REVIEW OF RELIABILITY CONCEPTS APPLIED TO BEAM LOSS MONITORING SYSTEMS

Bernd Dehning, CERN, Geneva, Switzerland

Abstract

Beam loss measurement systems are often used for the protection of equipment against the damage caused by impacting particles creating secondary showers and their energy dissipation in the matter. Depending on the acceptable consequences and the frequency of particle impact events on equipment reliability requirements are scaled accordingly. Increasing reliability often leads to more complex systems. The downside of complexity is a reduction of availability, therefore an optimum has to be found for these conflicting requirements. A detailed review of selected concepts and solutions from real-life examples will be given to show approaches used in various parts of the system from the sensors, signal processing, and software implementations up to the requirements for operation and documentation.

SAFETY SYSTEM DESIGN APPROACH

All considerations start with the recognition that the probable frequency and probable magnitude of a non conformal behaviour could lead to a damage of the system integrity. The combined likelihood of frequency and magnitude determines the risk for a certain system (see Fig. 1, first column). A reduction of the risk could be reached with a safety system providing protection, but larger complexity reduces the availability of the protected system (see Fig. 1, first row). To come to a quantitative demand for a safety level the probable frequency of events and probable magnitude of its consequence are used by the SIL (Safety Integrity Level) approach [1] or by the As Low As Reasonably Practicable (ALARP) approach. For both approaches

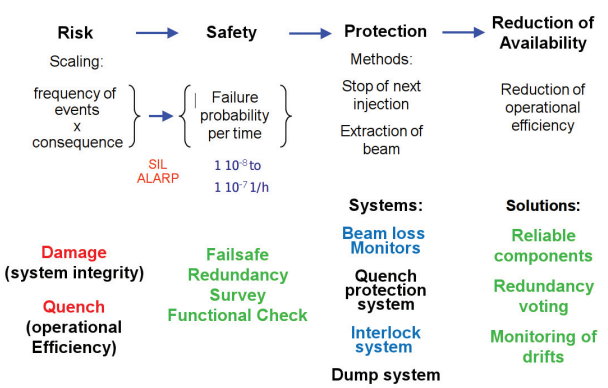

Figure 1: Schematic of the LHC protection system design approach (items in green are discussed in this paper).

a failure probability per time is estimated by the calculation of the risk of a damage and the resulting down time

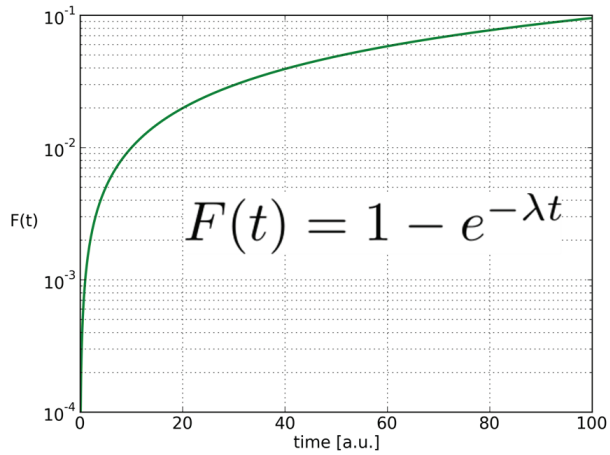

Figure 2: Exponential failure probability.

of the equipment [2]. In the case of a failure in the safety system itself, it should fall in a failsafe state with the consequence of reducing the operation efficiency. The main design criteria for the safety system are listed in the safety column: failsafe, redundancy, survey, functional check. In the protection column the methods for the protection of an accelerator are listed: stop of next injection applicable for a one path particle guiding system (linac, transfer line) and extraction of the beam for a multi path system (storage ring). The accelerator safety system is consisting of a beam loss measurement system, an interlock system and a beam dump system. If superconducting magnets are used, some beam loss protection could also be provided by the quench protection system. The availability column lists the means used in the design of the safety system to decrease the number of transitions of the system into the failsafe state. The effect of the number components added to a system to increase the probability of a safe operation results in a reduction of the availability of the system. This negative consequence of the safety increasing elements are partially compensated by the choice of reliable components, by redundancy, voting and the monitoring of drifts of the safety system parameters.

