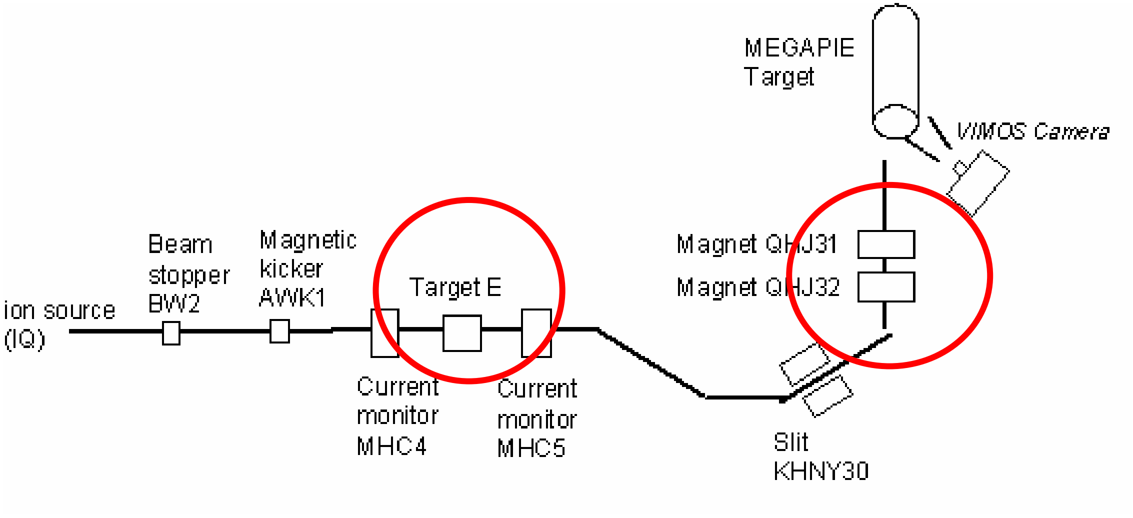
SAFETY EVALUATION OF THE MEGAPIE EXPERIMENTAL FACILITY: RESULTS AND INSIGHTS FROM THE APPLICATION OF PROBABILISTIC SAFETY ASSESSMENT

Luca Podofillini, Vinh N. Dang

Risk and Human Reliability Group
Paul Scherrer Institute, Villigen PSI, Switzerland

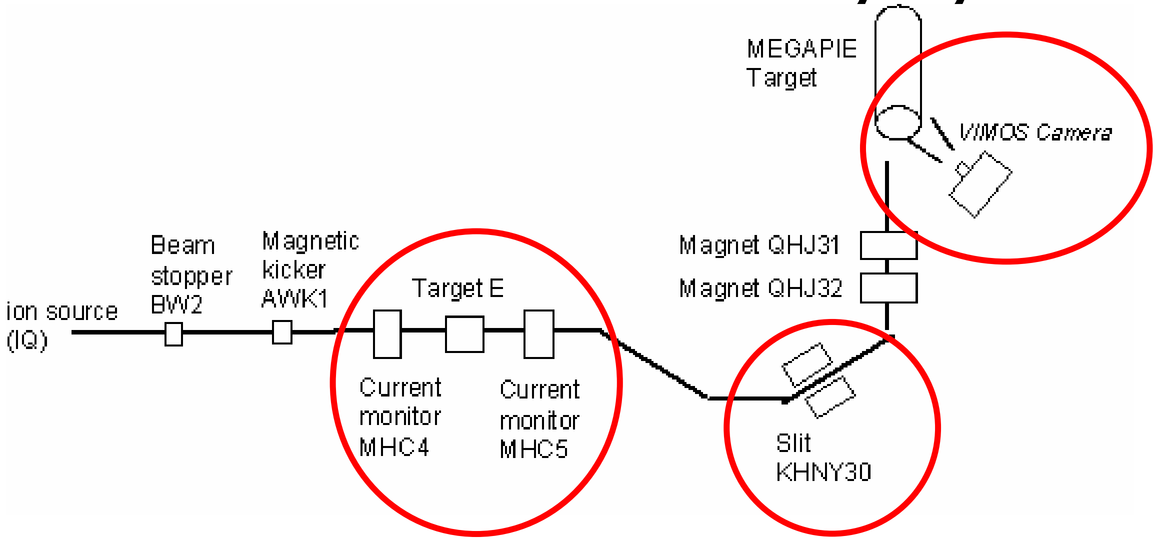
May 7, 2007

Issues for MEGAPIE safety



- **Over-Focused beam →** excessive intensity onto the target → breach of the LMC [MEGAPIE safety report; Smith, 2006]
- "Critical" components to avoid over-focusing are:
  - Scattering **Target E** - diffuses beam intensity distribution
  - Quadrupoles QJ31-QJ32 - located downstream of two out of three safety systems

MEGAPIE safety systems



- MHC4/5 – monitors transmission across scattering Target E
- KHNY30 –limits allowed spread of the trajectory → Detects if protons are correctly scattered by Target E
- VIMOS – visually monitors beam intensity distribution

Beam shutdown if
parameters are outside
allowed range

!!! There are additional safety barriers, e.g. components settings supervisions, that were outside the scope or this analysis

