - the contribution of the new automation to the CDF
  - the sensitivity of the result to various values and assumptions
  - adequacy of the redundancy/diversity

Reliability estimation - problems

Failure data based on histories exist for

- Modules
- Hardware components

for similar or almost similar components to be installed in Lo

⇒Single failure probabilities can be estimated reasonably well

No data for CCF and new software

- Dependencies between different channels of RPS,
- Dependencies between RPS and ABU,
- Dependencies between RPS and ABU and MBU

Importance of the automation

- about 1 % of the Core Damage Frequency (CDF)
- plant modifications are not allowed to increase CDF and LERF
- CDF = 5,1E-5/a, power operation 2,3E-5/a
  - Internal events and internal and external hazards for power and non-power states and transfers between them
    - Fires and floods and seismic, severe weather and man-made external hazards

Initiator groups according to the automation needed or available

Initiator	Description	Available or needed automation
LLOCA	Large loss of coolant accident	RPS, ABU and MBU
MLOCA	Medium loss of coolant accident	RPS, ABU and MBU
SLOCA	Small loss of coolant accident	RPS, ABU and MBU
PRISE	Primary to Secondary leakages	PREV(TXS), RPS, ABU and MBU
VLOCA	Outside containment leakages	PREV(T2000), RPS, ABU and MBU
TRAN1	Transient 1 (PCP LOCA)	PREV(TXS), RPS, ABU and MBU
TRAN2	Transient 2 (PCP LOCA)	NPC/PREV(TXS), RPS, ABU and MBU
TRAN3	Transient 3 (Loss of FW)	RPS and recovery
TRAN4	Transient 4 (Loss of FW)	PREV(T2000), RPS and recovery
TRAN5	Transient 5 (No automation	-
LOOP	Loss of offsite power	RPS, ABU and MBU
TRIP	Reactor trip	RPS, ABU, MBU and Manual trip
PTS	Pressurized thermal shock (Spray)	Manual recovery (TXS)
REACT	Reactivity accident	PREV(TXS / T2000)

Single and common cause failure probabilities for new automation components

	Similar transmitt.	Diverse transmitt.	p/T transmitt.	Software	Hardware	DC power	AV42
A	5E-04	5E-04		1E-03	1E-03	1E-05	4,4E-04
B	5E-05	1E-05		5E-05	5E-05		
C				1E-06	1E-06		
D				1E-07	1E-07		
E				0	5E-07		
F	1E-05	5E-06	0			1E-08	1E-05

A Single failure
B CCF of single automation system (NPC, PREV, RPS, ABU or MBU)
C CCF of programmed systems with same platforms or softwares (T2000 or TXS)
D CCF of programmed systems with different platforms or softwares (T2000 and TXS)
E CCF of programmed and non-programmed systems (MBUTXS - TXS/T2000)
F Global CCF

Single failure events are excluded from the preliminary fault tree model because of their small risk importance.

Manual recovery failure probabilities

	LLOCA	MLOCA	SLOCA	PRISE	VLOCA	TRAN	Description
RT	0,1	1E-04	1E-04	1E-04	1E-04	1E-04	Manual reactor trip
LPI-accu	1	1					Manual opening of LPI-accumulator line valves
LPI	1	0,1					Manual start of low pressure injection
HPI		0,1	0,1				Manual start of high pressure injection
SPRAY	0,1	0,1					Manual start of containment spray
Sump	0,1	0,1	0,1				Manual control of sump line valves
Tank	1	1	1				Manual control of ECCS-tank line valves
VF	1	1	0,1				Manual control of Service water system
TF	1	1	0,1				Manual ctrl of component cooling water system
EY	1	1	0,1	1	1	1E-03	Manual start of diesel generators
RL-iso				1			Manual isolation of Main Feed Water
RA-iso				1			Manual isolation of main steam line
TC-iso					0,1		Manual isolation of purification line
MFW-iso						1E-03	Manual isolation of Main Feed Water
FW						1E-03	Manual start of feed water system
AEFW blind						1,4E-02	Manual blind start of Additional Emergency FW
AV42 bypass	1	0,1	0,1	0,1	0,1	0,1	Manual bypass of AV42 priority unit
YD-iso						1E-02	Manual isolation of PCP seal lines
TE-iso					0,1		Manual isolation of let down line

MBU recovery times and probabilities: <15 min 1, 15-30 min 0,1, >30 min 1E-2, >4 h 1E-3

Assumptions

AV42 priority module

- AV42 priority control module in every safety class 2 and 3 controls
- It is possible to by-pass AV42 failures in special cases
- Operator has no time to by-pass AV42 in case of LPI after LLOCA
- Operator has no time to by-pass AV42 in case of LOCA and ECCS-tank valve erroneous position
- Operator has no time to by-pass AV42 in case of LLOCA or MLOCA and TF- or VF-failures
- Unavailability of AV42 by-pass is included to MBU recovery