FAILURE PROBABILITY AND FAILURE RATE REDUCTION

To illustrate the available means to increase the safety of systems basic functional dependencies are discussed. A often valid assumption is given by the exponential time dependence of the failure probability $F(t)$ (see Fig. 2). With increasing time the probability of the occurrence of a failure in a system approaches 1. The failure rate λ is assumed

ISBN 978-3-95450-119-9

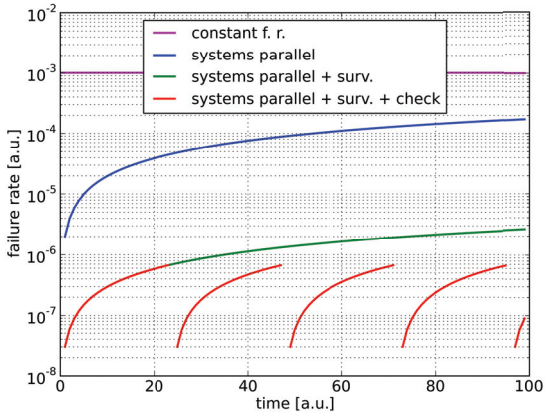

Figure 3: Failure rates of different systems as function of time (arbitrary units).

to be time independent (see Fig. 3, magenta curve). In a next step two systems with the same functionality are assumed working in parallel to allow a redundant operation. The failure rate λ decreases drastically for short times, but approaches finally the failure rate from a single system (see Fig. 3, blue line). It should be noted that the failure rate curve changed from the time independent to a time dependent behaviour. A further reduction of the failure rate could be reached by a survey of the system. With a survey of a system some failure modes could be detected in advance and a repair can be planned (see Fig. 3, red-green line). This procedure results in a shift of the failure rate curve to lower values not approaching any more for infinite times the single system rate. Another strong reduction could be reached if the system could be regarded as new after a certain time period. The failure rate curve shows the time dependence of the surveyed system in the period $t_0 = 0$ to $t = t_1$ repeated after every time period (see Fig. 3, red lines). The conclusion that a system could be regarded as new after a certain time is justified if the system is subjected to a test. Functional tests will verify that the system has the defined functionality on request. In the case of an internal failure of a system the very basic requirement is a failsafe behaviour. Internal failure will will not contribute to the un-safety of the system but contribute to the non availability.

PROTECTION SYSTEM OVERVIEW

As an example for a protection system the CERN LHC beam loss monitoring (BLM) system will be used. The system will be discussed from a viewpoint focusing on the protection, reliability and availability aspects.

The main purpose of the BLM system is the conversion of particle shower informations in electrical signals and comparing them with limits. In case that limits are exceeded the extraction of the LHC beam from the ring is initiated to stop the irradiation of equipment. In the case of LHC the protection function is often linked to the quench prevention of the superconducting magnets since the threshold levels for beam extraction are lower (orders of magnitude) as for the damage protection of equipment [3].

The very first element of the protection system is the sensor detecting the irradiation of equipment. The conversion of the particle shower magnitude is done by ionisation chambers [4] or secondary emission detectors [5] (see Fig. 4, left block). The front-end acquisition electronics converts the analogue detector signal in a digital and transmits the signal to the back-end and control unit. The

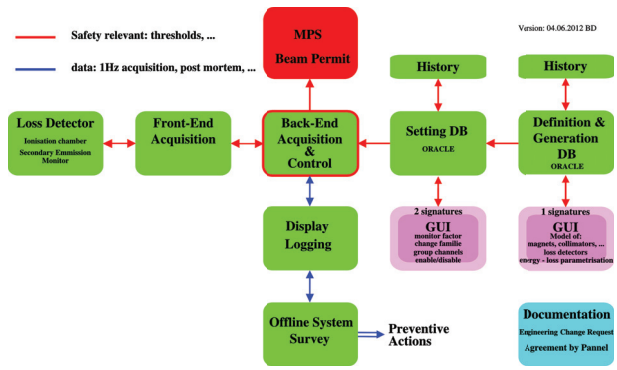

Figure 4: Schematic of system emphasising the information flow from the sensor up to the beam permit signal transmission. The red framed (Back-End Acquisition & Control) unit is the local decision making centre.

back-end and control unit is the decision making centre of the whole system. The measured signals arrive here and are compared with the limits. In addition the beam permit signals are generated (see Fig. 4, red block) taking the information of the system settings (see Fig. 4, right blocks) into account. The measurement data and all setting informations are distributed to the display and the logging data bases (see Fig. 4, bottom blocks) from this unit too. The control functionality is linked to the survey and test functionality discussed below.

