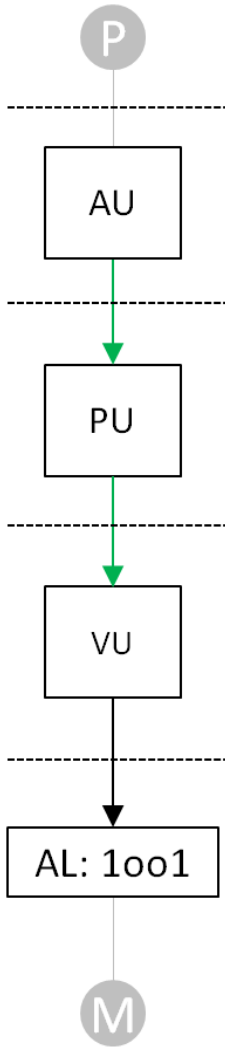
Sensitivity Analysis for the Evaluation of Failure Effects on an I&C Test System

PSAM 14, Los Angeles, USA, 9/18/2018

Dr. Christian Müller, GRS, Germany

Basic Structure of Model Systems



Acquisition Unit

AU: Digitization of input signals and transmission as data telgrams via communication network to PU

Processing Unit

PU: Select 2nd maximum and compare result with limit value (high); if limit is exceeded, forward control signal to VU

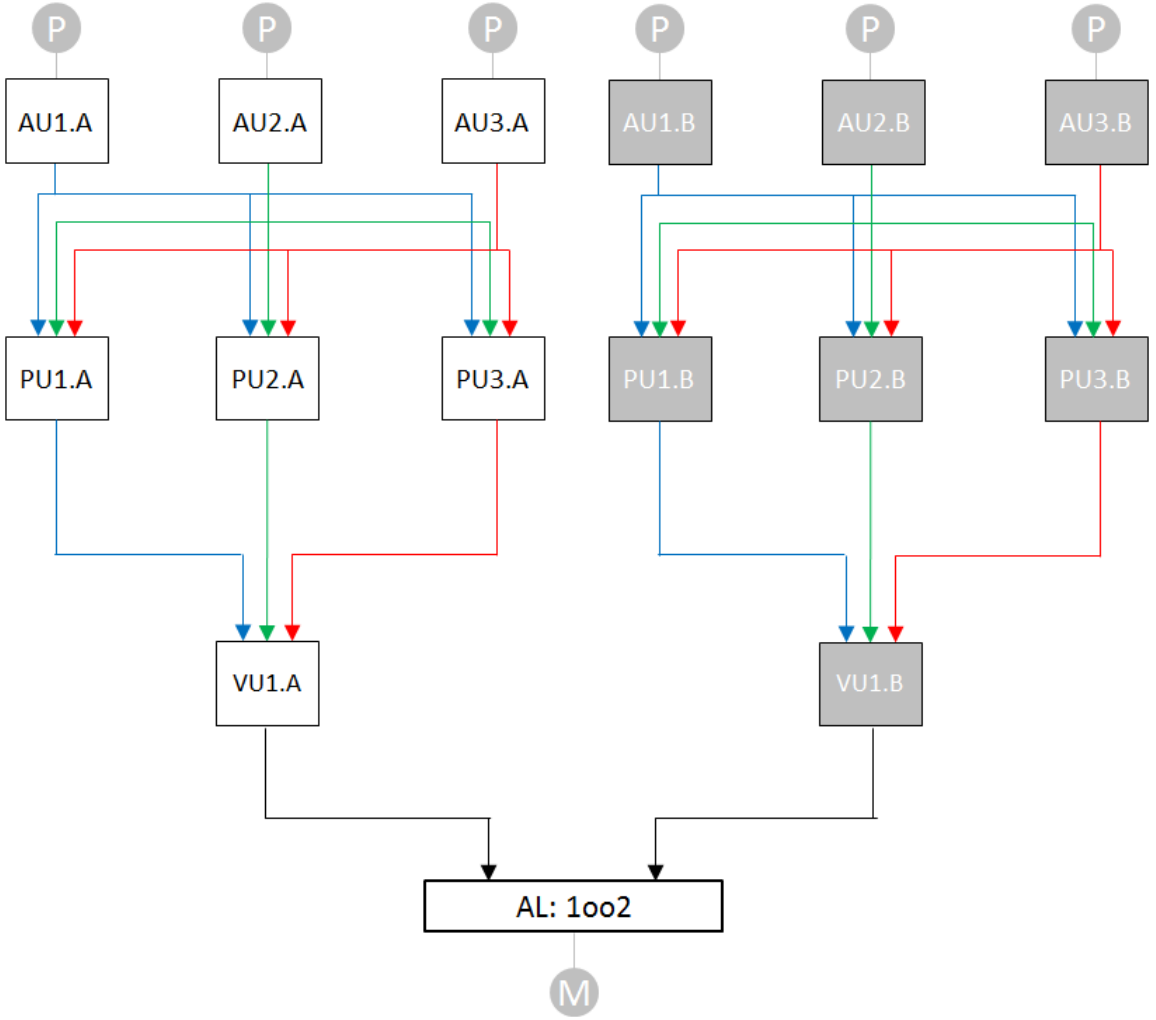
Voting Unit

VU: n-out-of-m voting; if necessary, form control signal for a component
(e.g. M - motor)

