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

Abstract

The Beamline Personnel Safety System (BPSS) at synchrotron radiation source (ANKA) started operation in 2003. The paper describes the safety related design and evaluation of serial, parallel and nested radiation safety areas, which allows the flexible plug-in of experimental setups at ANKA-beamlines.

It evaluates the resulting requirements for safety system hard- and software and the necessary validation procedure defined by current national and international standards, based on probabilistic reliability parameters supplied by component libraries of manufacturers and an approach known as 'Designated Architectures', defining Safety Functions in terms of sensor-logic-actor chains.

An ANKA-beamline example is presented with special regards to (self-) Diagnostic Coverage (DC), which is not part of classical Markov process modelling of systems safety.

INTRODUCTION

The Beamline Personel 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 hutches of ANKA.

When system design started in 2002 the approach to use Programmable Logic Controllers (PLC) for safety related functions and not a hardwired logic 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 BPSS reliability of new ANKA beamlines to the certifying authority (regional council) in Germany. At the time when the ANKA-BPSS life cycle was designed, the reliability for components and the overall system was defined in terms of safety Categories (Cat 1-4) based on the risk analysis given within the European Standard EN 954-1 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 by software diagnostics and not by hardware measure. In accordance to existing standards the methods to evaluate safety functions were adapted and revised.

Since the end of 2011 the EN-954-1 has been replaced by the 'harmonized' standard ISO 13849 1-2 which links the Safety Integrity Level (SIL) concept to Performance Levels (PL) defining an approach in terms of probabilistic failure rates for components and systems.

As a consequence of the new 'machinery directive' [1] each replacement of safety hard- or software on the pre-2011 beamlines has to be re-evaluated according to the methods suggested by ISO-13849 requesting the migration of the existing safety documentation to the new standard.

SAFETY SYSTEM CONTROL LAW

Radiation and personnel access at the same location at the same time are excluded fail-safe, with a time invariant probability of unknown dangerous risc, equivalent to a Performance Level (PL) of ~ 10-8 undetected dangerous events per hour over the planned live-time of the ANKA-BPSS safety system (20 years+).

System Features

In terms of process control this will be achieved by

- at least one upstream radiation shutter which is closed and interlocked in front of an accessible hutch.
- downstream access doors or monitored radiation shields which are kept closed and interlocked if a safe shutter state isn't reached in a fixed span.
- an accelerator beamdump which is initialized in case of interlock break of shutter or hutch door, component or subsystem failure.
- the use of a redundant frontend shutter safety controller supervising local beamlines in repair mode, if the local beamline safety controller is switched off.
- all the components, subsystems and the whole safety system ANKA-BPSS are monitored with Diagnostic Coverage (DC) at a level >99%. The controller hardware, the software modules and the safe fieldbus (Safety-BusP*) [2] are certified according to SIL 4.

DETERMINISTIC SYSTEM MODEL

In the first stage of abstraction, the radiation shutter-hutch access door module is defined as the basic building block of the ANKA-BPSS. safety states and transitions in Figure 1 illustrates the module of the 'exclusive OR' logic coupled radiation shutter-access door mechanism. Several modules are combined to build the Discrete Event System (DES) model of the entire beamline safety system in Figure2. This, called automaton, is also applicable to model temporary intra-hutch radiation shields or plug-in experimental setups requesting safety functionality.

*trademark

ISBN 978-3-95450-139-7

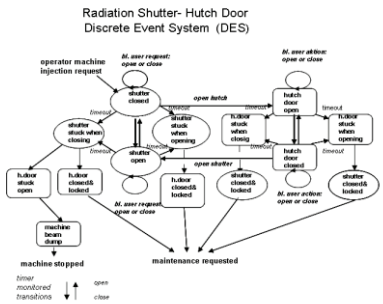

Figure 1: The shutter – hutch access door automaton as standard ANKA –safety module, the system model considers blocking events in case of safe detected, non-regular operation (stuck) of shutter and/or hutch door.

Pure shutter- or door states are reached by bidirectional transitions under normal operation. Transitions between shutter-hutch states are unidirectional.