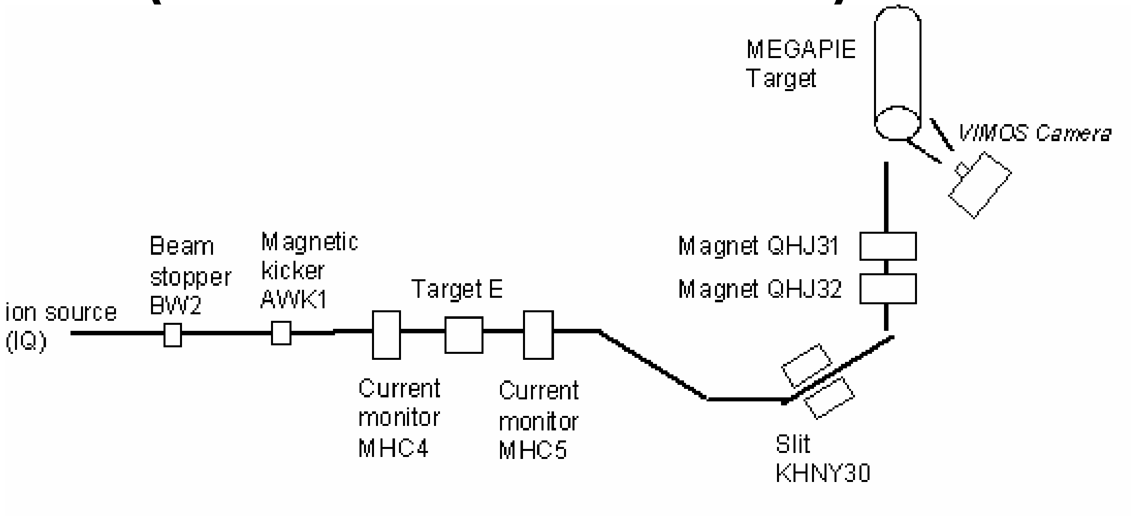
Goals of this study

- Evaluate **redundancy and diversity** of the MEGAPIE safety system
- Suggest possible **safety-enhancing improvements**

⇩ The tool

- Probabilistic safety assessment (PSA): methods to **analyze** systems, **model** scenarios and failures, **calculate** risk and its contributors
  - “event trees and fault trees”

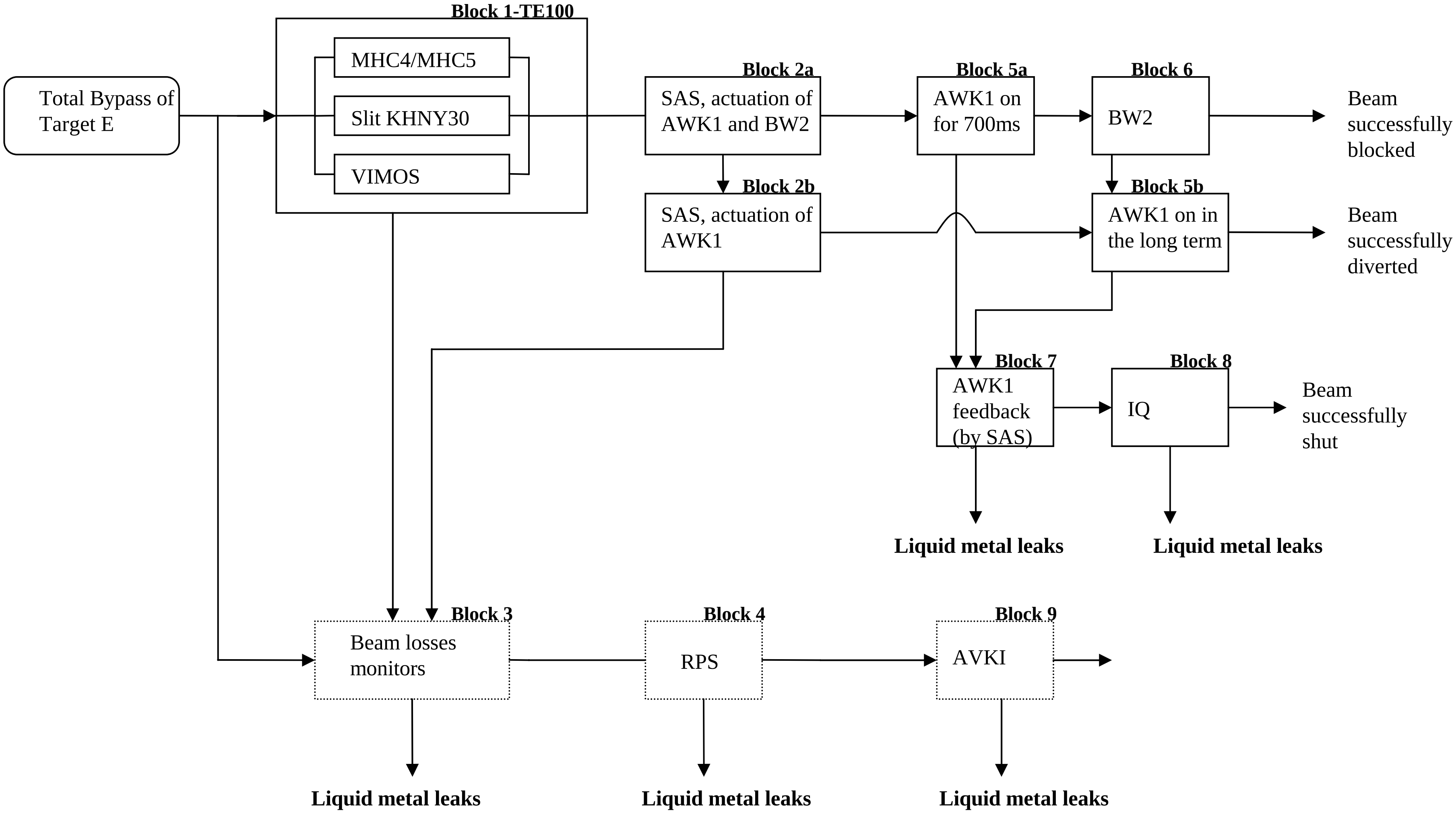
Initiating events (How accidents start)