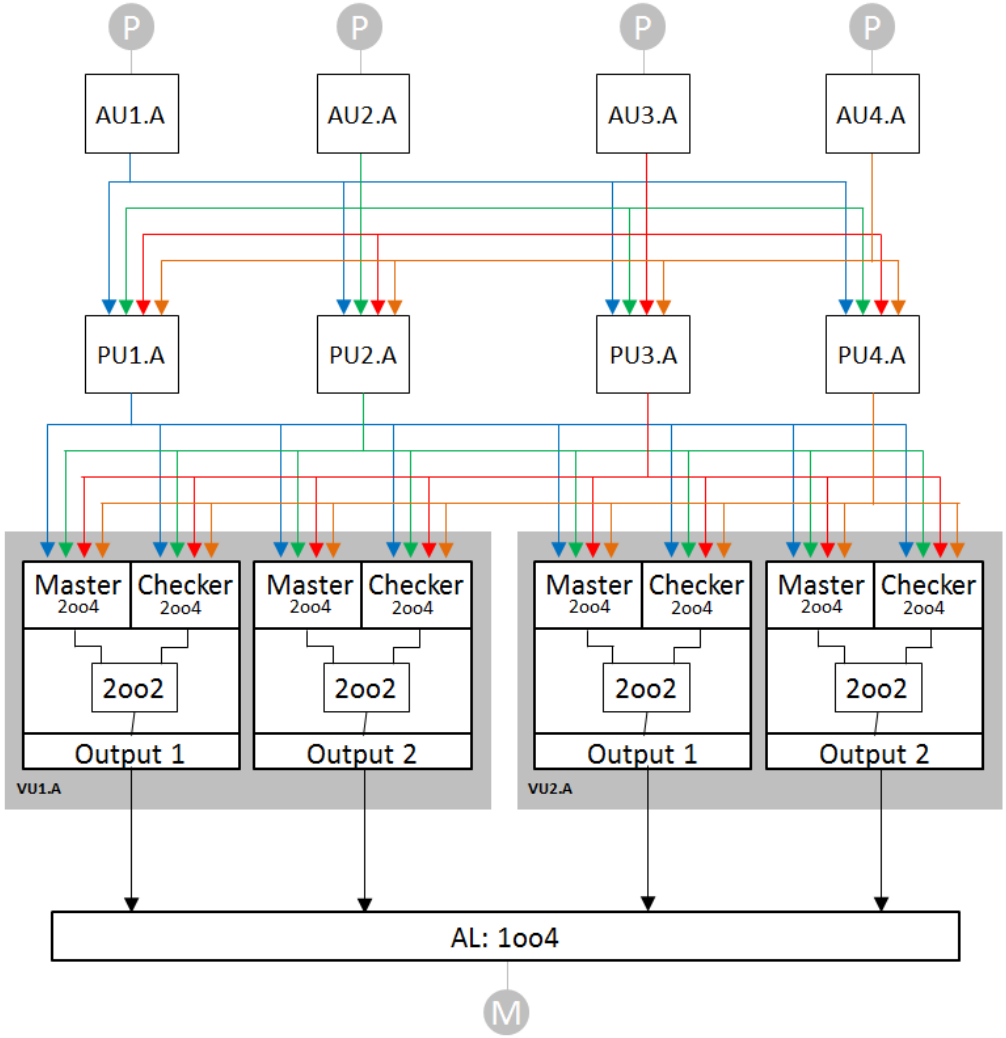
Overview of Model Systems

- A222
  - 2 VU, 2 PU, 2 AU
- A133
  - 1 VU, 3 PU, 3 AU
- A333
  - 3 VU, 3 PU, 3 AU
- A133A133
  - 1 VU (A), 3 PU (A), 3 AU (A) + 1 VU (A), 3 PU (A), 3 AU (A)
- A133B133
  - 1 VU (A), 3 PU (A), 3 AU (A) + 1 VU (B), 3 PU (B), 3 AU (B)
- A2MC(1)33
  - 2 VU (1 Master-Checker subunit each), 3 PU, 3 AU
- A2MC(2)44
  - 2 VU (2 Master-Checker subunits each), 4 PU, 4 AU

Example: Model System A133B133

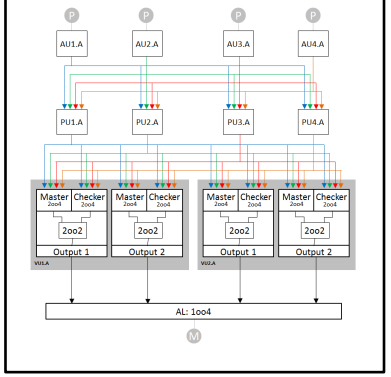


Example: A2MC(2)44

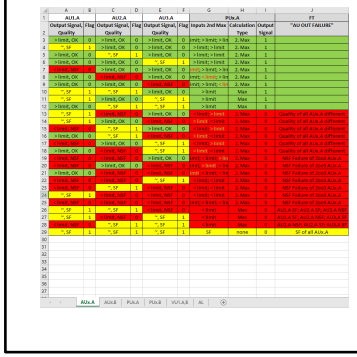


Methodology

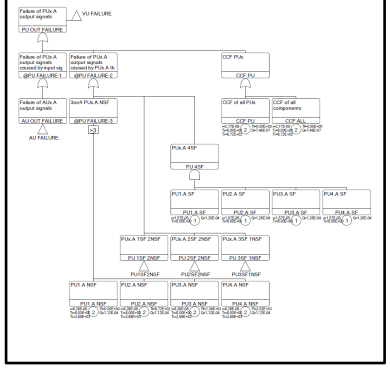
Model System



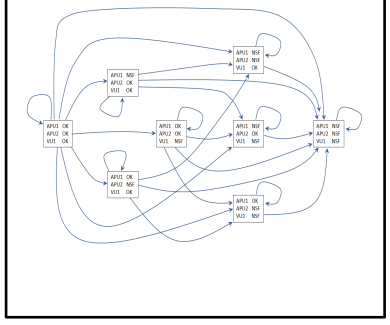
FMEA (mod.)



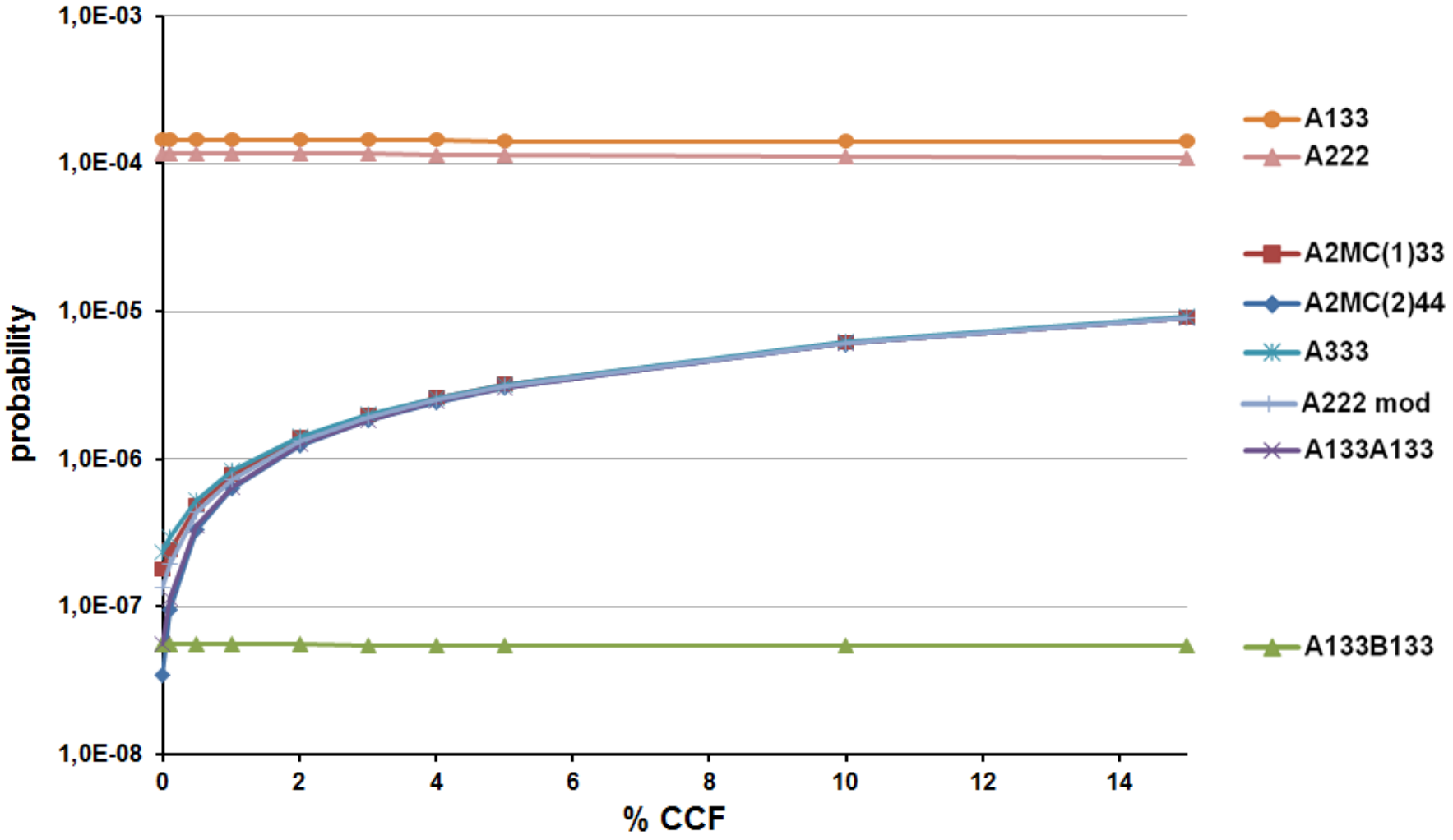
FTA (ext.)