In the LHC case ionisation chambers [4] and secondary emission detectors [5] are used. Their signals is digitised with a current to frequency converter [6, 7] (see Fig. 5, front-end acquisition in tunnel). Up to the end of the analogue signal chain the signal is not redundant, because no technical solution has been found splitting the detector signal and at the same time allowing a large dynamic of the signal (9 orders of magnitude). To cope with this requirement for the analogue front-end a low failure rate circuit concept has been chosen. To avoid the consequences of single event effects and to increase the availability of a channel the signal is triplet in the front-end logic. Two voting blocks are used to generate the signal transmitted over a redundant optical link. A redundant optical link has been chosen to increase the availability of the link, which is limited by the MTBF of the transmission LASER. The signals are decoded and cyclic redundancy checks (CRC) are calculated for both signal chains (see Fig. 5, back-end acquisition at the surface). At the front-end CRCs are also

ISBN 978-3-95450-119-9

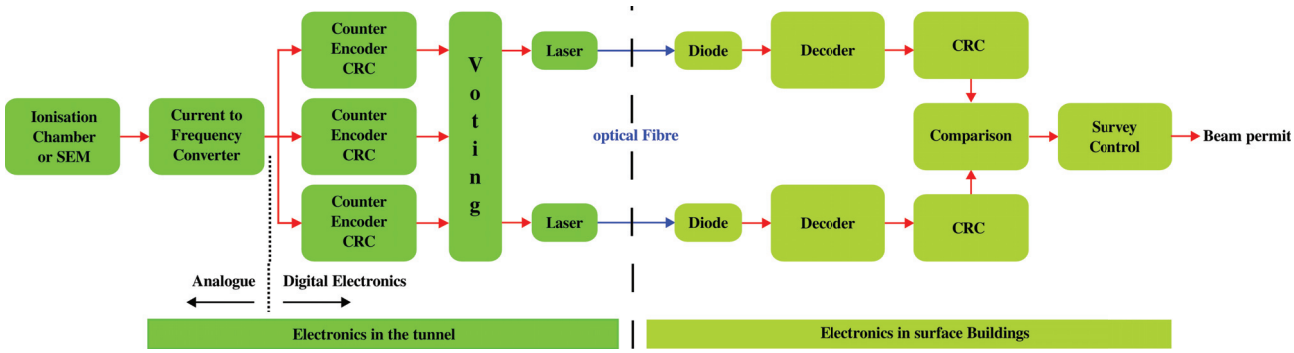

Figure 5: Schematic of the CERN LHC beam loss measurement and protection system.

calculated and transmitted to be able to compare the CRCs of each line and also the CRCs for both lines. This procedure ensures a high reliability and also maximises the availability of the data link [8, 9]. The effect of the implementation of redundancy and tripling in the data transmission and treatment and the verification of loss free data transmission (CRC) are listed in table 1. The most important technique to increase the reliability of a system is given by an failsafe design. In the case of an internal failure of a system it should make the transition to a state which ensures the protection of the system. This could be done by assigning the active state to: system is allowed to operate. In case of an internal failure e.g. no power is supplied the state will switch to a passive state and the system is protected.

Table 1: Procedure and Techniques with the Potential to Increase the Reliability and Availability of Acquisition Systems

	Comment position of monitor	Safety gain	Availably gain
Failsafe	active state = beam permit	yes	no
Voting		yes	yes
Redundancy		yes	yes
CRC	Cyclic redundancy check	yes	no

FAULT TREE ANALYSIS

The fault tree treatment of the system has been chosen to calculate from the component level up to the system level the damage risk, the false alarm and the warning probability [10]. Taking into account the component failure, the repair and the inspection rate. The false alarm slice of the fault tree (see Fig. 6) shows the signal chain for different false alarm generators (memory, beam energy from control unit (combiner) and energy transceiver) of back-end electronics [11]. The different inputs are linked together with a boolean "OR" so that every single input generates in the same way a false alarm and therefore a down time of the system and the LHC. The results of the fault tree analysis have been essential for the design of the hardware and the software, especially for the estimates of failure rates of the optical links and the propagated consequences of it up to the system damage and false rate probabilities. An optimisation process has been done to balance the probabilities of damage rate and false alarms. The failure rate calculations lead also to the definition of functional tests and their frequency. Failure modes are also defined for the limit values, detector names, channel assignments and many more information needed by the system. Therefore the setting management and the meta data verification tests are also treated in the fault tree analysis.