SG safety valves

- SG safety valve (RA) control is not dependent on TXS and AV42

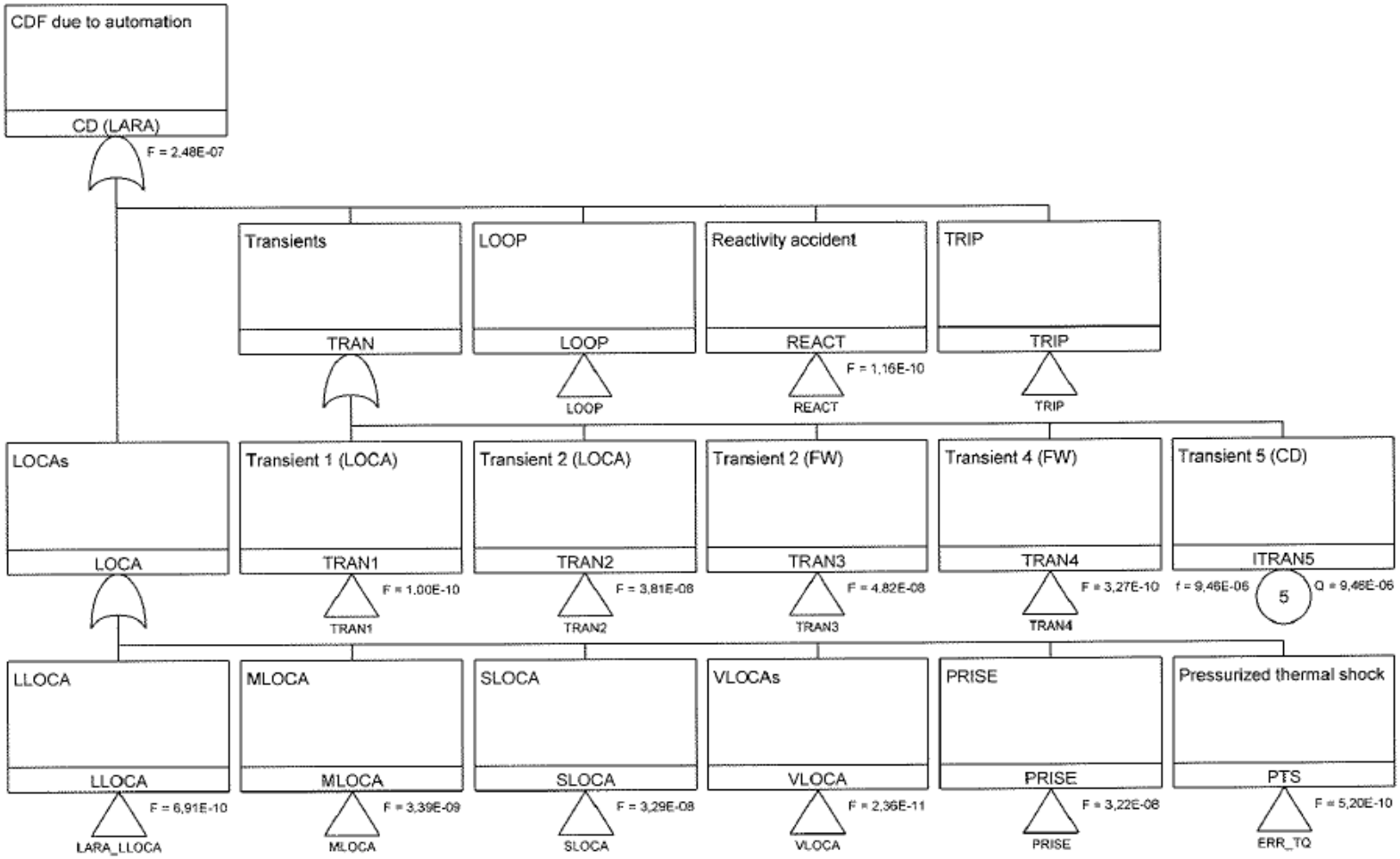
Pressirizer PORV and high capacity relief valves

- PORV and high capacity relief valves (YP12) controls are not dependent on TXS and AV42