Markov



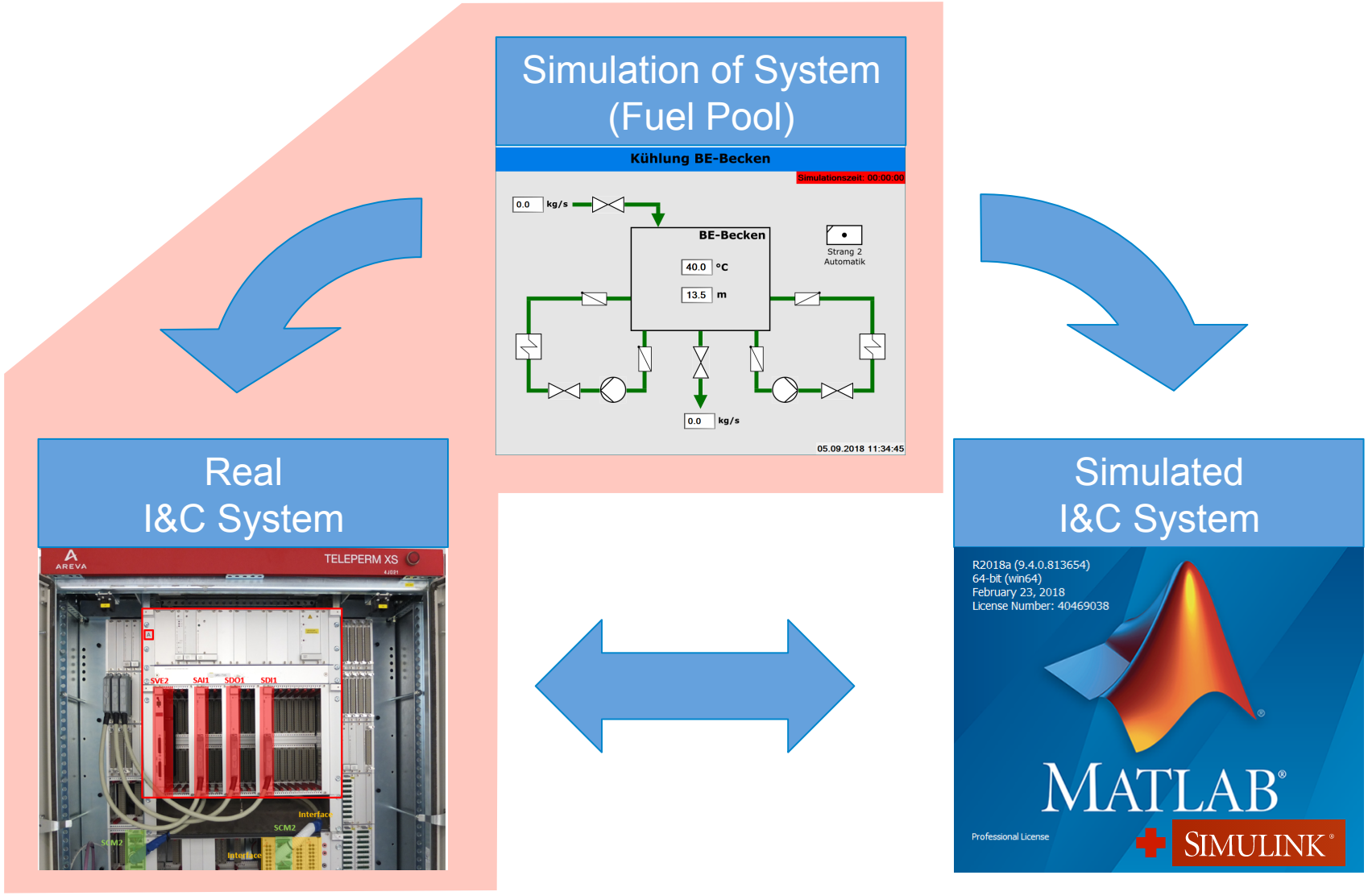
Results: e.g. Sensitivity to Changes in Percentage of CCF



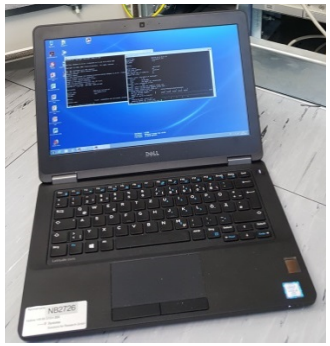
Conclusions (Part 1)

- A new methodology for the sensitivity analysis for the evaluation of failure effects on I&C systems has been developed
  - Based on: FMEA, FTA, Markov processes
- Sensitivity to the variation of failure rates of individual components has expected effects on the overall reliability of the system function
- Sensitivity analysis with respect to CCF:
  - Generally: significantly increased probability of system failure with the percentage of CCF
  - Exception: Model system A133B133, whose architecture consists of diverse subsystems (assuming complete diversity of hardware and software)
    - Although real proportion of CCF is unknown, the evaluation has shown that diverse I&C architectures already offer a clear advantage even for very small percentages of CCF (< 1 %)
- FTA (based on FMEA) can efficiently model and analyze a large number of different architectures of digital I&C

Development of I&C Test Environment at GRS

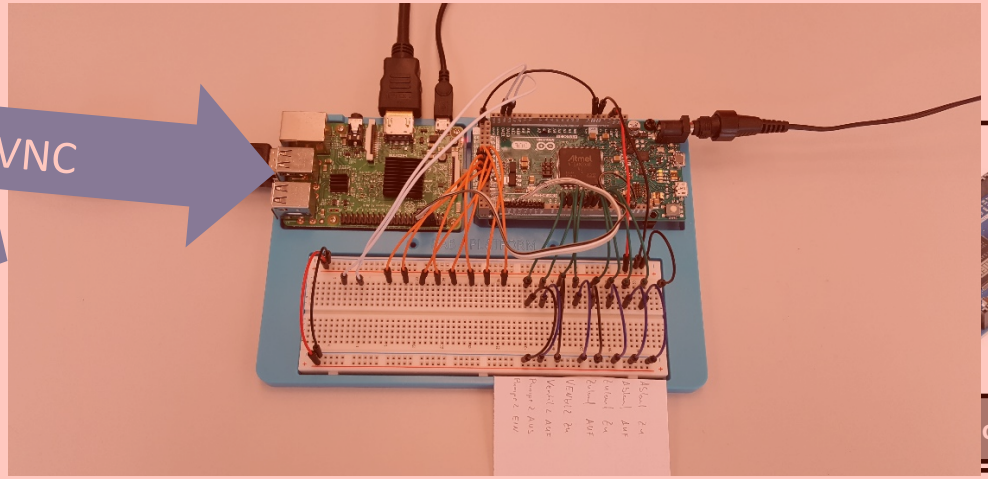


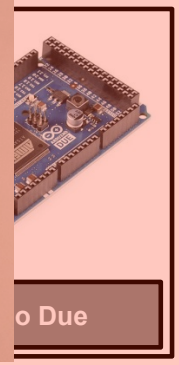
Schematic Structure with Real I&C System



