Evaluation of the beamline personnel safety system at ANKA under the aegis of The 'Designated Architecture' Approach

K.Cerff, D.Jakel, R.Stricker, M.Hagelstein, I.Birkel, KIT, ANKA, Karlsruhe, Germany

Introduction

- The Beamline Personnel Safety System (BPSS) is established as a Safety Instrumented System (SIS) to control the exclusive access of ionizing radiation OR persons to the beamline radiation areas at ANKA.
- When system design started in 2002 the approach to use Programmable Logic Controllers (PLC) for safety related functions was rather new in process control. Since then not only the number of ANKA beamlines monitored by the BPSS has increased but also the national and international standards for component and system safety have evolved and changed the needs to prove beamline radiation safety functions to certifying authority.
- At design time of the ANKA-BPSS life cycle, the reliability for components and the overall system was defined in terms of safety categories 1-4 (Cat) based on the risk analysis given within the European standard EN 954-1 defining safety categories, following the principle of 'good engineering practice'.
- During the last years the development of smart safety sensors and actuators went on, more and more they are monitored rather by software diagnostics than by hardware measure.
- In accordance to the new European standard EN-ISO 13849 1-2, the methods to evaluate safety functions were adapted and revised, due to the required quantification of Performance Level (PL) by EC-machinery directive.

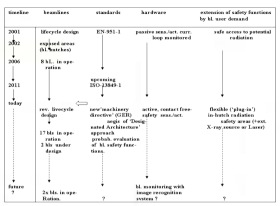

Figure 1: external factors and evolution of ANKA-BPSS since 2001.

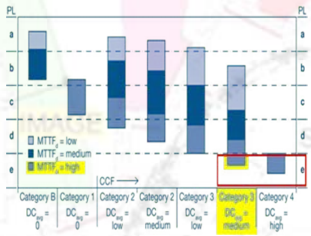

Figure 2: matching of EN-941 based category and EN-ISO 13849 performance level concepts.

Control Law and Safe Beamline States

The state dynamics depend on a set of coordinated safe transisitions of radiation shutters and/or doors, which are event driven.They are monitored and interlocked on the proposition of ANKA-safety control law.

- **The access of ionizing radiation and persons at the same time and location in a radiation control area is excluded with a PL ~ 10-8.**

In terms of process control this will be achieved by

- at least one closed and and interlocked upstream radiation shutter in front of a radiation hutch with opened access doors.
- downstream access doors or monitored radiation shields which are kept closed and interlocked, if a safe shutter state isn't reached in a fixed period of time.
- the initialisation of an accelerator beamdump in case of an interlock break of a shutter, hutch door or a subsystem/safety hardware component failure.
- a redundant frontend shutter safety controller supervising local beamlines in maintenance mode, if the local beamline safety controller is switched off.
- by monitoring all the components, subsystems and the whole safety system ANKA-BPSS with software based Diagnostic Coverage (DC) at a level >99%. The controller hardware, the software modules and the safe fieldbus (SafetyBusP*) are certified according to SIL 4.
- the operation of beamline safety functions is exclusively controlled by control law and safety PLC as BPSS system master.

*trademark

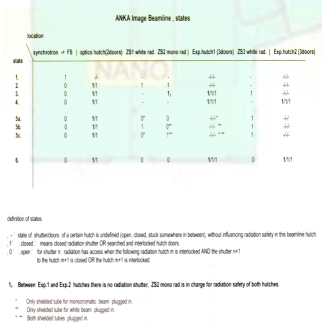

Figure 3: table of door-hutch and safety flange docking states (stations for radiation shielded vacuum tube in Exp hutch1, here for new IMAGE beamline).

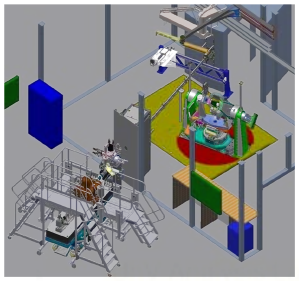

Figure 4: realized, variable safety functions in ANKA-NANO-beamline experiments hutch 1: shielded tube operation AND hutch access OR diffractometer operation NAND hutch1 access.