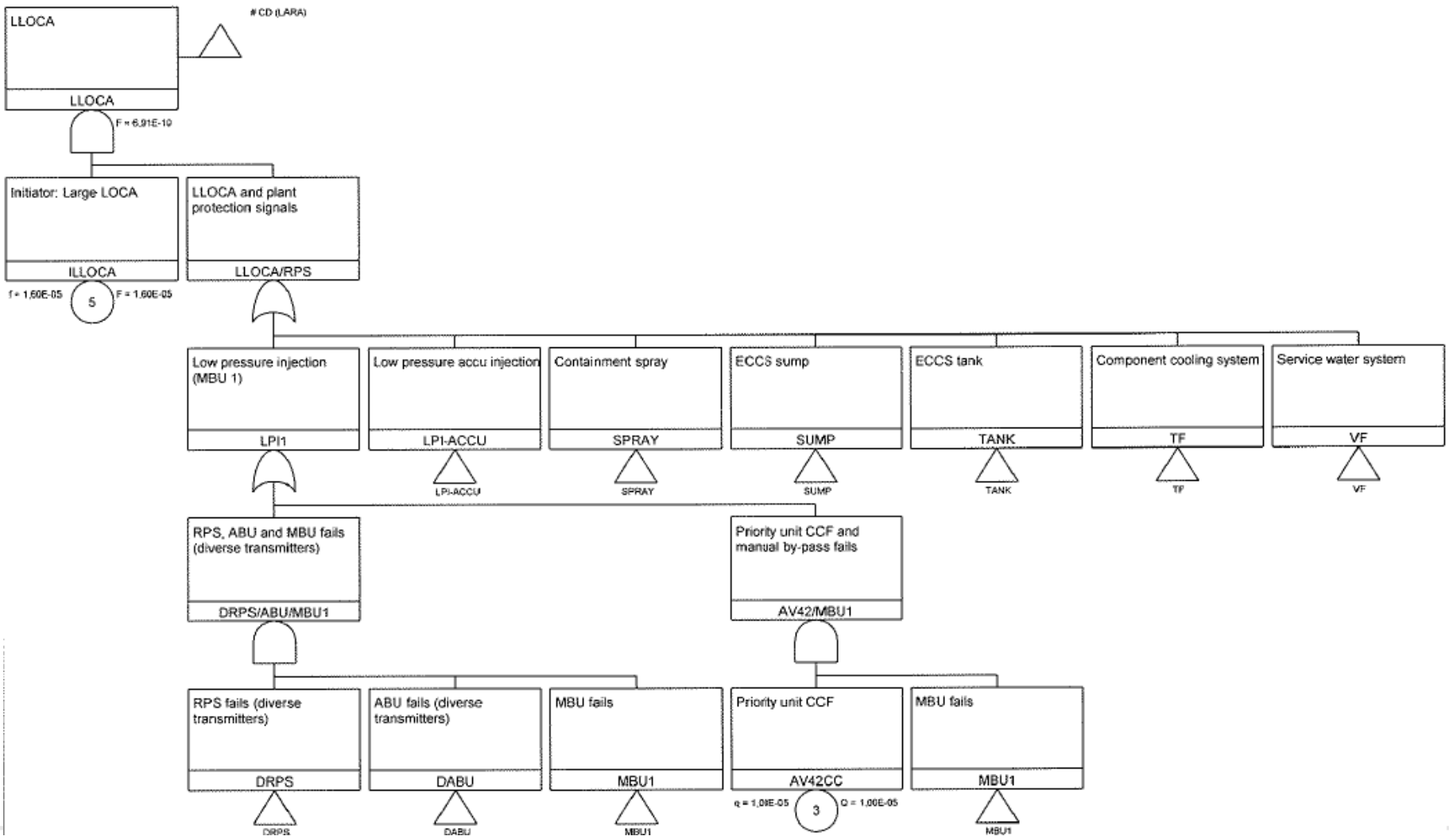
Manual Trip

- Manual Trip is not dependent on other automation systems

Fault tree

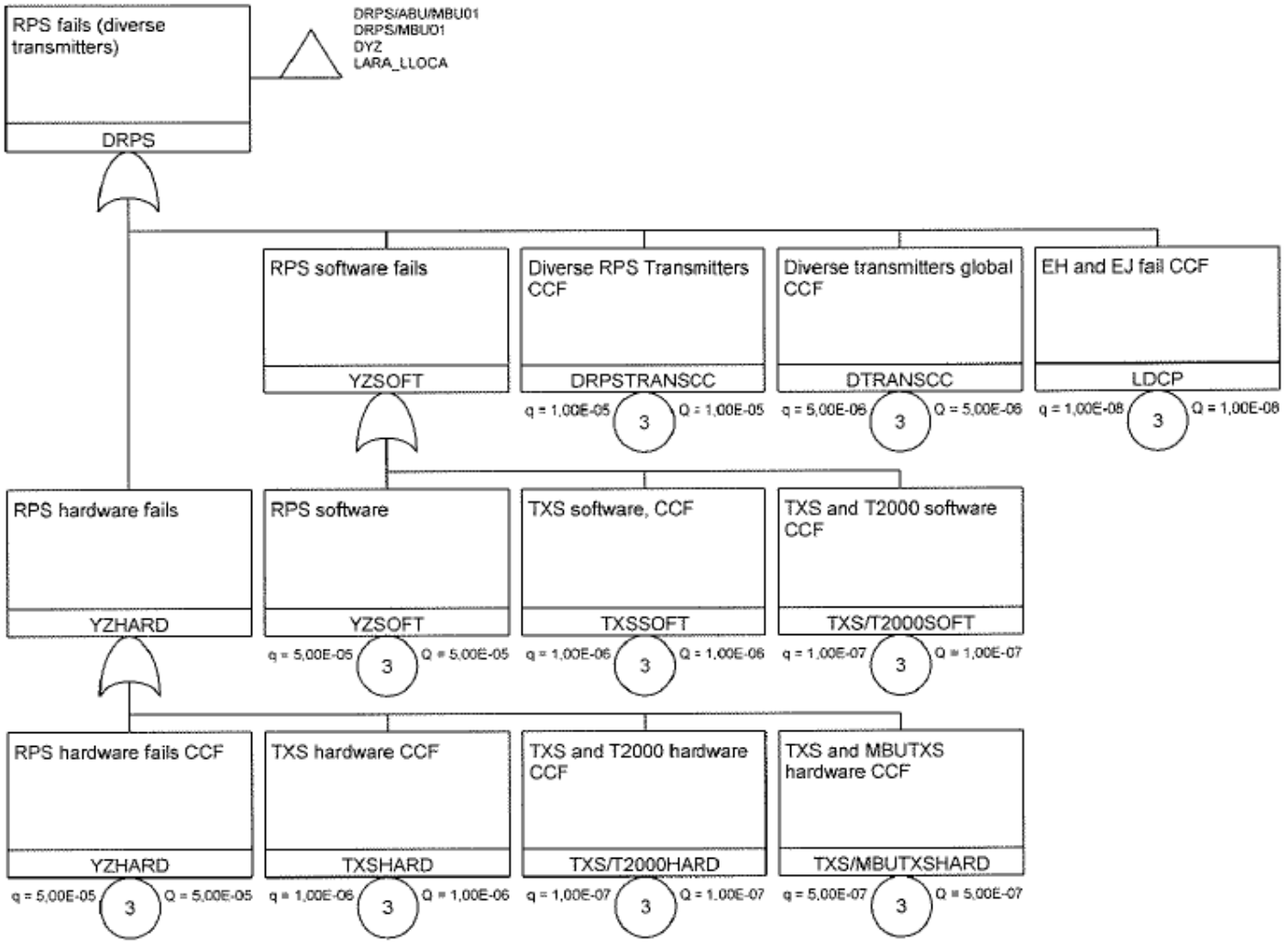

CDF due to automation
CD (LARA)
F = 2,48E-07
Transients
TRAN
LOOP
LOOP
Reactivity accident
REACT
F = 1,16E-10
TRIP
TRIP
LOCAs
LOCA
Transient 1 (LOCA)
TRAN1
F = 1,00E-10
Transient 2 (LOCA)
TRAN2
F = 3,81E-08
Transient 2 (FW)
TRAN3
F = 4,82E-08
Transient 4 (FW)
TRAN4
F = 3,27E-10
Transient 5 (CD)
ITRAN5
f = 9,46E-06
5
Q = 9,46E-06
LLOCA
LLOCA
F = 6,91E-10
LARA_LLOCA
MLOCA
MLOCA
F = 3,39E-09
MLOCA
SLOCA
SLOCA
F = 3,29E-08
SLOCA
VLOCAs
VLOCA
F = 2,36E-11
VLOCA
PRISE
PRISE
F = 3,22E-08
PRISE
Pressurized thermal shock
PTS
F = 5,20E-10
ERR_TQ