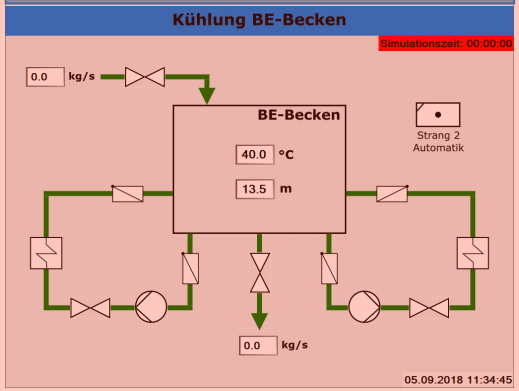
VNC

VNC

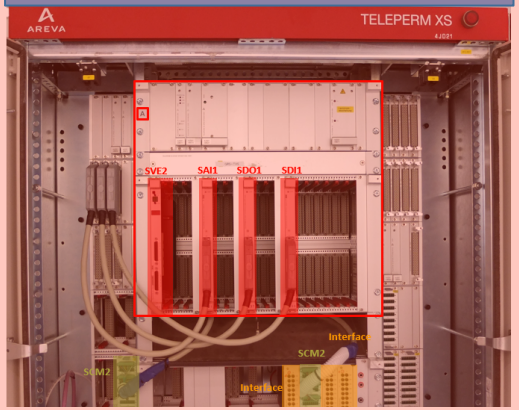




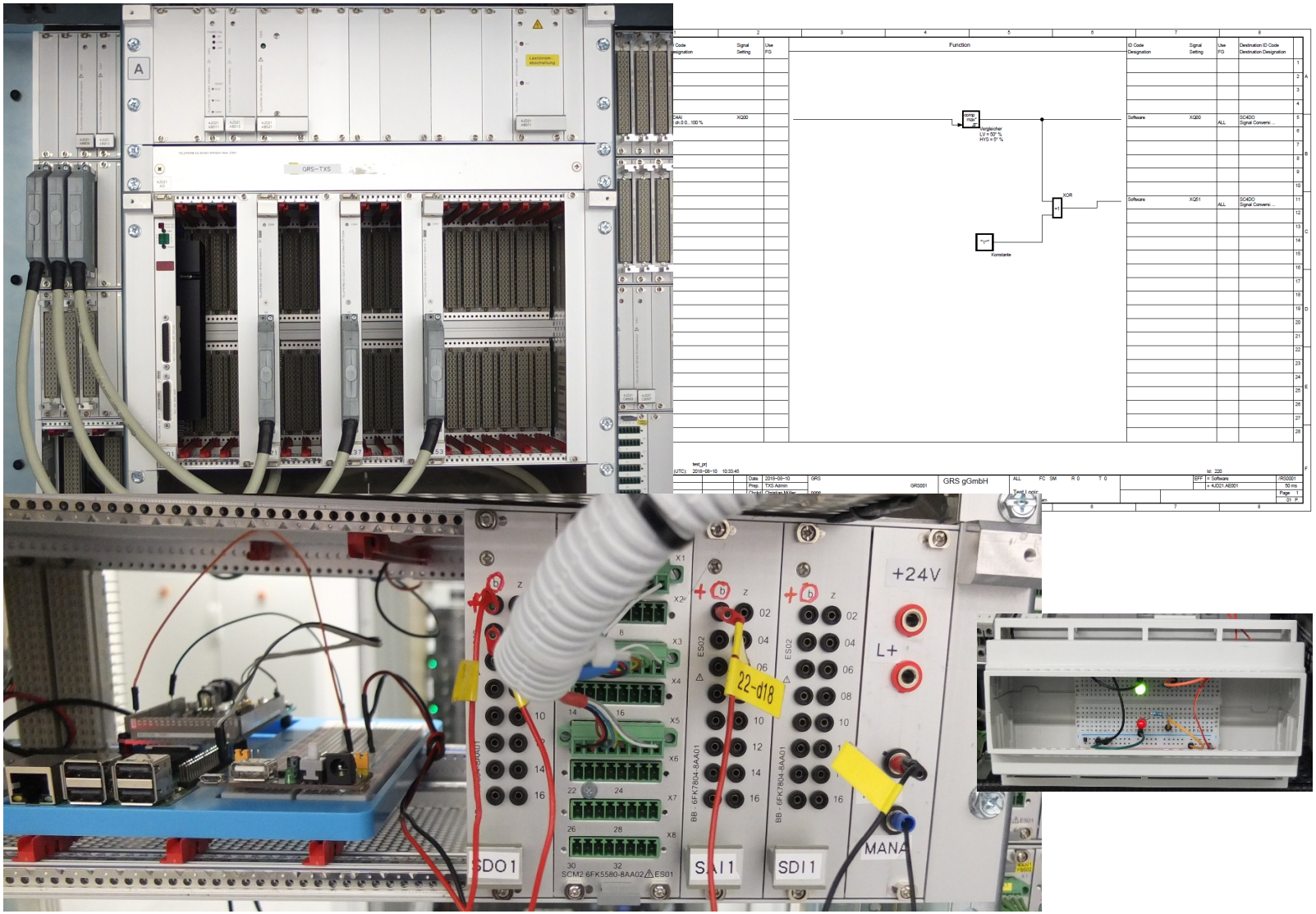
Simulation of System [Fuel Pool]



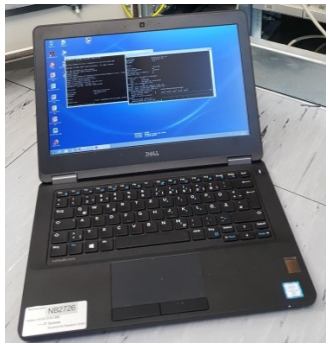
Real I&C System



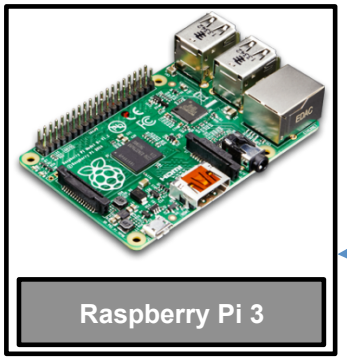
Actual Status: Real I&C System



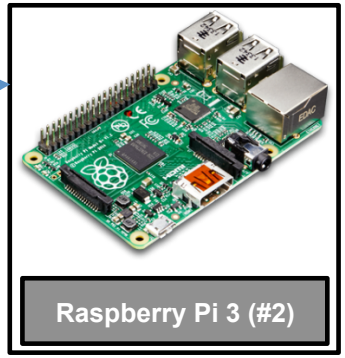
Schematic Structure with Simulated I&C System