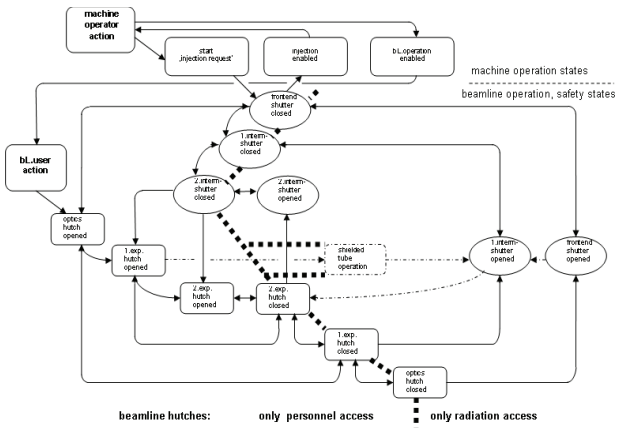

Figure 2: simplified DES model (without blocking states of Fig. 1) of an ANKA beamline composed of three nested safety automata and one optional automa-ton inside the first experiments hutch (shielded tube to connect at times the optics hutch with the second experiments hutch and allow concurrent safe access of persons to the first experiments hutch).

The diagrams show

- the finite-state, deterministic model safety system logic as a single sample realisation of the control law stated above.
- conceivable combinations of user input events, manipulating shutter and hutch doors, under the restriction to lead to inherent safe system states.
- the alarm handling (beamdump) in case of subsystem failure.
- the influence of accelerator states on beamline interlock operation mode.

DISCRETE EVENT SYSTEM DYNAMICS

User interaction with the safety system is varying in frequency from moderate demand of some events per minute, toggling radiation shutter between open-close states, to some events per hours, accessing radiation hutch when preparing beamlime experiments, to low demand of one event per day or even week (in shutdown period).

On the level of safety functions such a shutter or door event triggers a timer, monitoring the span to reach a limit switch position of radiation shutter (< 10 sec.) or the fixed maximum search time (<30 sec.) to arm the hutch interlock. In case of time overflow an appropriate alarm event, depending on frontend shutter position is initiated.

On software level, state changes are resolved on the time base of a program cycle, being 1 msec. Safety alarm events with highest priority are handled in a range of 20 to max. 50 msecs. from sensor input to output of shut-down signal, being sufficient for a safe radiation shut-down within 150 msec. [3].

The directed graphs Fig1/2. show only one possible representation of the probabilistic process, driving beamline states, initiated by different players. There is the probability of a fatal transition between such states defining the risk probability of a dangerous system failure [4] which has to be analysed.

MARKOV RELIABILITY ANALYSIS

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 [4], due to applicability for our safety system with DC we use the Markov Minimal Cut Set approach [5].

System Top-down Decomposition and Markov Cut Set Analysis

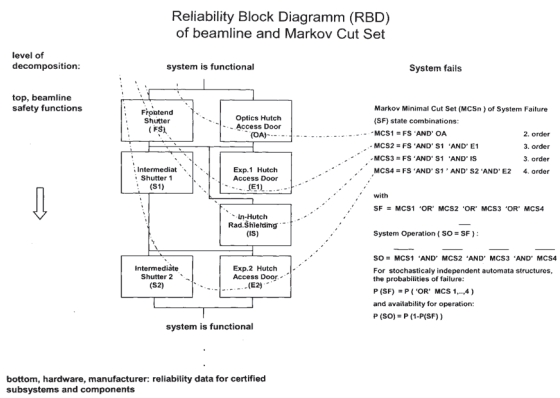

Figure 3: The RBD shows the beamline example in terms of the minimal Markov Cut Set. First order dangerous failure of shutter or access door is compen-sated by complementary door or hutch safety function. An undetected dangerous failure of a complete shutter-hutch door automaton or an intra hutch shield, s. Fig.1 defines the worst case scenario.

The stochastic timed automata are decomposed down to the component level in serial and parallel structures, building a Reliability Block Diagram (RBD).

The Markov probability of system safe failure P(SF) is defined as 'OR' composition of the minimal cut set (MCS k=1,..,4) of states, s. Fig.3. The probabilistic availability of

ISBN 978-3-95450-139-7

a system P(SO) is the complement of P(SF) for stochastic independent structures. For stochastic dependent subsystems there is only a weak dependency of P(SF) in RBD serial structures, but a strong one for parallel structures. This may affect structures with many identical components, the related kind of failure is known as Common Cause Failure (CCF). In this case failure probabilities of minimal cut set with members 1 to n sums up, for beamline example is n = 4.

$$P'(SF) = \sum MCS_k \quad , k=1,..,n$$

To minimize P'(SF) for CCF the concept of diversity is applied. In terms of probability this means to take measures to make the transition probabilities stochastically independent, so the 'OR' composed P(SF) of low order MCS is valid. At ANKA safety system the CCF is reduced by

- use of a triple modular diverse redundance PLC with 3 out of 3 voting, redundant CAN-bus controllers and safety extended CAN-data protocol [2].
- SIL-4 certified Software blocks.
- Independent hardware test channels, leading to a DC >99% with appropriate system control logic.