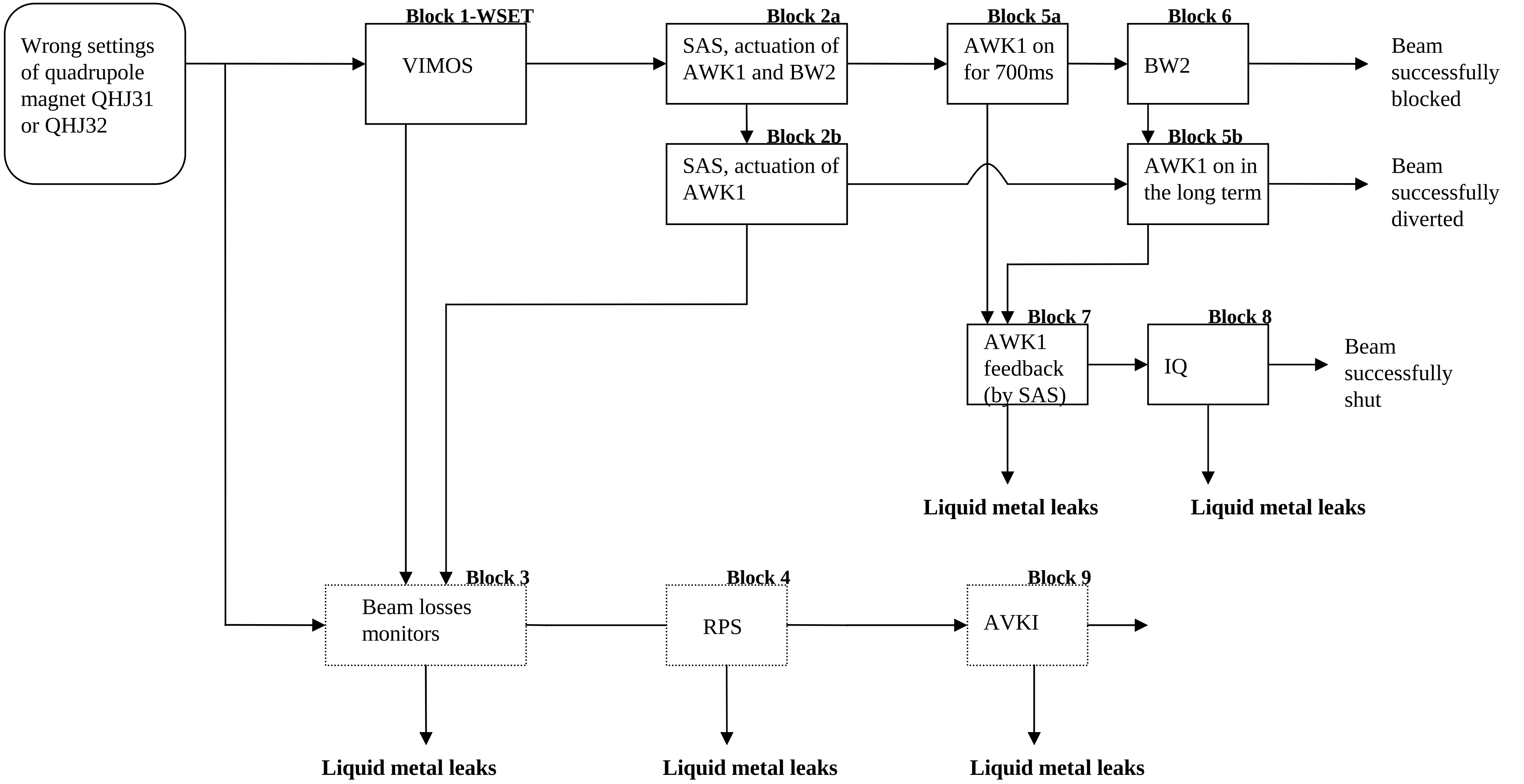
- Three events potentially initiating an accident of excessive beam over-focus:
  - TE-BY - total bypass of Target E by protons beam
  - WSET1 - Wrong settings of QHJ31 or QHJ32. Wrong settings loaded into the components control devices
  - WSET2 - Wrong settings of QHJ31 or QHJ32. Magnets failure to set or of control devices to command current