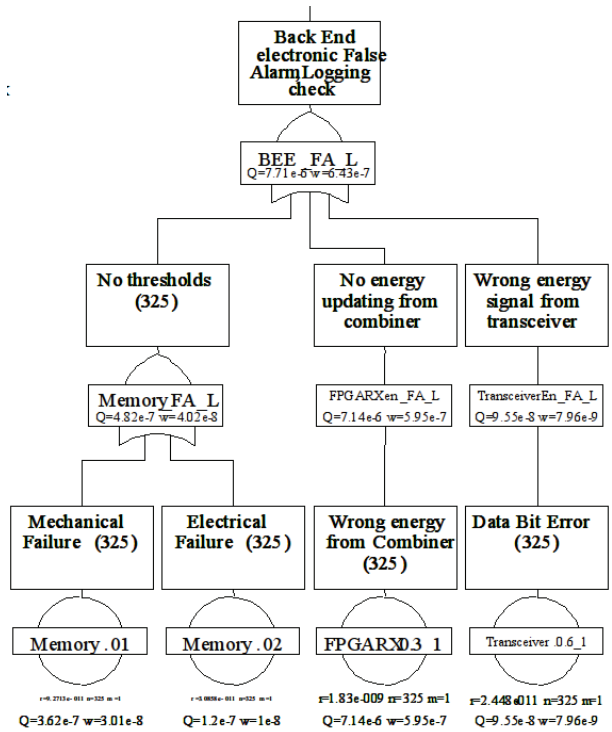

Figure 6: Image section of the false alarm generation fault tree of the LHC BLM system. The part describing the Back-End acquisition is shown.

FUNCTIONALITY CHECKS

As an example for a check the signal distribution inside the VME crate for the beam energy and the beam permit line test is discussed [12, 13] (see Fig. 7). The initiation of the test is done by a client to allow an optimal scheduling for it. The control unit (combiner card) holds a down time counter requiring every 24 hours the execution of func-

ISBN 978-3-95450-119-9

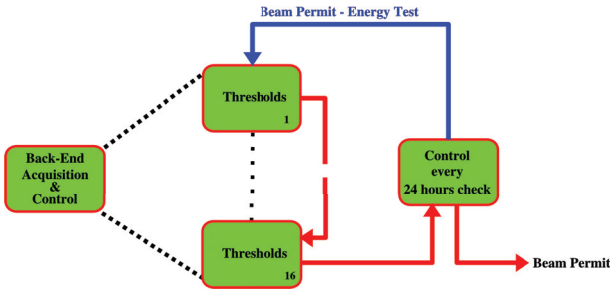

Figure 7: Beam permit line functionality check.

tional tests. If the tests are not done in time it inhibits the beam permit immediately if no beam is circulating or when the beam present flag becomes false. For the tests the whole system is changing the status to "test mode" and e.g. the control units send to each acquisition card (threshold card) in sequence the request to inhibit the beam permit line (see Fig. 7). The results of the tests are analysed by the controller and in case a false status is detected a manual intervention is needed to repair the system before the test could be passed without a false status detected. The distribution of the beam energy levels between the controller and the acquisition card is tested by changing the energy levels in the test mode which should result in an action of the acquisition card sending back the appropriate threshold settings for comparison with the settings sent.

In a second example the test of the whole acquisition chain is presented [14, 15]. An electrical signal is introduced in the sensor by the capacitive coupling of the sensor electrodes and by a harmonic modulation of the applied high voltage supply (see Fig. 8). This test includes the complete signal chain except the ionisation process in the ionisation chambers or the secondary electron emission in the SEM detectors. The particle shower conversion to an electrical signal process in the detector is tested every few years with a radiative source placed on the outside of the detector. The long time span for this test is possible, because the failure mode of a complete gas exchange with air (ionisation chamber) or loss of the vacuum (secondary emission detector) of the detectors will still result in an appropriate signal not losing the protection functionality. Also this test is initiated and the results are analysed by the back-end unit (survey and control) (see Fig. 8) allowing in the case of a negative result to inhibit directly the beam permit line.

