FAIR Commissioning & Control Working Group

Notes from the meeting held on the 21st October 2015

e-mail distribution: FAIR-C2WG-ALL at GSI.de, participants list

Agenda:

- High-Intensity Operation: Between Poka-Yoke and Machine Protection (jump below), C. Omet
- Fast Beam Abort System (jump below), M. Mandaković
- AOB

1. High-Intensity Operation: Between Poka-Yoke and Machine Protection, C. Omet

In his presentation (see link), Carsten Omet provided an overview and systematic analysis of the SIS100 machine protection system. The concept covers a wide range from soft operator or control system failures (i.e. Poka-Yoke) to fast beam abort scenarios that could damage part of the machine (i.e. machine protection).

C. Omet formalised the terminology of 'hazard' being a situation that poses a level of threat to the accelerator, that are dormant or potential, with only a theoretical risk or damage; and 'incident/accident' once a 'hazard' becomes 'active'. The product of consequences and probability of the incident create a 'risk', where a given amount of 'risk' needs to be counter-balanced by appropriate technical measures mitigating the risk. C. Omet provided several 'risk' evaluation examples using known incidents at LHC, SPS and J-PARC.

Risk is not a threshold effect but a continuous gradient, and depending on the level of risk and time-scales the appropriate mitigations (see slide 11 for details) range from:

- hard machine protection mitigated by the FAIR machine and system design (e.g. through passive absorbers, machine optics, material choices)
- quench prevention, mitigated, for example, by using BLMs triggering a Fast Beam Abort System before the losses reach the critical quench threshold,
- minimisation of machine activation (ALARA principle), and
- 'Mistake Proofing' or 'Poka-Yoke' that consist of intercepting common mistakes, procedural errors, etc. that may affect the machine performance mitigated by settings monitoring, automated sequencer, operational procedures etc.

C. Omet explains, that 'Poka-Yoke' (jap. For: to avoid [yokeru] inadvertent errors [poka]) or 'mistake proofing' is a commonly used concept in the industry for quality insurance and to improve overall production quality (see: 'Toyota Production System'). The aim of this concept is to “eliminate product defects by preventing, correcting, or drawing attention to human errors as they occur”[1].

1see e.g. https://en.wikipedia.org/wiki/Poka-yoke

The concept is intertwined with the machine and system design, active protection, and procedural protection through, for example, the beam-presence-flag, management of critical settings and intensity ramp-up concept discussed in an earlier FC^{2}WG meeting (see Meeting #3 and slides for reference).

C. Omet highlighted that until now, most of the SIS18 devices are designed to self-protect when internal failures occur, but do not necessarily have an optimum behaviour with respect to the beam as the impact on the beam or rest of the machine could be more severe than to the self-protecting device alone. Thus the new paradigm targeted for FAIR and SIS100 consist of: 1. Avoid that a specific failure can happen; 2. Detect failure at hardware level and stop beam operation; 3. Detect initial failure using for example beam instrumentation. In case an error is detected, some of the possible responses are inhibiting further injection, extracting the beam into the emergency beam dump, or stopping the beam using beam absorbers or collimators.

C. Omet identified the melting of the epoxies commonly used in the insulation of the magnet wiring, as one of the most vulnerable items. Early estimates indicate that beam U^{28+} intensities below $3 \cdot 10^{10}$ particles per cycle could probably be considered as safe w.r.t. epoxies ($\leftrightarrow$ melting temperature of about 422 K). 'Set-up' or 'pilot beams' should thus ideally be at half or a quarter of that intensity. Two other noteworthy critical devices are the electro-static extraction septa that may be destroyed by the circulating primary beam impacting the wires, and the SIS100 emergency dump.

In second part of his presentation, C. Omet presented the result of his Failure Modes and Effects Analysis (FMEA) that was performed on the system level of SIS100. The aim was to identify machine failures according to the IEC 61508 standard. He used standardised values for the assessment of severity for personnel safety, and mapped these qualitatively for assessing the severity of machine protection. Only single uncorrelated (i.e. not combined) errors were considered to reduce the initial complexity (see slides for details).

Concerning the detailed FMEA analysis, C. Omet highlighted the major risk contributors and how these could be mitigated, grouping them into 'magnets, bus-bars, and current leads', 'power converters', 'RF acceleration system', 'injection and extraction system', 'global and local cryogenic system', 'control system' (including also operational mistakes), and 'beam dynamics and others'. The major failure contributors in absolute numbers without weighing their severity or their failure-recovery-times are: 'cavity gap arc ignition (~2000 events/a)', 'electro-static septum sparking (6000 events/a)', and 'operator failures/wrong data delivered to device (5000 events/a)'. Some of the most severe failures that are hard to detect at warm temperatures and that imply long repair times are cold leaks and defects in the cryo system.