Model of scenario TE-BY

Event sequence diagrams: required functions and systems

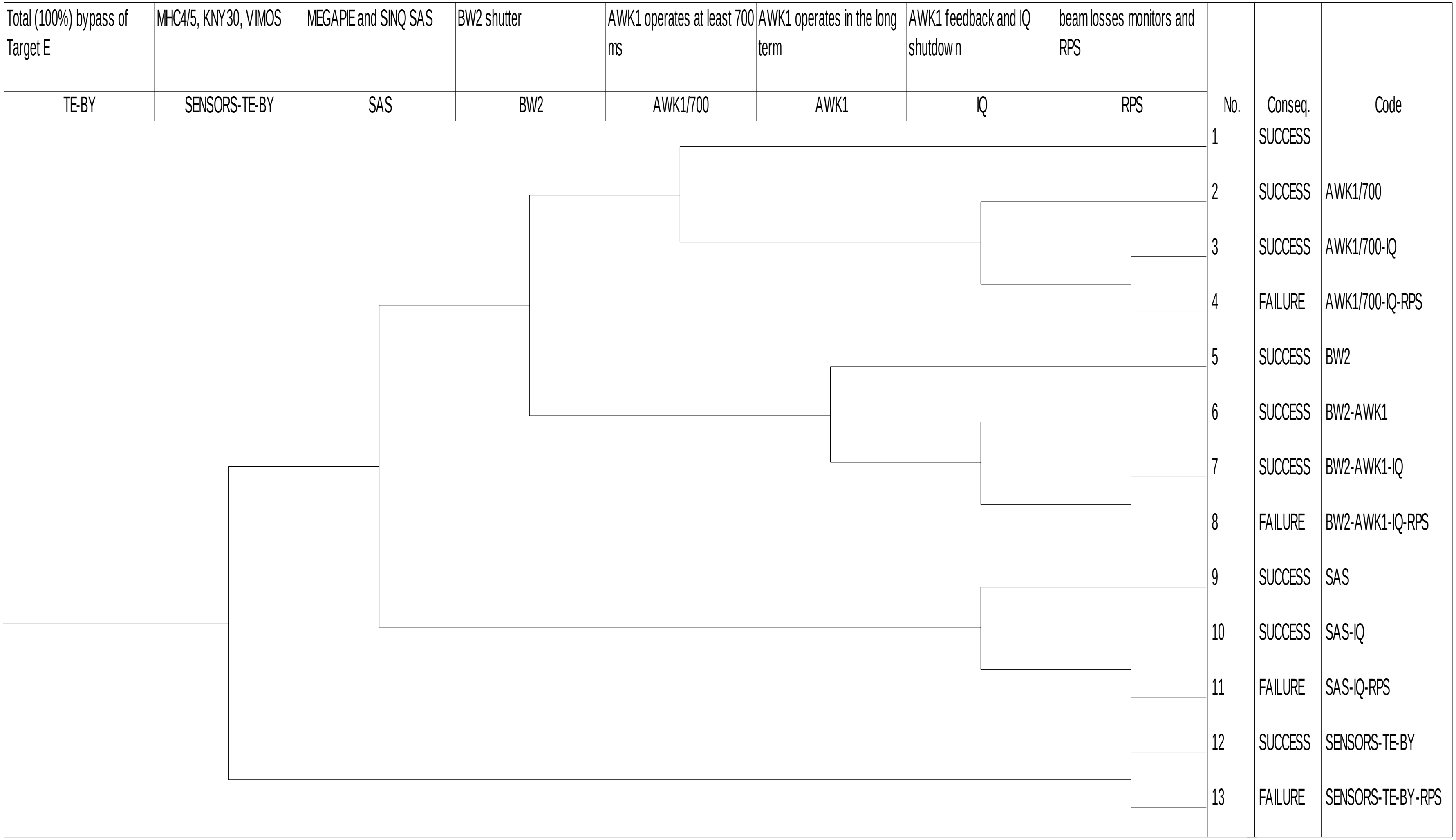


Model of scenario WSET1



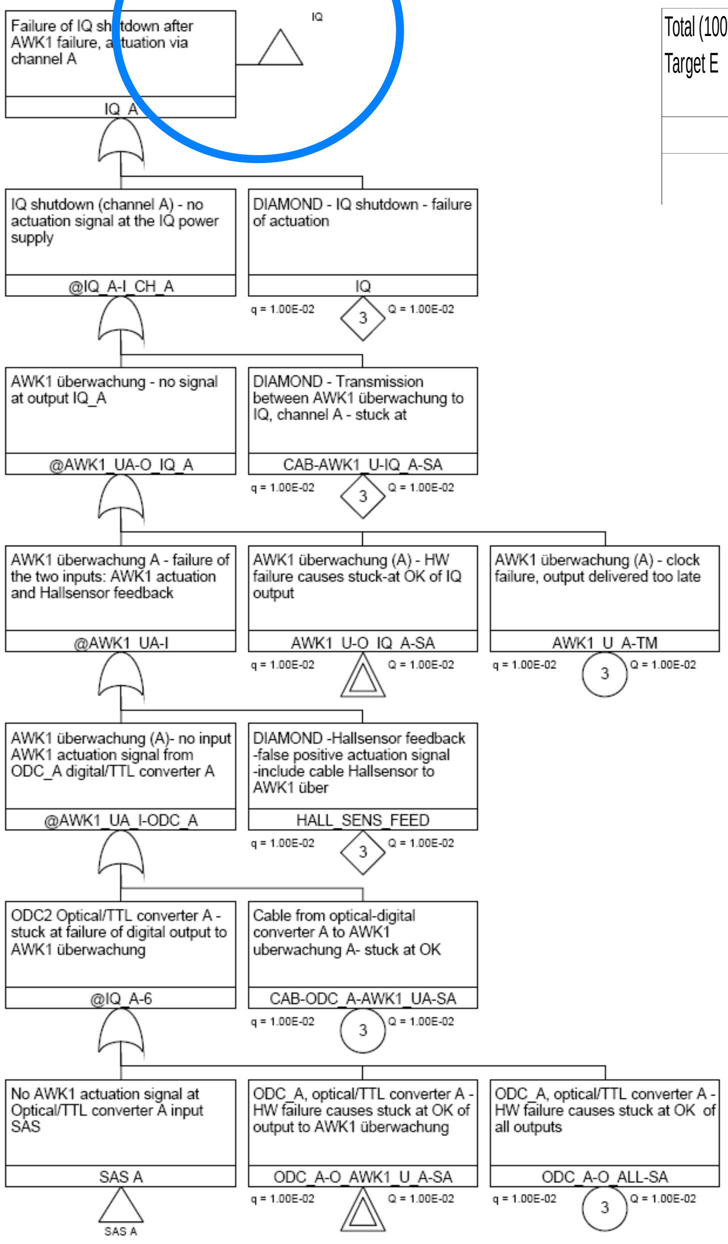
Model of scenario TE-BY

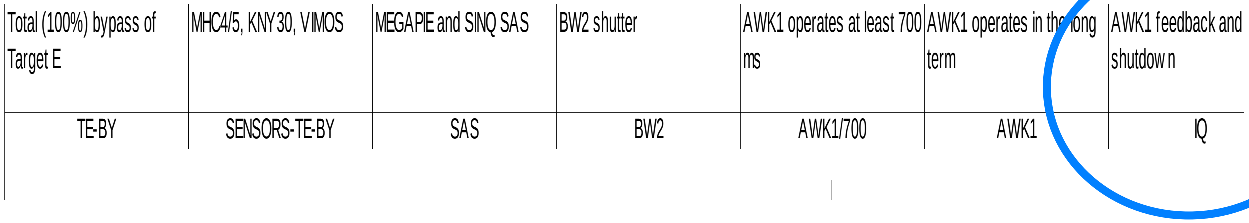
Event Trees: sequence of functions and systems