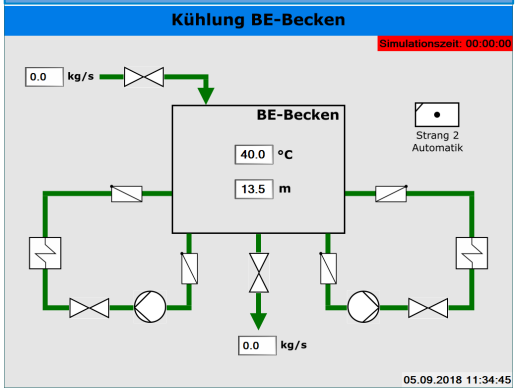
VNC



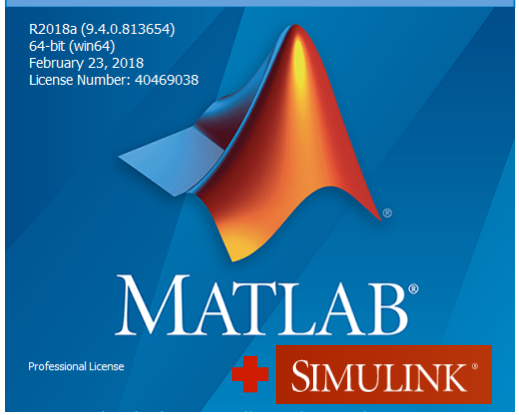
Serial Interface



Simulation of System [Fuel Pool]



Simulated I&C System



Conclusions (Part 2)

- The methodology for the sensitivity analysis of failure effects in modern digital I&C systems is currently extended and validated by the development of a test environment
- The test environment at GRS will consist of:
  - A simulation of a process engineering system (fuel pool)
  - A real I&C system
  - A simulated I&C system
- Actual status:
  - The development of the process engineering simulation is finished (although it will be further developed in the future)
  - The development of the interface between the process engineering simulation and the real I&C system is finished and tested
- Next steps:
  - Engineering of I&C functions for the real I&C system
  - The first tested architecture will correspond to model system A222
  - Development of I&C simulation (MATLAB/Simulink)

Acknowledgements

The authors want to acknowledge the support provided by the

German Federal Ministry for the Environment, Nature Conservation and Nuclear Safety

for funding the GRS development of the methodological approach to the sensitivity analysis of failure effects in modern digital I&C systems and the development of the I&C test system.

Contact

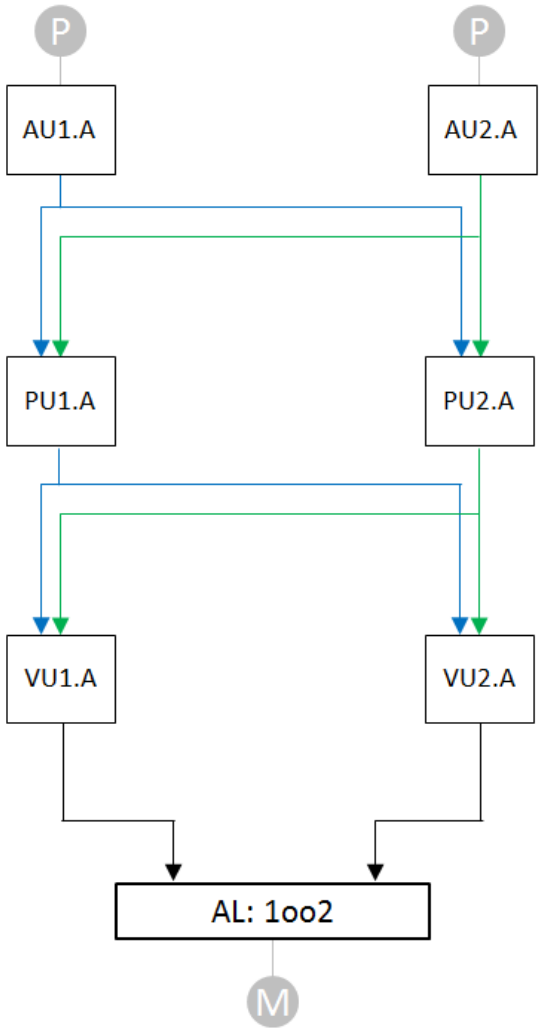
Dr. Christian Müller
Electrical and I&C Systems

Gesellschaft für Anlagen- und Reaktorsicherheit (GRS) gGmbH
Forschungszentrum, Boltzmannstraße 14
85748 Garching bei München

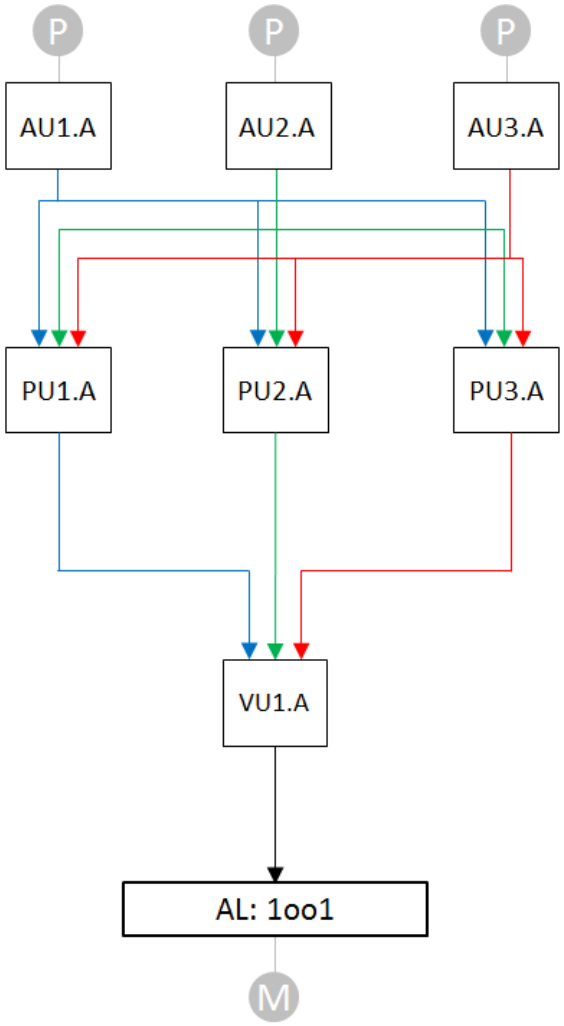
phone: +49 (0) 89 - 3 20 04 - 499
e-mail: christian.mueller@grs.de