SETTING MANAGEMENT

The system setting management includes the settings for the beam permit thresholds and also settings used for the operation of the system [16, 17]. These operational settings include hard and firmware informations to verify that the configuration stored in the data base images the installed system (see table 2). The table illustrates the variety of the meta data needed for the interpretation of the measured values or to check the configuration of the system. E.g. the match between measured value, channel Official Names,

Table 2: Parameters Deployed on each Back-End Unit (threshold comparator module)

Parameters	Data 32bit	Description
Threshold Values	8192	16 channels x 12 Sums x 32 Energies
Channel Connected	1	generating or not a beam permit
ChannelMask	1	"MASKABLE"/"UNMASKABLE"
Serial A	1	Cards Serial Number (channels 1-8)
Serial B	1	Cards Serial Number (channels 9-16)
Serial	2	Threshold Comparators
Firmware Version	1	Threshold Comparators Firmware
Expert Names	128	
Official Names	128	
DCUM	16	position of monitor
Family Names	128	Threshold Family Name
Monitor Coefficients	16	Monitor Threshold Coefficients
Last LSA update	2	Timestamp: MASTER table
Last Flash update	2	Timestamp: non volatile memory
Flash Checksum	1	CRC value for/from table integrity.

channel Expert Names, DCUM (position of monitor) and monitor coefficient needs to be given and tested. To reduce the complexity of the meta data information chain (see Fig. 4, right blocks) a single path is defined for the meta data flow joint with the measurement data in the back-end unit. The back-end unit distributes the measurement values together with the meta data to ensure its consistency and to have only one location where the data integrity need to be tested. This concept is essential to reduce the number of possible failure modes for meta data corruption.

Having expressed the importance of a failure mode optimised meta data flow the check of the data is done by the comparison of the data stored in a reference setting data base (Oracle) and the memories of the back-end electronics FPGAs (see Fig. 9). Also for this test a down time counter located in the back-end unit (survey and control) request all 24 hours a comparison of the data stored at both locations. If the test is not initiated or the result of it is negative the beam permit is inhibited. Since the comparison is done in a different software environment the additional functionality required in the back-end unit is marginal, but it is required to test the comparison code from time to time.

Descriptive Metadata

Meta data need to be generated and the option for required changes needs to be provided. To reduce the failure modes of human beings the graphical user interfaces (GUI) accessing the setting data base (see Fig. 4, right block) needs to be optimised by allowing for all data manipulation steps comparisons with previous data, for number changes check on the magnitude of the changes and several confirmation steps. The last confirmation steps request the electronic signature of two independent persons. The generation of sets of meta data required initially and for larger changes during the operation periods is for the LHC system done by a GUI for the data base access. The meta data generation like limits for the beam abort thresholds are parametrised and the calculation is done by code loaded into the data base (Oracle) (see Fig. 4, most right block). The calculation done in the data base environment

ISBN 978-3-95450-119-9

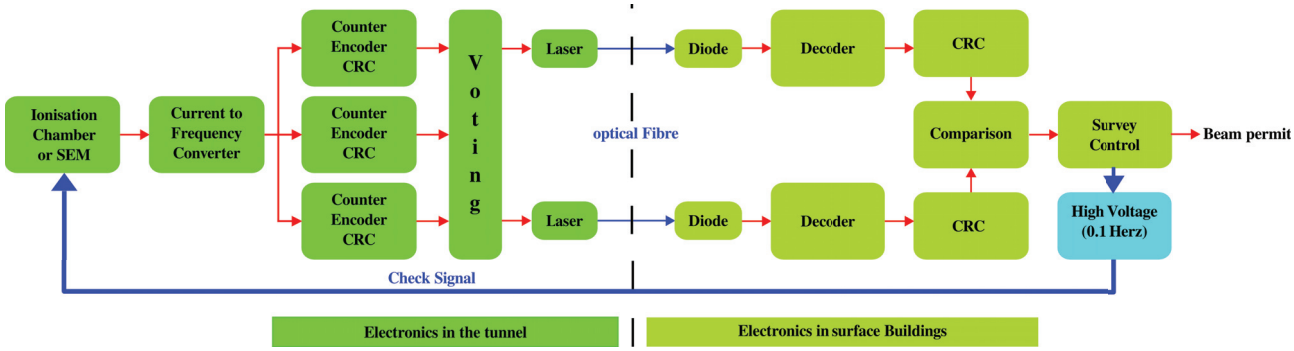

Figure 8: Check of the whole acquisition chain.