Total (100%) bypass of Target E	MHC4/5, KNY30, VIMOS	MEGAPIE and SINQ SAS	BW2 shutter	AWK1 operates at least 700 ms	AWK1 operates in the long term	AWK1 feedback and IQ shutdown	beam losses monitors and RPS
TE-BY	SENSORS-TE-BY	SAS	BW2	AWK1/700	AWK1	IQ	RPS

No.	Conseq.	Code
1	SUCCESS	
2	SUCCESS	AWK1/700
3	SUCCESS	AWK1/700-IQ
4	FAILURE	AWK1/700-IQ-RPS
5	SUCCESS	BW2
6	SUCCESS	BW2-AWK1
7	SUCCESS	BW2-AWK1-IQ
8	FAILURE	BW2-AWK1-IQ-RPS
9	SUCCESS	SAS
10	SUCCESS	SAS-IQ
11	FAILURE	SAS-IQ-RPS
12	SUCCESS	SENSORS-TE-BY
13	FAILURE	SENSORS-TE-BY-RPS


Failure of IQ shutdown after AWK1 failure, actuation via channel A
IQ_A
IQ
IQ shutdown (channel A) - no actuation signal at the IQ power supply
@IQ_A-I_CH_A
DIAMOND - IQ shutdown - failure of actuation
IQ
q = 1.00E-02
3
Q = 1.00E-02
AWK1 überwachung - no signal at output IQ_A
@AWK1_UA-O_IQ_A
DIAMOND - Transmission between AWK1 überwachung to IQ, channel A - stuck at
CAB-AWK1_U-IQ_A-SA
q = 1.00E-02
3
Q = 1.00E-02
AWK1 überwachung A - failure of the two inputs: AWK1 actuation and Hallsensor feedback
@AWK1_UA-I
AWK1 überwachung (A) - HW failure causes stuck-at OK of IQ output
AWK1_U-O_IQ_A-SA
q = 1.00E-02
Q = 1.00E-02
AWK1 überwachung (A) - clock failure, output delivered too late
AWK1_U_A-TM
q = 1.00E-02
3
Q = 1.00E-02
AWK1 überwachung (A)- no input AWK1 actuation signal from ODC_A digital/TTL converter A
@AWK1_UA_I-ODC_A
DIAMOND -Hallsensor feedback -false positive actuation signal -include cable Hallsensor to AWK1 über
HALL_SENS_FEED
q = 1.00E-02
3
Q = 1.00E-02
ODC2 Optical/TTL converter A - stuck at failure of digital output to AWK1 überwachung
@IQ_A-6
Cable from optical-digital converter A to AWK1 uberwachung A- stuck at OK
CAB-ODC_A-AWK1_UA-SA
q = 1.00E-02
3
Q = 1.00E-02
No AWK1 actuation signal at Optical/TTL converter A input SAS
SAS A
SAS A
ODC_A, optical/TTL converter A - HW failure causes stuck at OK of output to AWK1 überwachung
ODC_A-O_AWK1_U_A-SA
q = 1.00E-02
Q = 1.00E-02
ODC_A, optical/TTL converter A - HW failure causes stuck at OK of all outputs
ODC_A-O_ALL-SA
q = 1.00E-02
3
Q = 1.00E-02



Total (100%) bypass of Target E	MHC4/5, KNY30, VIMOS	MEGAPIE and SINQ SAS	BW2 shutter	AWK1 operates at least 700 ms	AWK1 operates in the long term	AWK1 feedback and shutdown
TE-BY	SENSORS-TE-BY	SAS	BW2	AWK1/700	AWK1	IQ

Fault trees

- **Systematic analysis** of the possible causes of functional failures
- **Functional** failures are systematically traced back to **basic events** failures (ANDs/ORs)
- Basic events: **basic components failure modes** (cables, electronic devices, power supplies, software)

Application of PSA to experimental facilities: challenges

- Use of **digital and software** systems
  - Difficult to **predict** and **quantify** failure modes
  - Timing failures may be difficult to incorporate in fault trees
- Use of one-of-a-kind components
  - **Lack of data** to quantify probabilities of basic events

↓

- Emphasis on **qualitative results** from the PSA
- No attempt to quantify failure events probabilities

What may qualitative results give?