Backup

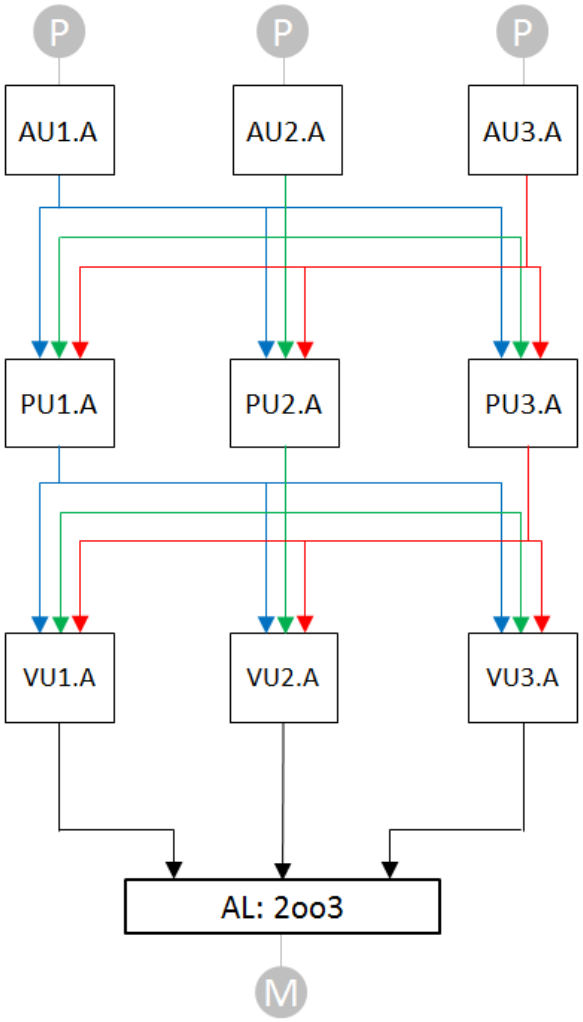
A222



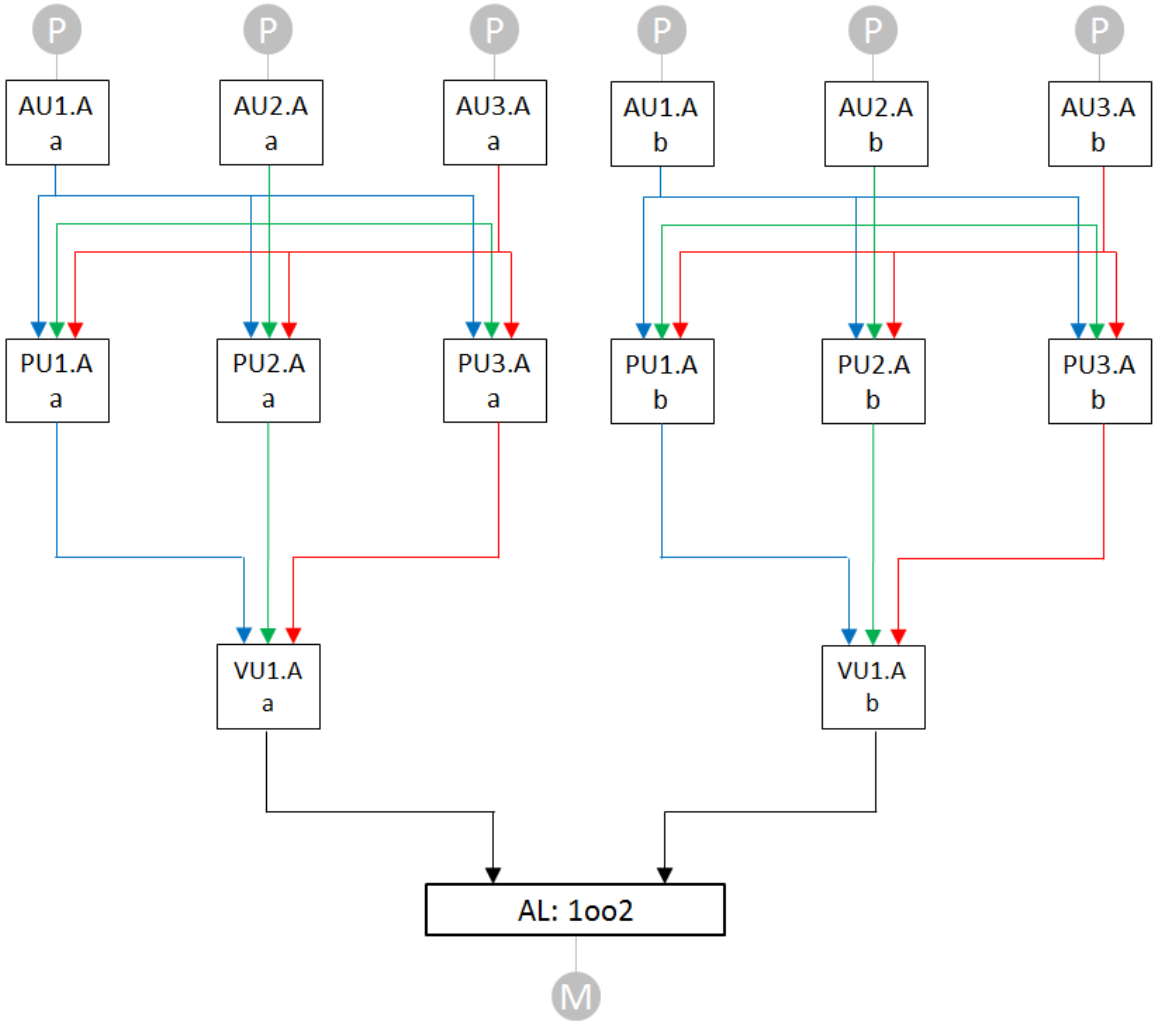
A133



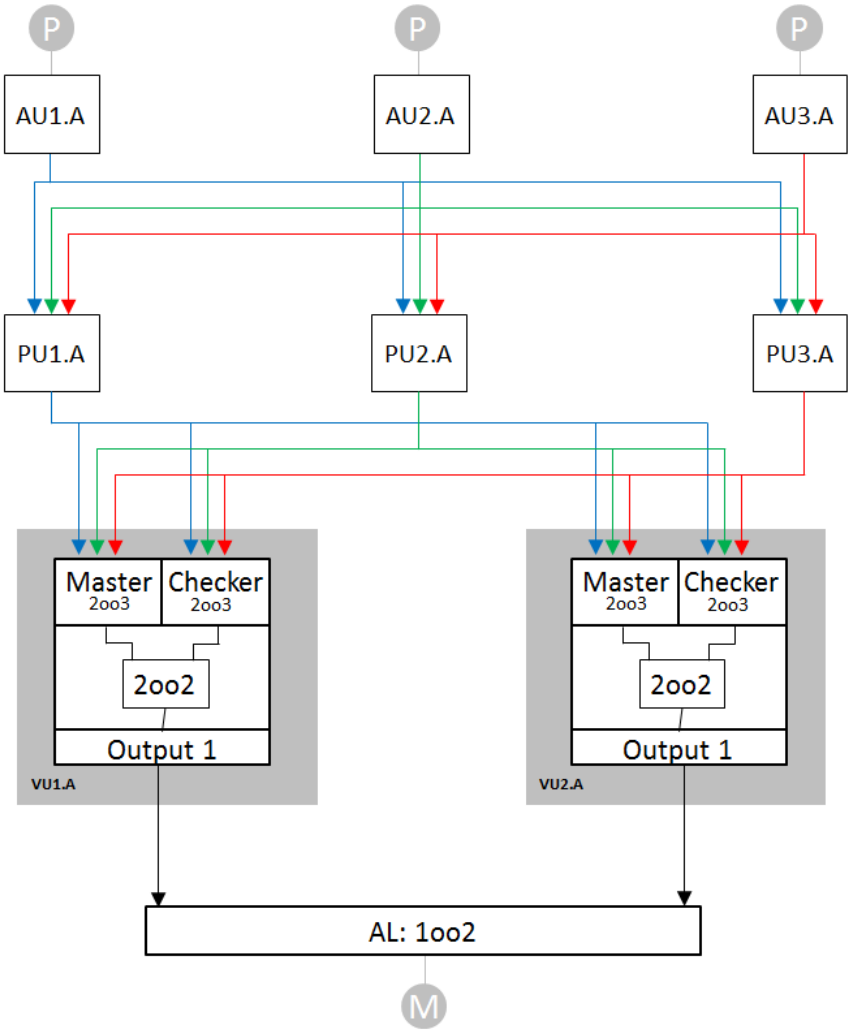
A333



A133A133


P
P
P
P
P
P
AU1.A a
AU2.A a
AU3.A a
AU1.A b
AU2.A b
AU3.A b
PU1.A a
PU2.A a
PU3.A a
PU1.A b
PU2.A b
PU3.A b
VU1.A a
VU1.A b
AL: 1oo2
M