Fault tree

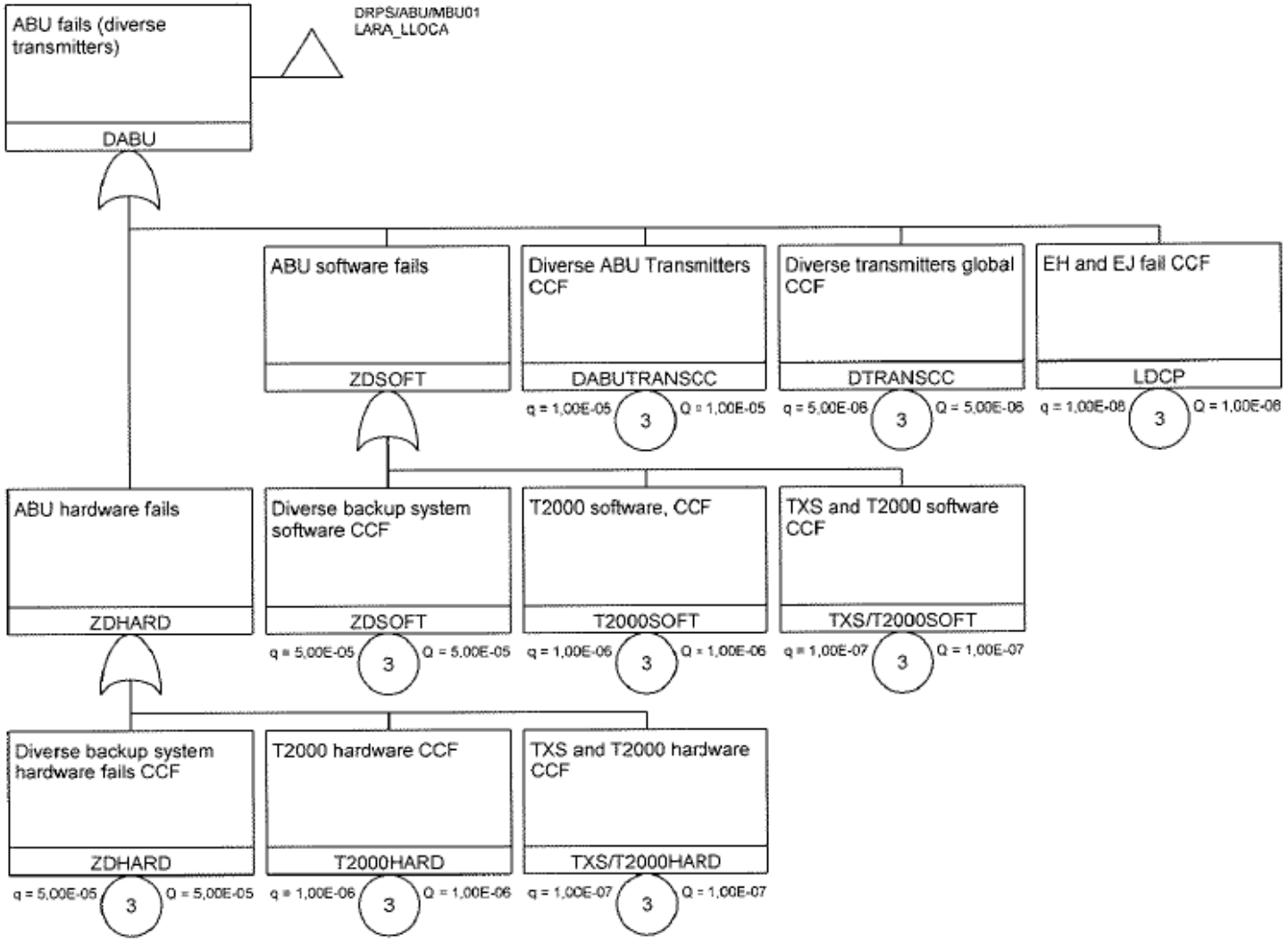


Fortum

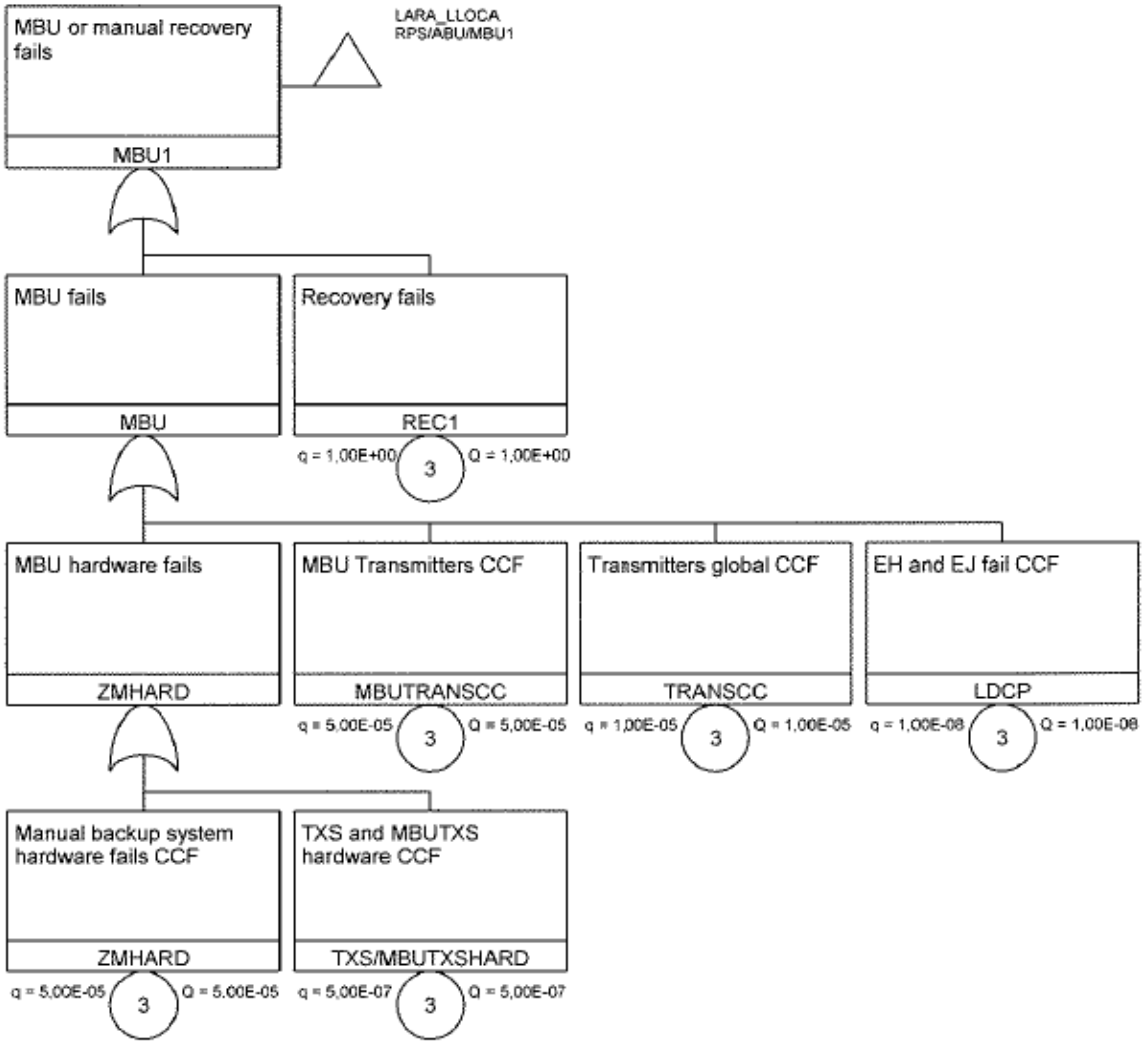
Fault tree


RPS fails (diverse transmitters)
DRPS
DRPS/ABU/MBU01
DRPS/MBU01
DYZ
LARA_LLOCA
RPS software fails
YZSOFT
Diverse RPS Transmitters CCF
DRPSTRANSCC
q = 1,00E-05
3
Q = 1,00E-05
Diverse transmitters global CCF
DTRANSCC
q = 5,00E-06
3
Q = 5,00E-06
EH and EJ fail CCF
LDCP
q = 1,00E-08
3
Q = 1,00E-08
RPS hardware fails
YZHARD
RPS software
YZSOFT
q = 5,00E-05
3
Q = 5,00E-05
TXS software, CCF
TXSSOFT
q = 1,00E-06
3
Q = 1,00E-06
TXS and T2000 software CCF
TXS/T2000SOFT
q = 1,00E-07
3
Q = 1,00E-07
RPS hardware fails CCF
YZHARD
q = 5,00E-05
3
Q = 5,00E-05
TXS hardware CCF
TXSHARD
q = 1,00E-06
3
Q = 1,00E-06
TXS and T2000 hardware CCF
TXS/T2000HARD
q = 1,00E-07
3
Q = 1,00E-07
TXS and MBUTXS hardware CCF
TXS/MBUTXSHARD
q = 5,00E-07
3
Q = 5,00E-07