- The PSA model (ETs and FTs) is processed by software (Risk Spectrum®)
- Minimal Cut sets: **sequences of failure events** that may lead to system failure given occurrence of the scenario

It is possible to:

- Identify **single, double, triple, points of failure** …
- Evaluate adequacy of safety systems (**redundancy and diversity**)
- (Independently on the probability of the sequences)

Results for scenario TE-BY

- 6 first-order cutsets (**common cause failures** – i.e. failures of multiple components at the same time)
- **No single point of failure** → MCH4/5, KHNY30, VIMOS constitute a **diverse protection** against scenarios originated by bypass of Target E (TE-BY)

#	**Event**	**Description**
1	OPT_PAN1-O_ALL-SA	Optical lead panel 1 - common cause stuck at failure of all outputs, due to loss of isolation
2	OPT_PAN2-O_ALL-SA	Optical lead panel 2 - common cause stuck at failure of all outputs, due to loss of isolation
3	S_SAS_A_B-CCF-ALL	SINQ SAS A and B - Common cause stuck at OK
4	M_SAS_A_B-CCF-ALL	MEGAPIE SAS A and B - Common cause stuck at OK
5	DOC_A_B-CCF-ALL	DOC, TTL/optical converters A and B - Common cause stuck at OK
6	ODC_A_B-CCF-ALL	ODC, optical/TTL converters A and B - Common cause stuck at OK

Results for scenario WSET1

- 16 first-order cutsets (10 related to failures of the VIMOS system)
- **Relevant safety contribution of** VIMOS: it is the only monitoring system able to catch WSET1
- VIMOS is devised with **multiple protections** against several failure modes
- Two Failure events identify scenarios where VIMOS would continue to evaluate the same frame, not recognizing a disturbance in the beam intensity distribution:

Event identifier	**Description**
VIMOSSW-SA	VIMOS SW - stuck at while executing due to programming error or operating system failure
FRAMEGRR-BUFFER-SA	Frame Grabber - memory buffer stuck-at due to buffer failure or software failure to save new picture

Specific safety-enhancing recommendations

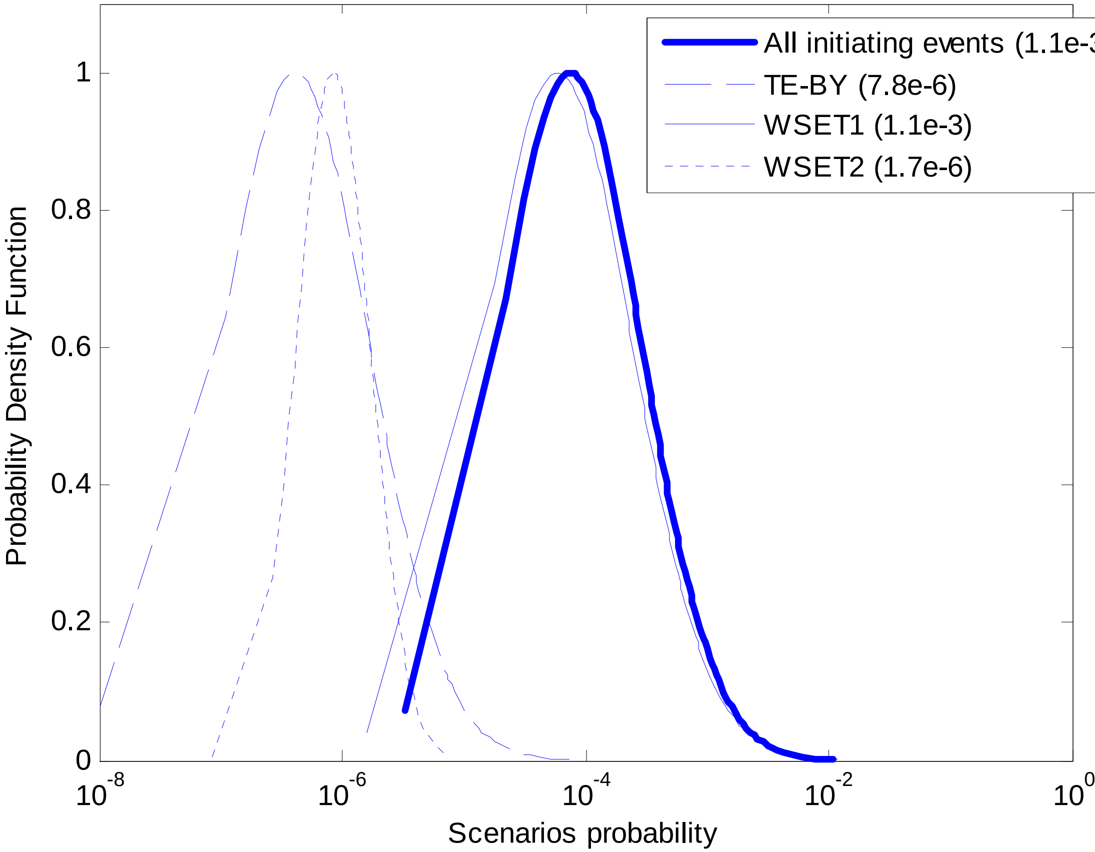
Recommendations

- Two (additional) recommendations to make sure VIMOS is actively processing valid pictures:
  - Implement an automatic check (e.g. control on signal variance)
  - Formalize daily routine checks in the control room

Yet, quantification has benefits (in conference Paper)

PSA handles uncertainties !!

- Prioritize scenarios, components, failure modes based on their impact on risk
- Prioritize recommendations based on their potential for risk-reduction



Conclusions

- PSA can provide safety insights and identify measures for informing designers of the safety of experimental installations
- Lack of data is certainly a challenge but should not discourage (PSA treats uncertainties)
- Prioritize the identification of weaknesses, rather than the value of the risk

Shifts the focus

from probabilities

to understanding risk

Conclusions

- PSA can provide safety insights and identify measures for informing designers of the safety of experimental installations
- Lack of data is certainly a challenge but should not discourage (PSA treats uncertainties)
- Prioritize the identification of weaknesses, rather than the value of the risk