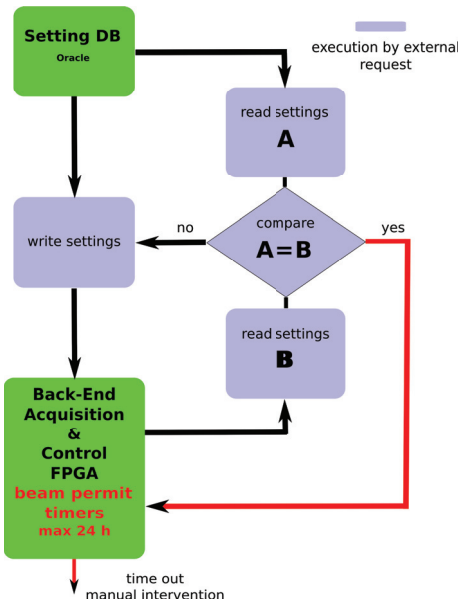

Figure 9: Comparisons of descriptive meta data base reference settings with settings in the back-end acquisition and control unit. In the flow diagram indicated is the decision logic.

where data base software changes and updates are done in a coherent manner should ensure the long time maintainability [18].

Documentation

In a complex system foreseen for an operation over decades the documentation is essential to describe the system for the transfer of knowledge. For a safety system the function of the documentation extends in the direction of avoiding failure modes and failures. The documentation of the design starting with the specification up to the documentation for the operation and changes to the system needs to be distributed to the clients that they could be commented and finally agreed by each of them. At the LHC standardized forms, electronic procedures and signatures are in use to organise the process, e.g. an engineering change request (ECR) is requesting the description of the motivation for a change, the description of the proposed change and an estimate of the impact of the change onto the functionality of the concerned system and onto other systems.

SNAPSHOTS OF LOSS MEASUREMENTS TRIGGERED BY EVENTS

The loss measurement recording rate has been set up with different speeds 40 μs, 80 μs, 80 ms and 1.3 s integration times. The two first periods are event triggered to cope with the amount of data and the later are read out with 12 Hz and 1 Hz. The event triggered measurements are used to analyse losses occurring at particular times during the operation or depending on measurements and the analysis data acquisition freezing events are sent out. The 12 Hz measurements are used for the collimator positioning feedback system and the 1 Hz measurements are used for he continuous observation of the accelerator status. High res-

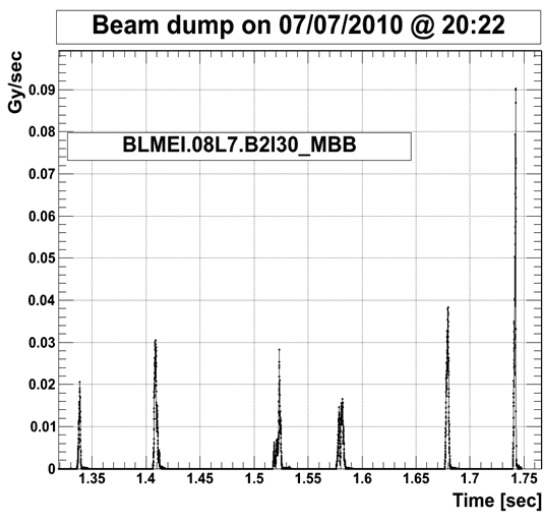

Figure 10: Example of a particle loss triggered event recording. The trigger has been generated at 1.74 s. The measurements recorded before the trigger event revealed loss precursors. The losses are caused by collisions between the beam and dust particles.

ISBN 978-3-95450-119-9

olution data have not only been used for the detailed study of beam losses caused by dust events (see Fig. 10), but also for the check of nonconformities of the acquisition system. The test of the system under extreme condition, high loss levels with a large leading signal transition reveals an insight in the system performance. The advantage of having different measurement signal published is given by the option of executing consistency checks. In the case of the LHC even several clients checked the consistency of measurement data.

ACQUISITION DATA BASE

The measurement and meta data storage and the fast retrieval of it is also essential for the check of the system. Beyond the example discussed in the previous section requiring an extended data storage an extreme case is the check of the noise amplitudes of the system (see Fig. 11). For an protection system with limits leading automatically to a beam abort and to down time of the accelerator avoiding false aborts caused by rare events (noise) is a strong requirement. It is extreme, because rare signals need to be retrieved reading the stored measurement data from acquisition periods lasting weeks. The measurements with the shortest integration periods 40 μs show the largest signal fluctuation, because the signal averaging is not leading to a reduction of it. To reduce the amount of data to be stored an on-line measurement data reduction algorithm has been implemented in the back-end unit. Only maximum values of the short integration times are stored for the 1 Hz read out. This procedure reduces the data to be stored already by over 4 orders of magnitude. In addition a retrieval time optimised data base structure has been implemented for this purpose.