DESIGNATED ARCHITECTURE APPROACH

On bottom level of decomposition the RBD is modelled by the designated architecture approach, according to standard DIN EN ISO13849-1 and EN/IEC 62061.

For evaluation of the Performance Level (PL), the free SISTEMA* software [6] of the German 'Institut für Arbeitsschutz' (IFA)[#] is available. We use a manufacturer specific software tool [7] with fieldbus component SafetyBusP* not yet available in SISTEMA* library.

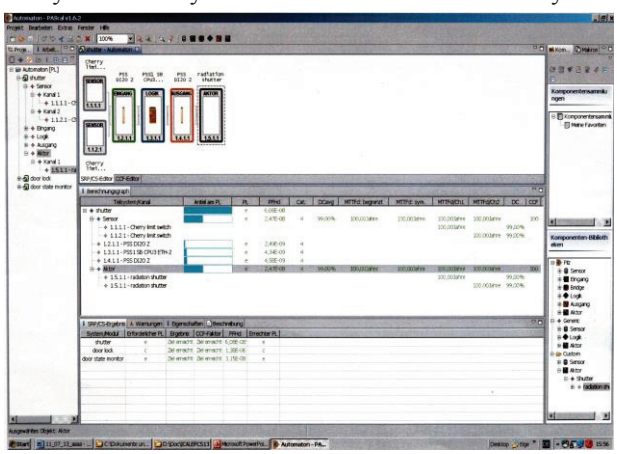

Figure 4. Designated Architecture approach: -Sensor-Input-Logic-Output-actor-chains calculated by [7].

Calculation of Performance Level

Figure 4 shows the decomposed automaton. with three Designated Architecture submodules. For the combined shutter- hutch access door the worst case residual risc is (both fail together) PL = 9,23x10-8.

The door lock with a lower PL = 1,38x10-6 is not part of the door access safety function, which is supplied by the door switches, monitoring the open/close door states. The door lock is a measure to prevent users from accidently opening a searched radiation hutch at beam operation time, triggering a beamdump by activating safety switches. The calculation Fig.4 shows the fraction of PL contributed by components (cyan bars), the contribution of electronic subsystems (PLC, safe fieldbus) is negligible in the range of PL ~10-9 failures per hour, the highest degradation in PL is supplied by electro-mechanical sensor/actor components.

SUMMARY

The ANKA distributed safety system design needs first a classical system analysis to set up system control law, to simplify system logic model, to exclude fatal states and to guarantee a failure safe behaviour in the limits of the defined safety system functionality

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 Levels for a dedicated safety soft- and hardware. The manufacturers of safety components supply product safety data libraries within the framework of standard ISO-13849 1-2 and EN/IEC 62061. The quantification of safety system PL has to be provided for future ANKA-beamlines to receive operation license by the certifying body.

REFERENCES

[1] M. Hauke et al, "Funktional safety of machine controls ",BGIA Report 2/2008e, http://www.dguv.de/ifa/Publikationen/Reports-Download/BGIA-Reports-2007-bis-2008/BGIA-Report-2-2008/index-2.jsp

[2] M. Brinkmann, "SafetyBUSp–the first safe fieldbus system – CAN in automation", http://www.can-cia.org/fileadmin/cia/files/icc/7/brinkmann.pdf

[3] Cerff, K. H. and Mexner, W., "An investigation of different data buses at ANKA and their influence on the performance of the ANKA con-trol systems, PCaPAC, March 22-25, 2005, Soken-dai, Hayama, Japan.

[4] J. Börcsök, "Functional Safety: Basic Principles of Safety-Related Systems", Hüthig 2007, ISBN-10: 3778529862.

[5] C.G. Cassandras and S. Lafortune, "Introduction to Discrete Event Systems ", Springer 2008, p. 55f.

[6] Software-Assistant, SISTEMA, Safety Integrity http://www.dguv.de/ifa/en/pra/software/sistema/index.jsp

[7] PILZ, PAScal Safety Calculator, http://www.pilz.com/enUS/eshop/00013000497038/PAScal-Safety-Calculator

[#] Inst. F. Occupatioanl Safety and Health of the German Social Accident Insurance, St. Augustin

ISBN 978-3-95450-139-7