Fault tree


ABU fails (diverse transmitters)
DABU
DRPS/ABU/MBU01
LARA_LLOCA
ABU software fails
ZDSOFT
Diverse ABU Transmitters CCF
DABUTRANSCC
q = 1,00E-05
3
Q = 1,00E-05
Diverse transmitters global CCF
DTRANSCC
q = 5,00E-06
3
Q = 5,00E-06
EH and EJ fail CCF
LDCP
q = 1,00E-08
3
Q = 1,00E-08
ABU hardware fails
ZDHARD
Diverse backup system software CCF
ZDSOFT
q = 5,00E-05
3
Q = 5,00E-05
T2000 software, CCF
T2000SOFT
q = 1,00E-06
3
Q = 1,00E-06
TXS and T2000 software CCF
TXS/T2000SOFT
q = 1,00E-07
3
Q = 1,00E-07
Diverse backup system hardware fails CCF
ZDHARD
q = 5,00E-05
3
Q = 5,00E-05
T2000 hardware CCF
T2000HARD
q = 1,00E-06
3
Q = 1,00E-06
TXS and T2000 hardware CCF
TXS/T2000HARD
q = 1,00E-07
3
Q = 1,00E-07

Fault tree


MBU or manual recovery fails
LARA_LLOCA
RPS/ABU/MBU1
MBU1
MBU fails
MBU
Recovery fails
REC1
q = 1,00E+00
3
Q = 1,00E+00
MBU hardware fails
ZMHARD
MBU Transmitters CCF
MBUTRANSCC
q = 5,00E-05
3
Q = 5,00E-05
Transmitters global CCF
TRANSCC
q = 1,00E-05
3
Q = 1,00E-05
EH and EJ fail CCF
LDCP
q = 1,00E-08
3
Q = 1,00E-08
Manual backup system hardware fails CCF
ZMHARD
q = 5,00E-05
3
Q = 5,00E-05
TXS and MBUTXS hardware CCF
TXS/MBUTXSHARD
q = 5,00E-07
3
Q = 5,00E-07

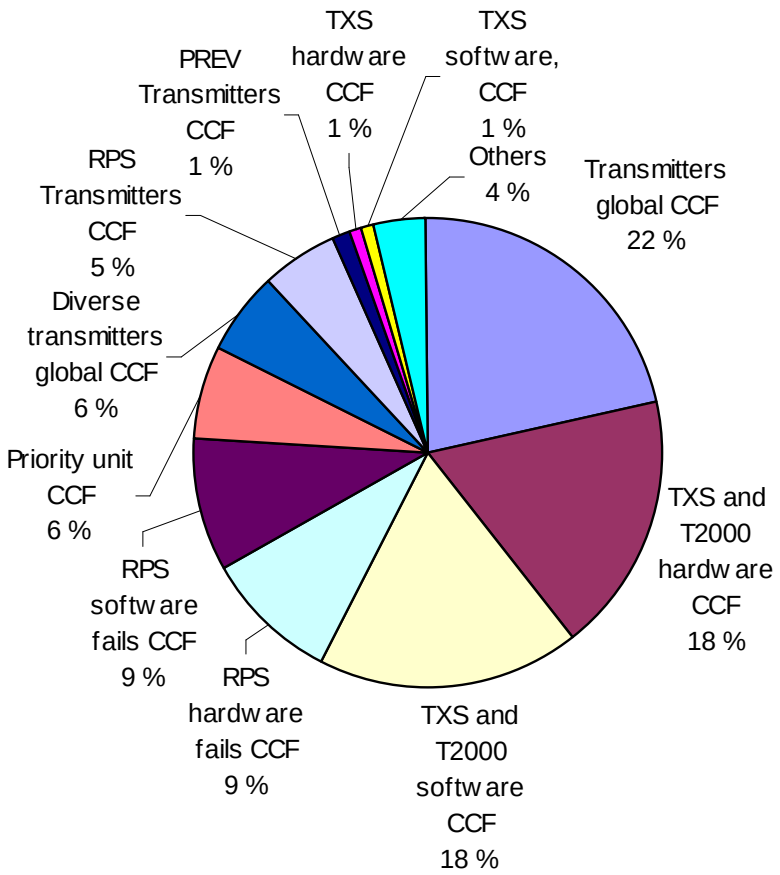
LLOCA and available RPS, ABU and MBU signals