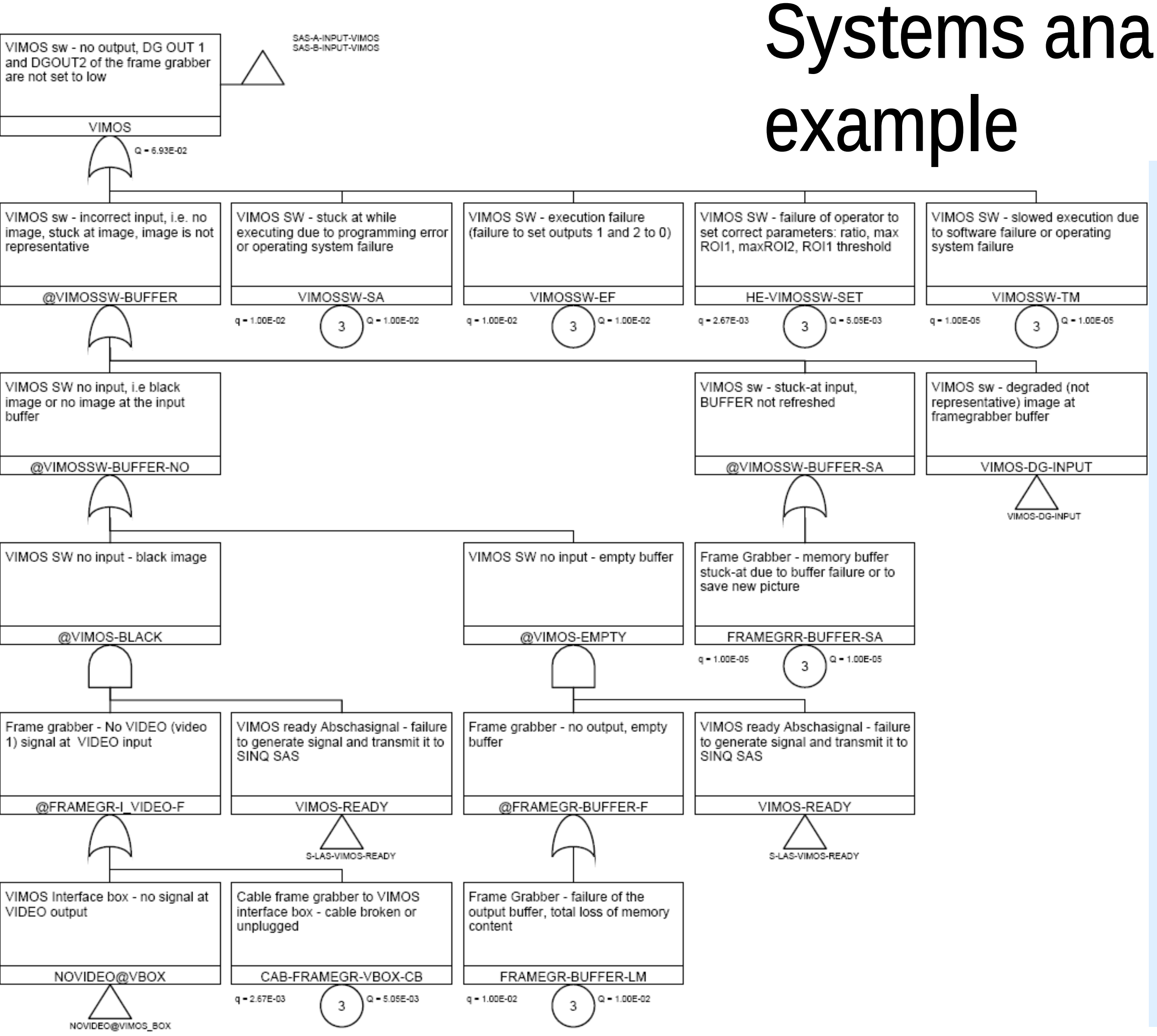
Shifts the focus

from probabilities

to understanding risk

Job openings in our group at PSI! Go to http://safe.web.psi.ch/

Systems analysis – Fault trees, example



VIMOS sw - no output, DG OUT 1 and DGOUT2 of the frame grabber are not set to low
VIMOS

VIMOS sw - incorrect input, i.e. no image, stuck at image, image is not representative
@VIMOSSW-BUFFER

VIMOS SW - stuck at while executing due to programming error or operating system failure
VIMOSSW-SA

VIMOS SW - execution failure (failure to set outputs 1 and 2 to 0)
VIMOSSW-EF

VIMOS SW - failure of operator to set correct parameters: ratio, max ROI1, maxROI2, ROI1 threshold
HE-VIMOSSW-SET

VIMOS SW - slowed execution due to software failure or operating system failure
VIMOSSW-TM

VIMOS SW no input, i.e black image or no image at the input buffer
@VIMOSSW-BUFFER-NO

VIMOS sw - stuck-at input, BUFFER not refreshed
@VIMOSSW-BUFFER-SA

VIMOS sw - degraded (not representative) image at framegrabber buffer
VIMOS-DG-INPUT

VIMOS SW no input - black image
@VIMOS-BLACK

VIMOS SW no input - empty buffer
@VIMOS-EMPTY

Frame Grabber - memory buffer stuck-at due to buffer failure or to save new picture
FRAMEGRR-BUFFER-SA

Frame grabber - No VIDEO (video 1) signal at VIDEO input
@FRAMEGR-I_VIDEO-F

VIMOS ready Abschasignal - failure to generate signal and transmit it to SINQ SAS
VIMOS-READY

Frame grabber - no output, empty buffer
@FRAMEGR-BUFFER-F

VIMOS ready Abschasignal - failure to generate signal and transmit it to SINQ SAS
VIMOS-READY