Discrete Event System Dynamics

- The system dynamics are modelled by the DES-shutter/hutch automaton, which is the basic modul of ANKA-beamline safety functions. It includes the model of known failure (stuck) events and describes the model of fail-safe system behavior.

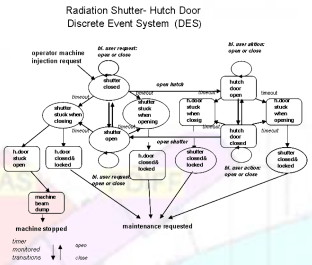

Figure 5: The shutter – hutch access door automaton as standard ANKA –safety module, the system model considers blocking events in case of safe detected, non-regular operation (stuck) of shutter and/or hutch door.

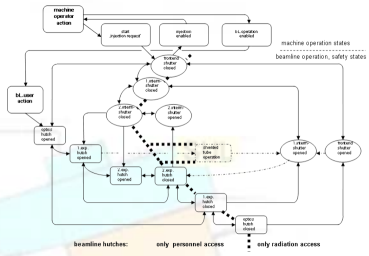

Figure 6: simplified DES model (without blocking states of an ANKA beamline, composed of three nested safety automata and one optional automaton inside the first experiments hutch (shielded tube to connect temporary the optics hutch with the second experiments hutch and allow concurrent safe access of persons to the first experiments hutch.

Markov Minimal Cut Set Analyse

- In the second stage of abstraction the combined beamline safety system states are regarded as stochastic timed structures. There are different methods to analyse such systems, due to applicability for our safety system with DC we use the Markov Minimal Cut Set approach extended by Diagnostic Coverage.
- The stochastic timed automata are decomposed down to the component level in serial and parallel structures, building a Reliability Block Diagram (RBD).

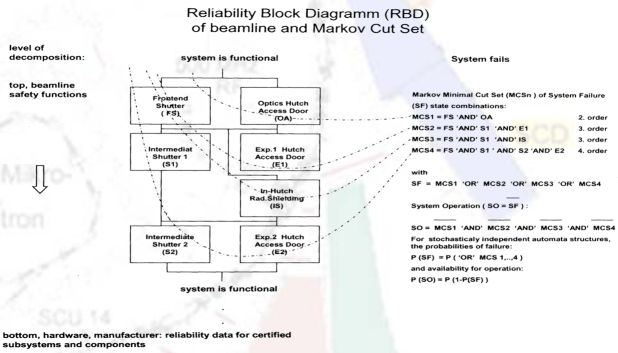

Figure 7: The RBD shows the beamline example in terms of the minimal Markov Cut Set. First order dangerous failure of shutter or access door is compensated by complementary door or hutch safety function. An undetected dangerous failure of a complete shutter-hutch door automaton or an intra hutch shield, s. Fig.5 defines the worst case scenario.

Designated Architecture Approach

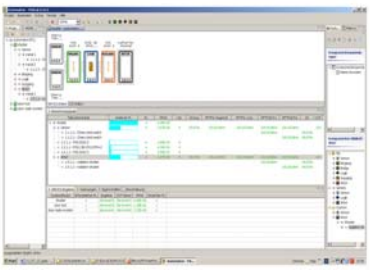

Figure 8: Calculation of Performance level PL of shutter-hutch door automaton, including the independent subsystems: shutter limit switches, door position switches and door lock.The PL calculation is based on data (component libraries) of different manufacturers.

Summary

- The 'Designated Architecture' approach is a complement to classical methods of safety analysis. It is a tool, helpful on the component or spare part level of decomposition to generate quantitative values of Performance Level (PL) for dedicated safety soft- and hardware. The quantification of safety system PL has to be provided for future ANKA-beamlines to receive operation license by the certifying body.