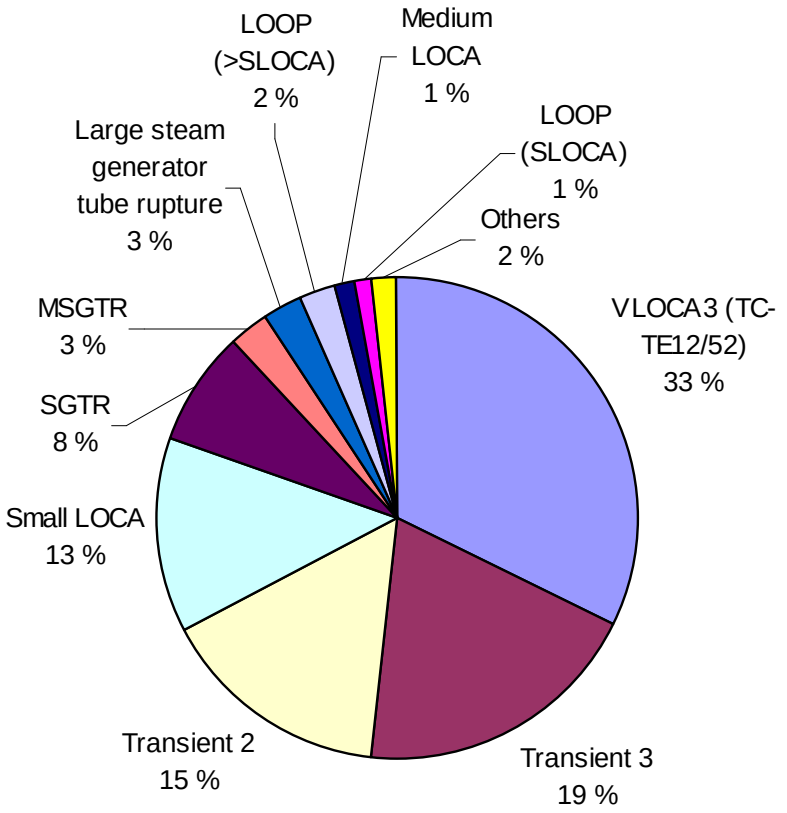
LLOCA x RPS x ABU x MBU Initiators	**IE**						**Cond. prob.**	**CD**	%	**Comment**
ALOCA	1,0E-06						3,1E-02	3,1E-08	15,7	
LLOCA	1,5E-05						1,1E-02	1,7E-07	84,3	
Total	**1,6E-05**						**1,2E-02**	**2,0E-07**	**100,0**	
Automation signals	**LLOCA Freq.**	**PREV**	**State of ECCS**	**RPS**	**ABU**	**MBU**	**Cond. prob.**	**CD**	%	**Comment**
LPI	1,6E-05	x	1	YZ26/27	ZD26/27	ZM26/27	1,5E-05	2,4E-10		
LPI-accu	1,6E-05	x	1E-03	YZ26	x	x	1,3E-07	2,0E-12		NPC: MOV´s basic states are open
Spray	1,6E-05	x	1	YZ21/22	x	ZM21/22	3,6E-05	5,7E-10		
Sump flow	1,6E-05	x	1	YZ41	x	ZM41	1,8E-05	2,8E-10		
Tank flow	1,6E-05	x	1E-02	YZ42	x	x	1,3E-06	2,0E-11		MOV´s basic states are open
TF	1,6E-05	x	1	YZ32	ZD32	ZM32	1,5E-05	2,4E-10		
VF	1,6E-05	x	1	YZ32	x	ZM32	2,7E-05	4,3E-10		
Total	**1,6E-05**						**4,3E-05**	**6,9E-10**	**0,3**	**Minimum cutset result**

The most important minimal cut sets

	CDF	%	Σ%		Events	Description
1	2,5E-08	10,2 %	10,2 %	2,5	IVLOCA3	Initiator: VLOCA3 (TC-TE12/52)
				0,1	REC01	Recovery fails
				1,0E-07	TXS/T2000SOFT	TXS and T2000 software CCF
2	2,5E-08	10,2 %	20,4 %	2,5	IVLOCA3	Initiator: VLOCA3 (TC-TE12/52)
				1,0E-07	TXS/T2000HARD	TXS and T2000 hardware CCF
				0,1	REC01	Recovery fails
3	2,5E-08	10,2 %	30,6 %	2,5	IVLOCA3	Initiator: VLOCA3 (TC-TE12/52)
				1,0E-08	LDCP	Loss of DC power
4	2,2E-08	8,7 %	39,3 %	1,5E-01	ITRANC	Initiator: Transient 3
				1,0E-05	TRANSCC	Transmitters global CCF
				1,4E-02	RECAEFW2	AEFW blind recovery
5	1,4E-08	5,6 %	44,9 %	1,4E-03	ISGTR	Initiator: SGTR
				1,0E-05	TRANSCC	Transmitters global CCF
6	1,2E-08	4,7 %	49,6 %	1,2E+00	ITRANB	Initiator: Transient 2
				1,0E-07	TXS/T2000HARD	TXS and T2000 hardware CCF
				0,1	REC01	Recovery fails
7	1,2E-08	4,7 %	54,3 %	1,2E+00	ITRANB	Initiator: Transient 2
				1,0E-07	TXS/T2000SOFT	TXS and T2000 software CCF
				0,1	REC01	Recovery fails
8	1,2E-08	4,7 %	59,0 %	1,2E+00	ITRANB	Initiator: Transient 2
				1,0E-08	LDCP	Loss of DC power
9	1,2E-08	4,6 %	63,6 %	2,3E-03	ISLOCA	Initiator: Small LOCA
				5,0E-06	DTRANSCC	Diverse transmitters global CCF
10	7,7E-09	3,1 %	66,7 %	1,5E-01	ITRANC	Initiator: Transient 3
				5,0E-05	RPSTRANSCC	RPS Transmitters CCF
				1,0E-03	RECAEFW	AEFW recovery