VIMOS Interface box - no signal at VIDEO output
NOVIDEO@VBOX

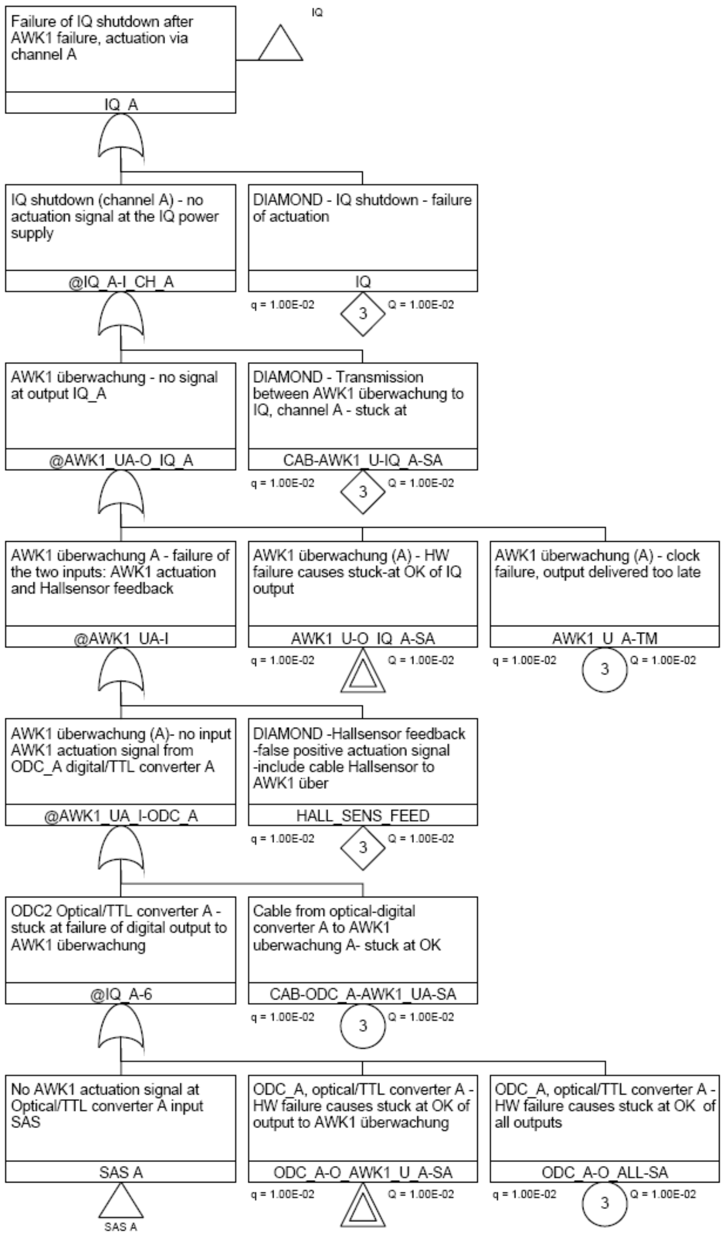
Cable frame grabber to VIMOS interface box - cable broken or unplugged
CAB-FRAMEGR-VBOX-CB

Frame Grabber - failure of the output buffer, total loss of memory content
FRAMEGR-BUFFER-LM

Failure modes for pc-based software (VIMOS)

- Challenging failure modes: part of the PC, SW, OP sys fail while other still function
- VIMOS software loads and processes over and over the same image (frame grabber memory failure).
- The VIMOS software fails to load new images with the result that it processes over and over the same image.

Systems analysis – Fault trees,


IQ
Failure of IQ shutdown after AWK1 failure, actuation via channel A
IQ_A
IQ shutdown (channel A) - no actuation signal at the IQ power supply
@IQ_A-I_CH_A
DIAMOND - IQ shutdown - failure of actuation
IQ
q = 1.00E-02
3
Q = 1.00E-02
AWK1 überwachung - no signal at output IQ_A
@AWK1_UA-O_IQ_A
DIAMOND - Transmission between AWK1 überwachung to IQ, channel A - stuck at
CAB-AWK1_U-IQ_A-SA
q = 1.00E-02
3
Q = 1.00E-02
AWK1 überwachung A - failure of the two inputs: AWK1 actuation and Hallsensor feedback
@AWK1_UA-I
AWK1 überwachung (A) - HW failure causes stuck-at OK of IQ output
AWK1_U-O_IQ_A-SA
q = 1.00E-02
Q = 1.00E-02
AWK1 überwachung (A) - clock failure, output delivered too late
AWK1_U_A-TM
q = 1.00E-02
3
Q = 1.00E-02
AWK1 überwachung (A)- no input AWK1 actuation signal from ODC_A digital/TTL converter A
@AWK1_UA_I-ODC_A
DIAMOND -Hallsensor feedback -false positive actuation signal -include cable Hallsensor to AWK1 über
HALL_SENS_FEED
q = 1.00E-02
3
Q = 1.00E-02
ODC2 Optical/TTL converter A - stuck at failure of digital output to AWK1 überwachung
@IQ_A-6
Cable from optical-digital converter A to AWK1 uberwachung A- stuck at OK
CAB-ODC_A-AWK1_UA-SA
q = 1.00E-02
3
Q = 1.00E-02
No AWK1 actuation signal at Optical/TTL converter A input SAS
SAS A
SAS A
ODC_A, optical/TTL converter A - HW failure causes stuck at OK of output to AWK1 überwachung
ODC_A-O_AWK1_U_A-SA
q = 1.00E-02
Q = 1.00E-02
ODC_A, optical/TTL converter A - HW failure causes stuck at OK of all outputs
ODC_A-O_ALL-SA
q = 1.00E-02
3
Q = 1.00E-02

- Challenge: Failure modes analysis for digital devices:
  – No output: i.e. signal goes to zero
  – Stuck at output: the signal does not switch to the correct output value when needed
  – Timing failure: output of the device is delivered too late (internal clock failure)
  – Wrong parameters set: parameters (e.g. thresholds for signal comparison, timing limits) are set to wrong values.