A2MC(1)33


P
P
P
AU1.A
AU2.A
AU3.A
PU1.A
PU2.A
PU3.A
Master
2oo3
Checker
2oo3
2oo2
Output 1
VU1.A
Master
2oo3
Checker
2oo3
2oo2
Output 1
VU2.A
AL: 1oo2
M

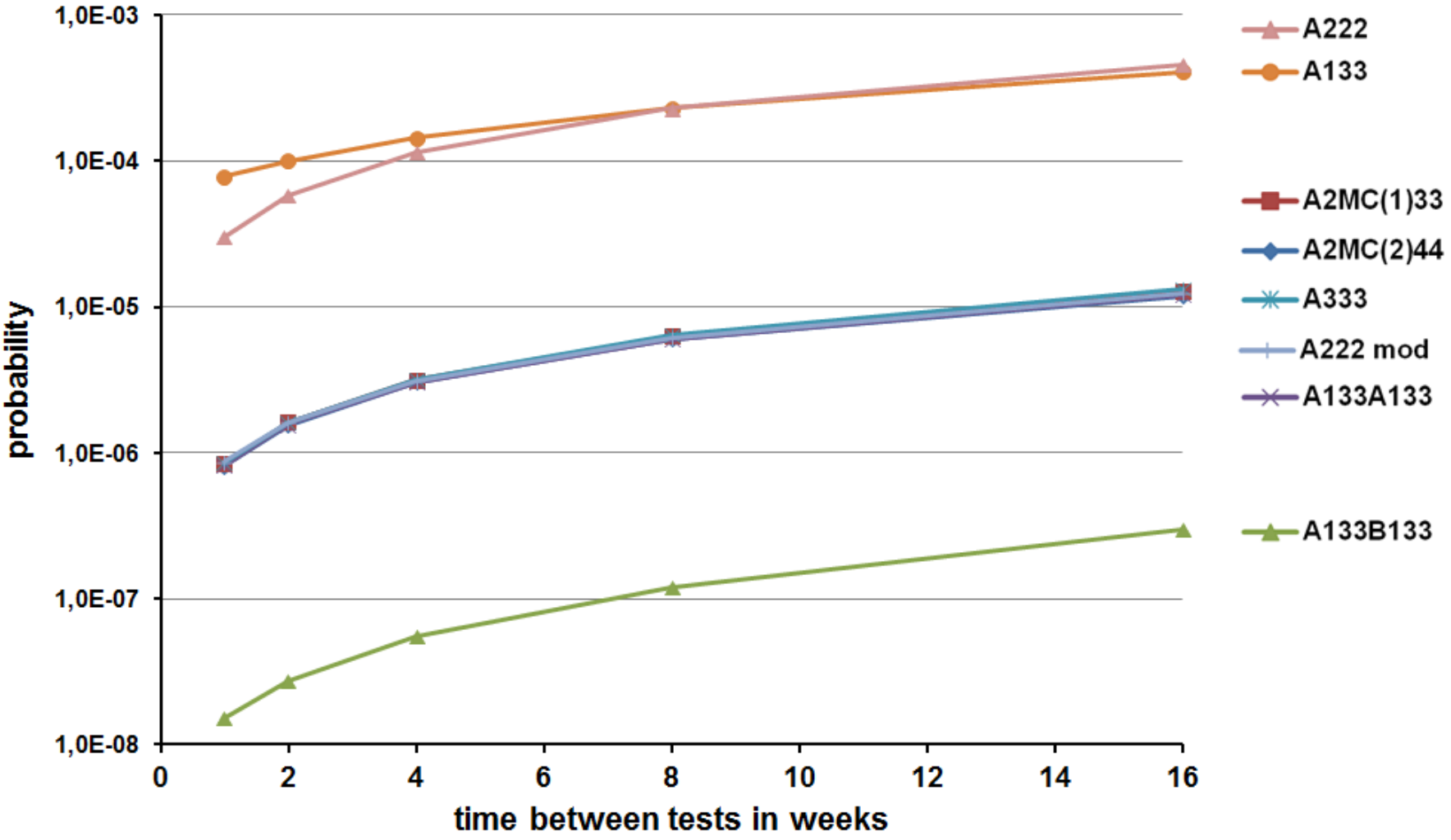
Failure Rates of Components

Kind of Failure	Failure Rate	Remarks
AL NSF	$1.000 \cdot 10^{-10}\ h^{-1}$	arbitrary value
AU NSF	$8.265 \cdot 10^{-8}\ h^{-1}$	incl. communication with PUs
AU SF	$2.098 \cdot 10^{-5}\ h^{-1}$	
PU NSF	$8.265 \cdot 10^{-8}\ h^{-1}$	incl. communication with VUs
PU SF	$1.573 \cdot 10^{-5}\ h^{-1}$	
VU NSF	$8.265 \cdot 10^{-8}\ h^{-1}$	no NSF for master-checker configuration
VU SF	$6.972 \cdot 10^{-6}\ h^{-1}$	
VU SF (MC)	$1.029 \cdot 10^{-5}\ h^{-1}$	MC - master-checker configuration
AU CCF	$2.175 \cdot 10^{-9}\ h^{-1}$	CCF of all AUs of one type of system
PU CCF	$2.175 \cdot 10^{-9}\ h^{-1}$	CCF of all AUs of one type of system
VU CCF	$2.175 \cdot 10^{-9}\ h^{-1}$	CCF of all AUs of one type of system
All CCF	$2.175 \cdot 10^{-9}\ h^{-1}$	CCF of all components of one type of system