By the proposed fail-safe concept, up to 85% of the total failures could be detected or mitigated by the proposed surveillance. Work is progressing to improve this. Assuming 6000 operating hours per year, and the assumed failure recovery times, C. Omet's estimates presently an initial machine availability for beam of 66% for SIS100.

Discussion:

F. Hagenbuck commented that the uncontrolled loss scenario mentioned in slide 16 are already larger than those allowed by radiation protection. C. Omet explained that the 3% radiation limits are tolerances given for 'prompt losses' not for systematic losses leading to activation. The actual losses need to be kept much lower in order to minimise activation and suppress dynamic vacuum effects.

H. Weick – in response to cases similar to the JPARC accident – asked whether there are measures planned for direct protection against similar slow extraction spikes at SIS100. C. Omet commented that these failures were due to a data supply and power converter supervision problem. For FAIR it is foreseen that all power converters detect these faults internally by comparing the actual and set reference values. In addition, part of these failures are also detected by the 'set-up-beam' and 'intensity ramp-up' concept that forces a pilot beam prior to a high-intensity beam being injected into or out of a machine.

R. Steinhagen highlighted that this analysis covers only SIS100 and not other parts of the facility. In the short-term, the individual experiments and MPLs should evaluate whether they need to add additional passive protection (e.g. absorber, collimator blocks) into their design, and in the long-term whether their machines need an active single or multiple inputs to the SIS100 Fast-Abort-System to suppress the 'extraction permit' to their target or experimental hall. CSCO would need this information to know if they need to also provide a fast abort system for other FAIR accelerators or experiments or whether these can self-protect themselves by passive means. R. Steinhagen further asked about the required lead times for the active systems and when the information would need to be provided to CSCO. M. Mandaković expressed that this input should be given as soon as possible. C. Omet recommended that this should be done before ordering sensitive components (showing systematic approach for different components in spreadsheet).

R. Steinhagen emphasized that the experiments should evaluate: 1. whether there are simple means that can self-protect themselves; and 2. the impact a destroyed target (for example), its probability and the consequences for replacing that target. D. Ondreka pointed out that Super-FRS may need input on what could go wrong (i.e. primary beam failure scenarios). For example, the probability of such failures and amount of intensity being extracted within 10/100 turns or a few milliseconds.

H. Weick asked whether redundant DCCT should be considered for added safety. C. Omet affirmed this, and mentioned that these were initially foreseen for all power converters but was considered to be too costly. Now only the most critical magnets (e.g. dipoles, fast quadrupole magnets) are equipped with this redundancy. H. Weick commented that this assessment may need to be re-evaluated also taking the consequences from an experimental point of view into account.

F. Hagenbuck asked about how much time is needed for such a S-FMEA analysis. C. Omet replied that he gathered the data (via multiple discussions) over about a year but estimates that the net amount of time was about four weeks.

2. Fast Beam Abort System, M. Mandaković

In his presentations (see link), Marko Mandaković provided a short summary of the active machine protection concepts and strategies, notably the Fast Beam Abort System (FBAS) that will be deployed for the of SIS100.

Initially, the primary aim of the FBAS was to protect only SIS100. However, it is being planned to use and extend the concept with a similar system to also protect subsequent accelerators or experiments. The individual equipment that have been identified by C. Omet's analysis as 'critical' are required to monitor their state and emit a machine protection signal (MPS) in case a relevant equipment failure or another inappropriate equipment state is detected. The MPS propagates these signals by a proprietary net and combines them with other machine states or operator settings. These signals must be processed in real-time to ensure the timeliness of the triggered actions. Some of the possible trigger actions are an emergency beam dump, magnet shut-down of magnets or to inhibit of further beam injection or extractions.

M. Mandaković explained that the SIS100 MPS distinguishes four classes of reaction times: class 0 – with no possibility of active reaction (implies to be handled through passive protection, or redundancy in the equipment); class 1 – requiring a very fast beam abort within about 40 us; class 2 – requiring a fast beam abort within 1-5 ms and subsequent FBAS trigger; class 3 – with slow reaction times within 100 ms being acceptable. The latter system is historically referred to at GSI as 'Interlock System' while technically FBAS is also an interlock system. (N.B. the 'dump of magnet energy' mentioned in slide 6 is optional and required only if a magnet has actually quenched. In any case this assessment will be done by the quench detection system).