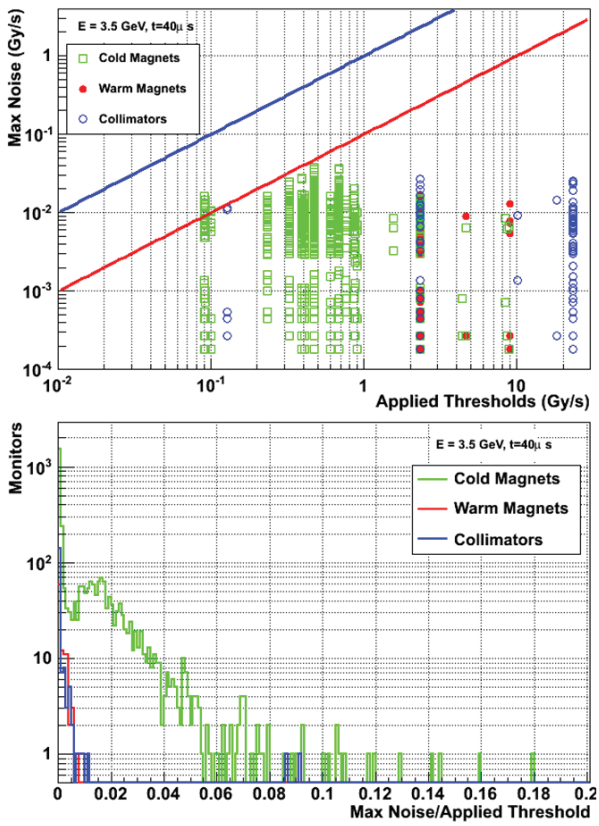

Figure 11: Noise level determination of all beam loss monitor channels. The LHC loss monitor channels are grouped by the observed loss creating elements cold and warm magnets and collimators. Top: Beam loss monitor noise signal taken during a duration with no beam circulating versus beam abort thresholds. The blue line indicates the threshold value and the read line the maximum noise goal set to avoid any noise false beam aborts. Bottom: Beam loss monitor spectrum normalised to the beam abort threshold.

PREVENTIVE ACTION

The discussion in the section: "FAILURE PROBABILITY AND FAILURE RATE REDUCTION" was emphasizing the reduction in failure rate by the survey of the system to recognise possible failure modes in advance. In the LHC system the survey task is realised by daily retrieval of relevant data base informations and an automatic comparison with limits for initiating actions. Reports are produced daily and weekly containing a different level of abstraction. An example of this procedure is given by the survey of the optical links. The links are redundant (see Fig. 5) and the calculations of different cyclic redundant checks (CRCs) open the options of the recording of differences between the CRC values and correlating it with board temperature variations (see Fig. 12). The limits for actions are set empirically to minimize the down time and the maintenance efforts needed.

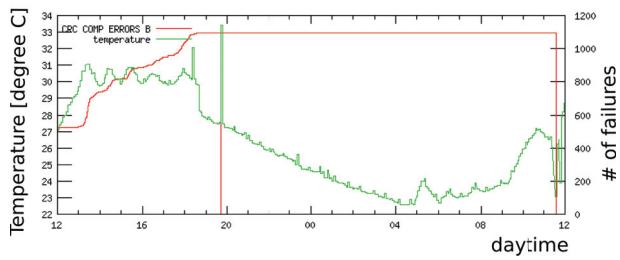

Figure 12: Optical link failures and printed circuit board temperatures versus daytime.

SUMMARY

A systematic design approach will start with the determination of the system failure rate. The failure rate magnitude could be based on well established standards first developed for the design of military equipment, by the air plane industry, for space missions and for nuclear power stations. The effect of increasing complexity by adding protection functionalities and therefore reducing the availability is best studied by reliability software packages [19]. The basic means of a reduction in failure rate are given by

ISBN 978-3-95450-119-9

a system layout with parallel, redundant information treatment in combination with a regular survey of the system status and functional test. A survey will open the option of preventive actions to reduce the failure rate. For a protection system a failsafe design is essential that in the case of a failure the protection is ensured.

Functionality checks staged for all levels of the signal treatment are implemented for the LHC BLM system. The checks of the information exchange inside the VME crate and the analogue and digital signal chain have been discussed. Examples have been given to emphasise the importance of the meta data information flow. The combination of measurement and meta data as early as possible in the signal chain is important for the reduction of failure modes and simplified test options. To reach low level failure rates rigorous tests have to be implemented to ensure the meta data conformity. The meta data generation and change options using a graphical interfaces need also to be analysed in terms of failure modes taking into account the maintainability in the future. For the LHC case the most stringent requirement for avoiding human being errors is the request of two signatures for validating meta data changes. Although listed last the documentation tasks should be started first including the planning for the reliability means and have to be continued as long as the system is alive.