Importance for Initiators and Automation components





Importance for Initiators and Automation components

ID	Description	Nom.val.	FV	FC	Sens.	Sens.
IVLOCA3	Initiator: VLOCA3 (TC-TE12/52)	2,5E+00	3,2E-01	3,2E-01	5,5E+00	
ITRANC	Initiator: Transient 3	1,5E-01	1,9E-01	1,9E-01	3,3E+00	
ITRANB	Initiator: Transient 2	1,2E+00	1,5E-01	1,5E-01	2,8E+00	
ISLOCA	Initiator: Small LOCA	2,3E-03	1,3E-01	1,3E-01	2,5E+00	
ISGTR	Initiator: SGTR	1,4E-03	7,8E-02	7,8E-02	1,8E+00	
IMSGTR	Initiator: MSGTR	7,0E-05	2,7E-02	2,7E-02	1,3E+00	
ILSGTR	Initiator: Large PRISE	3,5E-05	2,5E-02	2,5E-02	1,3E+00	
ILOOP1	Initiator: LOOP (>SLOCA)	2,9E-04	2,4E-02	2,4E-02	1,2E+00	
TRANSCC	Transmitters global CCF	1,0E-05	1,9E-01	1,2E+00	1,9E+04	3,3E+00
TXS/T2000HARD	TXS and T2000 hardware CCF	1,0E-07	1,6E-01	1,2E+00	1,4E+06	2,8E+00
TXS/T2000SOFT	TXS and T2000 software CCF	1,0E-07	1,6E-01	1,2E+00	1,4E+06	2,8E+00
YZHARD	RPS hardware fails CCF	5,0E-05	8,1E-02	1,1E+00	1,6E+03	1,9E+00
YZSOFT	RPS software fails CCF	5,0E-05	8,1E-02	1,1E+00	1,6E+03	1,9E+00
AV42CC	Priority unit CCF	1,0E-05	5,5E-02	1,1E+00	5,5E+03	1,6E+00
DTRANSCC	Diverse transmitters global CCF	5,0E-06	5,1E-02	1,1E+00	1,0E+04	1,5E+00
RPSTRANSCC	RPS Transmitters CCF	5,0E-05	4,8E-02	1,1E+00	9,5E+02	1,5E+00
PREVTRANSCC	PREV Transmitters CCF	5,0E-05	1,1E-02	1,0E+00	2,2E+02	1,1E+00
TXSHARD	TXS hardware CCF	1,0E-06	7,5E-03	1,0E+00	7,5E+03	1,1E+00
TXSSOFT	TXS software, CCF	1,0E-06	7,5E-03	1,0E+00	7,5E+03	1,1E+00
DRPSTRANSCC	Diverse RPS Transmitters CCF	1,0E-05	7,1E-03	1,0E+00	7,2E+02	1,1E+00
TXS/MBUTXSHARD	TXS and MBUTXS hardware CCF	5,0E-07	6,7E-03	1,0E+00	1,3E+04	1,1E+00
PREVHARD(T2000)	T2000 hardware fails CCF	5,0E-05	6,3E-03	1,0E+00	1,3E+02	1,1E+00
PREVSOFT(T2000)	PREV(T2000) software	5,0E-05	6,3E-03	1,0E+00	1,3E+02	1,1E+00

Importance for other basic events

ID	Description	Nom.val.	FV	RDF	RIF	Sens.
REC01	Recovery fails	1,0E-01	4,0E-01	1,7E+00	4,6E+00	7,1E+00
LDCP	Loss of DC power	1,0E-08	1,5E-01	1,2E+00	3,1E+06	2,7E+00
RECAEFW	AEFW recovery	1,0E-03	1,1E-01	1,1E+00	1,1E+02	2,2E+00
RECAEFW2	AEFW blind recovery	1,4E-02	8,9E-02	1,1E+00	7,2E+00	2,0E+00
COND05	Need for sump flow	5,0E-01	5,6E-02	1,1E+00	1,1E+00	1,1E+00
MAINVALVES	Main gate valves fails to close	5,0E-01	2,3E-02	1,0E+00	1,0E+00	1,0E+00
COND001	TH-tank valve position	1,0E-02	2,2E-02	1,0E+00	3,1E+00	1,2E+00
COND01	VF/TF are running	1,0E-01	1,1E-02	1,0E+00	1,1E+00	1,1E+00
MANTRIP	Manual trip	1,0E-04	1,8E-03	1,0E+00	1,9E+01	1,0E+00
CTWC782E	Conditional TWC probability	3,4E-04	1,6E-03	1,0E+00	5,6E+00	1,0E+00
REC00001	Test team and operator fails with TQ-test	1,0E-04	5,8E-04	1,0E+00	6,8E+00	1,0E+00
CTWC781E	Conditional TWC probability	6,5E-04	5,3E-04	1,0E+00	1,8E+00	1,0E+00
REC1	Recovery fails	1,0E+00	3,0E-04	1,0E+00	1,0E+00	1,0E+00
COND0001	TH-accu valve position	1,0E-03	4,3E-05	1,0E+00	1,0E+00	1,0E+00
REC0001	Recovery fails	1,0E-03	1,4E-06	1,0E+00	1,0E+00	1,0E+00
MANTRIPB	Manual trip (LLOCA)	1,0E-01	8,2E-08	1,0E+00	1,0E+00	1,0E+00

Concluding remarks

- With digital automation it is important to have diversity between redundant safety systems that perform safety functions of different task categories.
  - this is accomplished by applying different I&C system platforms that have different system software, libraries of the application software and main hardware modules
  - different platforms are used for systems of different safety classes
  - a back-up safety system has to be in another safety class so that it is designed on another platform, to avoid common cause failures and common software errors