The FBAS will need to define certain requirements on the equipment connecting to the MPS in order to achieve the required latencies and function. For example, while the self-protection of the equipment is outside the scope of the FBAS, it is required that the equipment issues first the beam abort signal and only then enters into a safe equipment state. The required delay is about 50 us. Out of the 50 us total latency, 40 us are required due to kicker synchronisation and cable delays. Further, as an interface requirement, equipment are required to provide both a fast electrical and fast optical return signal to the MPS as well as MPS qualification signals into the equipment to boot-strap and test the MPS's individual inputs (e.g. masking or forcing of MPS input channels on the equipment side etc.). Some of the interfaces and requirements are being described and defined in:

F-TG-C-05e-Control-System-Equipment-MPS-Interface (fast interface),

F-TC-C-02e-SIS100_fast_beam_abort_system_requirements,

F-TC-C-03e-SIS100_fast_beam_abort_system_concept,

F-TG-C-03e-Control-System-Equipment-Interlock-and-Status-Signal-Interface-v3.0, and

M. Mandaković pointed out that the following items need to be further addressed and discussed:

- Latency (600 us) of the slow interlock to the data master.
- As a proposal, the Timing System's return channel could be used to provide an alternate option for a faster than 100 ms but slower than 50 us reaction times. This would allow the majority of FAIR equipment that has a timing system to be included into the fast interlock supervision. It would need to be discussed whether a latency of about 10 ms is acceptable for most purposes (N.B. the initial estimate was 1-2 ms).
- Watch-dog functionality (stay-alive checks) for device connection to timing system would need to be discussed and whether an update rate of, for example, 100 ms is acceptable.
- The risk analysis as done for SIS100 (see previous talk) is also needed for the other machines and experiments to assess whether these need to be included into the FBAS or similar systems.
- Procedures for the FBAS qualification tests.
- Procedure for BLM threshold training.

Discussion:

D. Ondreka commented that primary functionality of the MPS should not be mingled with diagnostic functionality such as 'post mortem'. Not having a post-mortem system may have the disadvantages of not finding the cause of a dump but the MPS will work without it. R. Steinhagen commented that the 'post mortem' is a hard requirement to qualify that the MPS worked 'as good as new' or 'as designed'. The post mortem analysis must, for example, check that the dump has been executed properly. Without this check the machine may operate in an unknown and potentially unsafe state. Some of the dangerous failure events are very rare and the only option to ensure that these work for the designed purpose is to monitor their behaviour during normal operation.

D. Ondreka replied that verifying that the beam ended on the dump should be enough. R. Steinhagen said that the post mortem system should be used to verify if the beam was extracted on the dump as designed. A. Reiter asked, in response to this, how one could be sure that the beam actually hits the dump with the required parameters. C. Omet replied that the temperature measurements and BLM signals behind the dump are indicative. It needs to be seen whether a direct measurement using additional screens, for example, is necessary or possible from an integration point of view.

A. Reiter asked about the interface between the devices and the Fast-BAS (electrical vs. optical)? M. Mandaković replied that initially both electrical and optical interfaces were foreseen. However, for some systems, either one could be suppressed (e.g. as done for the power converter systems that supply only an optical system).

H. Weick asked whether these interfaces are only applicable for power converters or also for other systems, and whether there are already certain guidelines that should be fulfilled w.r.t. to the

electric and optical interfaces to the Fast-BAS. M. Mandaković affirmed that these would be applicable for all devices and that the implementation guidelines would be circulated via EDMS in due time.

A. Reiter asked whether the signal routing needs to be planned. C. Omet affirmed this.

D. Ondreka pointed out that there is a big difference between the quoted '5 ms' and '1 ms' worst-case latency as initially targeted for the timing system return channel. C. Omet mentioned that this requirement depends strongly on the beam drift and instability rise-times. This analysis started in parts but needs to be continued.

H. Weick asked whether the MPS signals could be grouped. For example, in some cases it does not matter which dipole is affected as long as the beam is aborted. D. Ondreka and C. Omet concurred as long as a detailed analysis is available afterwards to disentangle which dipole failed. R. Steinhagen noted that grouping of signals that may be masked for some operational cycles may be an exception (e.g. electron cooler for non-cooled beams). It would be up to CSCO to decide if masking is done centralised or distributed.

M. Mandaković iterated that only the summary condition are masked or propagated over the net. Detailed conditions would need to be read out from control system. Some devices have already been build or planned. CSCO has planned to use optical signals for new devices and fast electrical signals for existing devices. Signal transducers will be provided in order to change the signal from electrical to optical. This is done for cost reasons. The final details would need to be sorted out between the individual equipment groups and CSCO.

Next Steps and Actions:

- **MPLs and Experiments, notably HEBT, Super-FRS, APPA, CBM, CR,….:**
    - FMEA analysis also for accelerators, beam transfer-lines and experiments down-stream of SIS100 that may (either voluntarily or involuntarily) encounter high primary beam intensities (possibly also needed for SIS18 down-stream machines).
    - short term: assess whether the accelerators, beam transfer-lines and experiments down-stream of SIS100 need to have additional passive protection.
    - long-term: whether active single or multiple inputs to the SIS100 Fast-Abort-System to suppress the 'extraction permit' to their target or experimental hall are needed.

The next meeting is planned for: Wednesday 18th November 2015, 15:00-17:00 (SE 1.124c)

Reported by Ch. Hillbricht, R. J. Steinhagen