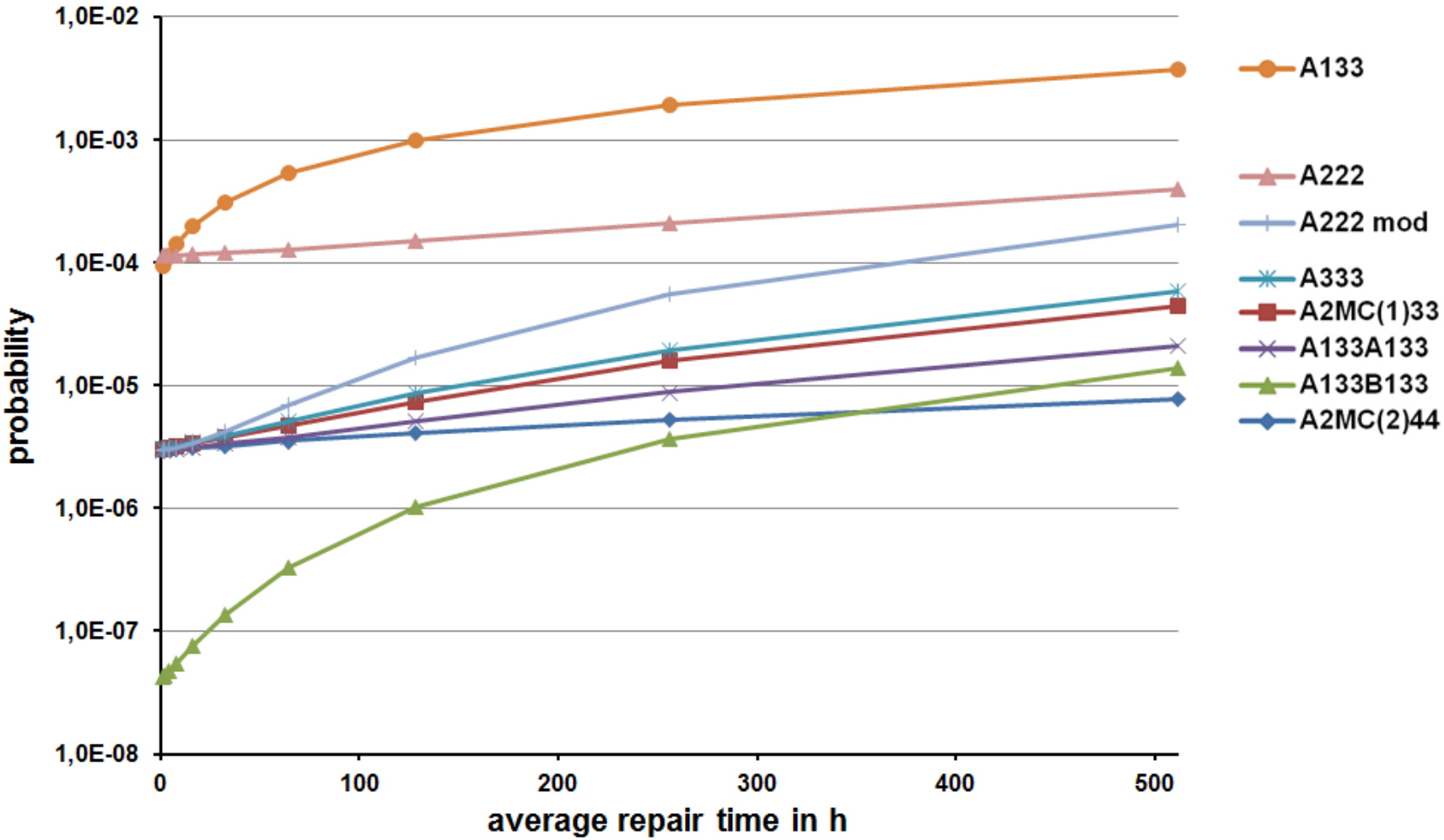
Results: Sensitivity S of Model Systems to Changes in Failure Rates

Failure Rate	A2MC(2)44	A2MC(1)33	A133B133	A133A133	A333	A133	A222 mod	A222
AL NSF	1.11	1.11	15.30	1.11	1.11	1.00	1.98	1.00
AU NSF	1.00	1.97	1.01	1.00	1.95	1.02	1.55	78.50
AU SF	1.00	1.27	1.00	1.00	1.27	1.01	1.16	1.02
PU NSF	1.00	1.68	1.01	1.00	1.67	1.01	1.15	1.00
PU SF	1.00	1.00	1.00	1.00	1.00	1.00	1.12	1.01
VU NSF			3.70	1.04	1.76	13.40	1.12	1.00
VU SF	1.00	1.22	2.65	1.03	1.38	6.94	1.11	1.00

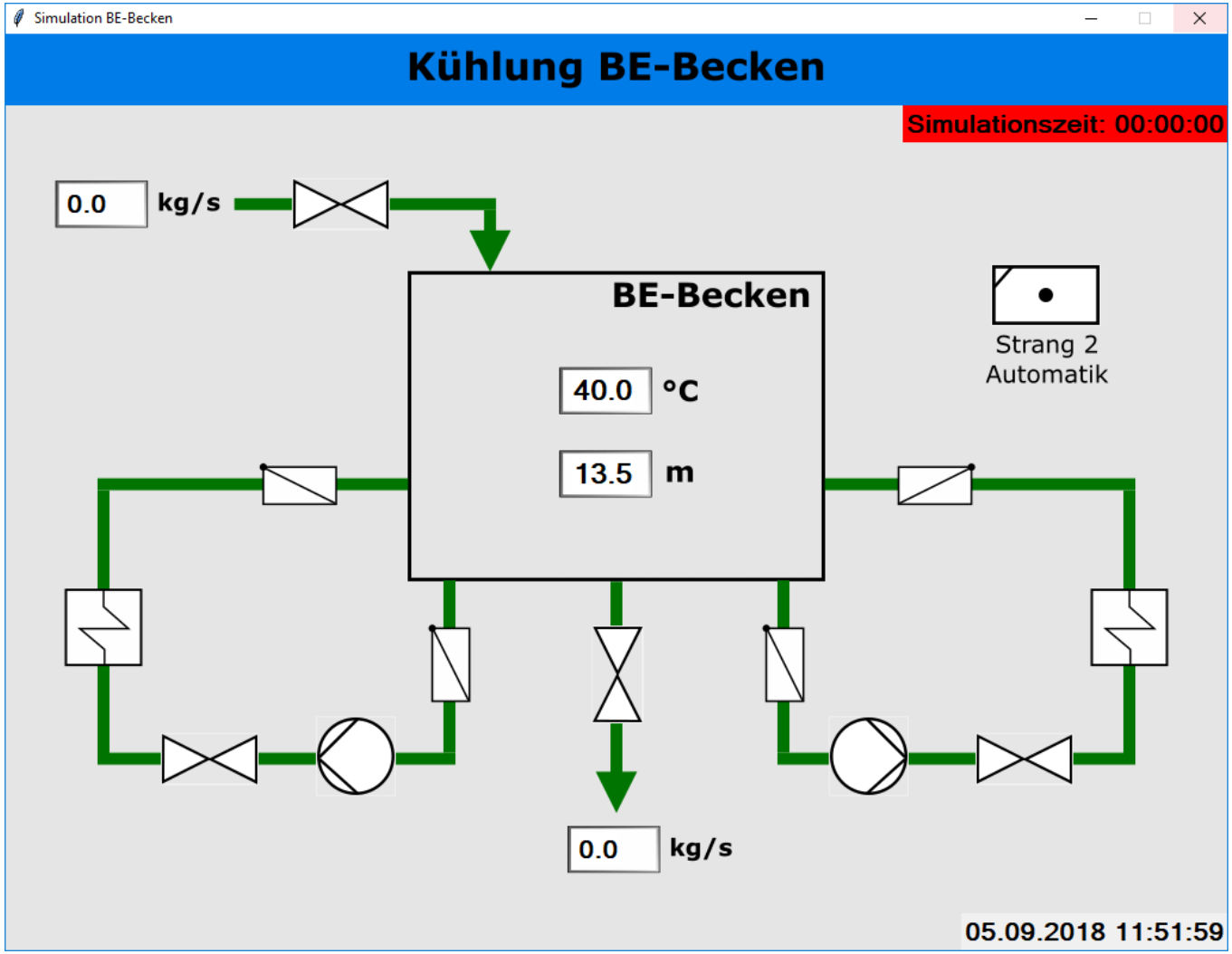
Results: Sensitivity to Changes in Time between Tests



Results: Sensitivity to Changes in Repair Time



Actual Status: Simulation of System (Fuel Pool)



Actual Status: Real I&C System