REFERENCES

[1] IEC SC (Subcommittee) 65 A. *IEC 61508 International Standard*. IEC, 2010.

[2] G. Guaglio. Reliability of beam loss monitors system for the large hadron collider. In *11th Beam Instrumentation Workshop (BIW 04), Knoxville*, volume 732, pages 141–149. AIP, 2004.

[3] B. Dehning, M. Dabrowski, A. Marsili, C. Zamantzas, G. Kruk, A. Nordt, V. Grishin, M. Sapinski, E. Nebot Del Busto, E. B. Holzer, E. Fadakis, E. Griesmayer, J. Emery, C. Roderick, E. Effinger, S. Jackson, M. Misiowiec, C. Kurfuerst, and A. Priebe. Overview of LHC beam loss measurements. https://cds.cern.ch/record/1379469, September 2011.

[4] M. Stockner and Christian Wolfgang Fabjan. *Beam Loss Calibration Studies for High Energy Proton Accelerators*. PhD thesis, Vienna Tech. University, 2006.

[5] Daniel Kramer, Bernd Dehning, and Miroslav Sulc. *Design and Implementation of a Detector for High Flux Mixed Radiation Fields*. PhD thesis, Liberec Tech. University, 2008.

[6] E. Effinger, B. Dehning, J. Emery, G. Ferioli, G. Gauglio, and C. Zamantzas. The LHC beam loss monitoring system's data acquisition card, 2006.

[7] E. Effinger, B. Dehning, J. Emery, G. Ferioli, and C. Zamantzas. Single gain radiation tolerant LHC beam loss acquisition card, 2007.

[8] C. Zamantzas, B. Dehning, E. Effinger, J. Emery, and G. Ferioli. An FPGA based implementation for real-time processing of the LHC beam loss monitoring system's data, 2006.

[9] C. Zamantzas, C. Da Vi, and B. Dehning. *The Real-Time Data Analysis and Decision System for Particle Flux Detection in the LHC Accelerator at CERN*. PhD thesis, Brunel University, 2006.

[10] G. Guaglio. *Reliability of the beam loss monitors system for the Large Hadron Collider at CERN*. PhD thesis, Univ. Clermont-Ferrand 2 Blaise Pascal, 2005.

[11] Reliability software from isograph - world leaders in reliability, maintenance and safety. http://www.isograph-software.com

[12] C. Zamantzas, C. F. Hajdu, S. Jackson, and B. Dehning. Reliability tests of the LHC beam loss monitoring FPGA firmware. https://cds.cern.ch/record/1268403, May 2010.

[13] B. Dehning, E. Effinger, A. Nordt, C. Zamantzas, and J. Emery. Self testing functionality of the LHC BLM system. https://cds.cern.ch/record/1375171, May 2011.

[14] J. Emery, E. Effinger, A. Nordt, M. G. Sapinski, C. Zamantzas, and B. Dehning. First experiences with the LHC BLM sanity checks. https://cds.cern.ch/record/1321592.

[15] J. Emery, E. Verhagen, B. Dehning, E. Effinger, C. Zamantzas, G. Ferioli, and H. Ikeda. LHC BLM single channel connectivity test using the standard installation. https://cds.cern.ch/record/1183414, May 2009.

[16] E. Nebot Del Busto, G. Kruk, A. Nordt, C. Roderick, M. Sapinski, M. Nemcic, A. Orecka, E. B. Holzer, S. Jackson, B. Dehning, C. Zamantzas, and A. Skaugen. Handling of BLM abort thresholds in the LHC. https://cds.cern.ch/record/1379461, September 2011.

[17] E. B. Holzer, M. Sapinski, T. T. Boehlen, L. Ponce, Daniel Kramer, M. Stockner, B. Dehning, D. Bocian, and A. Priebe. Generation of 1.5 million beam loss threshold values. https://cds.cern.ch/record/1124306, September 2008.

[18] Martin Nemcic. Calculation of abort thresholds for the beam loss monitoring system of the large hadron collider at cern. http://ab-div-bdi-bl-blm.web.cern.ch/ab-div-bdi-bl-blm/talks_and_papers/Nemcic, 2012.

[19] Sampriti Bhattacharyya. *Reliability Analysis and Controls for Accelerator Driven Systems Based On Project X*. PhD thesis, Ohio State University, 2012.

ISBN 978-3-95450-119-9