UITF BCM
PSS Interface and Overall Safety Requirements Specification

Revision 0.7: October 31, 2018
Author: Paul Metcalf (SSG)

Contents

Scope

This specification covers the overall safety and interface requirements for the BCM and BLA functions as they represent an input to the PSS safety system. This document is intended to cover the higher level architecture, diagnostic and hardware considerations required to progress with detailed hardware design, with some areas requiring final discussion between SSG and ICG also highlighted. More detailed lower level requirements and specifications will be developed as the project progresses however these will mainly be focused on software implementation, verification and validation. The following three cavities have been proposed for the UITF. All cavities will have overcurrent (BCM) functions. The beam loss (BLA) function is represented by:

$$BLA = |I_A - I_B - I_C|$$

Cavity	Location	Basic Function	Allowable Value
Cavity A	Quarter Cryogenic Exit	Total Beam Current	100nA (Low Power) 100µA (High Power)
Cavity B	Beam Dump	Beam Current To Dump	TBD
Cavity C	Target	Beam Current To Target	TBD
BLA	N/A	Beam Loss Accounting	100nA

Cavities

BCM and BLA Limitations

Note that there is no cavity installed upstream of the QCM, hence the BCM/BLA safety functions are not able to provide any protection against overcurrent or loss in the 200keV region when the beam is not passed through the QCM (such as when the faraday cup is inserted or there is beam loss within the Injector). This is deemed to be satisfactory due to the additional shielding located in this part of the UITF enclosure.

Also note that the PSS BCA and BLA functions do not include any modes of operation. For example, the BLA cannot provide any protection in the instance that beam is set to the wrong location. This is also deemed to be acceptable because the UITF enclosure is considered to be a single zone and the personal access system prevents access to the whole enclosure.

Document Schedule

The following documents will be available as part of the final package:

Phase	Document Title	Basic Content	Version
Preliminary Engineering Phase	Project Definition Document SSG-UITF-BCM-PDD-001	Project description, tasks, scope, safety categorization, concepts, risks, project management schedules and budgets, roles and responsibilities etc.	Final
	Hazard Identification and Risk Analysis SSG-UITF-BCM-HRA-002	Summary of safety hazards and risks as well as basic assessment of common failure modes and initiating events including DBIE (e.g. corrosion or loss of power, instrument air etc.), common causes etc.	Final
	Project Quality Plan SSG-UITF-BCM-PQP-003	Summary of document deliverables, review and approval requirements, material receiving requirements, fabrication requirements, change management, version control etc. Applies to software tools also.	Final
	Overall Safety Requirements Specification SSG-UITF-BCM-SRS-004	Contains overall safety objectives, safety functions and integrity level specifications with allocation to Sensor/LS/Actuator considering any redundancy.	Final
	Verification and Validation Plan SSG-UITF-BCM-VVP-005	Methodology for verification and validation including environmental certification plans.	Final

Phase	Document Title	Basic Content	Version
	Hardware Architecture Diagram SSG-UITF-BCM-ARCH-006	Provide enough detail at block level to understand the Inputs, Outputs, Diagnostics and Sub-Functions of the Sensor/LS/Actuator.	Preliminary
	HW/SW Design Requirements Specification SSG-UITF-BCM-PDD-007	Detailed sub-system and component hardware, software, diagnostic, systematic and administrative requirements needed to both define and ensure the integrity of the solution.	Preliminary
	Piping and Instrument Diagrams SSG-UITF-BCM-PID-008	Detail the instrument hook up/tie in to the process.	Preliminary
	General Arrangement Drawings SSG-UITF-BCM-GAD-009	Layouts drawings of component electronic housings, connector specifications, BCM cavity's etc.	Preliminary
	Schematic Diagrams SSG-UITF-BCM-SCHD-010	Schematic diagrams and board layouts of all hardware.	Preliminary
	Simulink Models SSG-UITF-BCM-MDL-011	FPGA application, diagnostic and interface logic. Also consider adding cavity and electronics models to this package.	Preliminary
	Design Manual SSG-UITF-BCM-DM-012	Summarize the design philosophy, design considerations and choices, and present at block level the design solution including its various states and modes of operation, interface requirements, alarm and trip settings, allowable values etc.	Preliminary
PDR	PDR Review Record SSG-UITF-BCM-PDRR-013	Review comments with disposition by DA on PDR Pack.	Final
Detailed Engineering Phase	Updated Hardware Architecture Diagram SSG-UITF-BCM-ARCH-006	Provide enough detail to understand the basic Inputs/Outputs/Diagnostics and Sub-Functions of the Sensor/LS/Actuator in order to proceed with hardware design. Is not intended to provide a specification for software.	Final

Phase	Document Title	Basic Content	Version
	Updated HW/SW Design Requirements Specification SSG-UITF-BCM-PDD-007	Detailed sub-system and component hardware, software, diagnostic, systematic and administrative requirements needed to both define and ensure the integrity of the solution.	Detailed
	Updated Piping and Instrument Diagrams SSG-UITF-BCM-PID-008	Detail the instrument hook up/tie in to the process.	Detailed
	Updated General Arrangement Drawings SSG-UITF-BCM-GAD-009	Layouts drawings of component electronic housings, connector specifications, BCM cavity's etc.	Detailed
	Updated Schematic Diagrams SSG-UITF-BCM-SCHD-010	Schematic diagrams and board layouts of all hardware.	Detailed
	Updated Simulink Models SSG-UITF-BCM-MDL-011	FPGA application, diagnostic and interface logic. Also consider adding cavity and electronics models to this package.	Detailed
	Updated Design Manual SSG-UITF-BCM-DM-012	Summarize the design philosophy, design considerations and choices, and present at block level the design solution including its various states and modes of operation.	Detailed
	Software and HDL Code SSG-UITF-BCM-SOFT-013	All configuration managed software deliverables including middleware, operating systems, interface drivers HDL code and third party soft/hard cores required to implement the solution.	Detailed
	Failure Modes and Effects Analysis SSG-UITF-BCM-FMEA-014	Detailed FMEA of hardware and software (the software FMEA is used to detect and treat SEU failures).	Detailed
	Reliability Block Diagram(s) SSG-UITF-BCM-RBD-015	RBD Diagram of Hardware	Detailed
	Test Cases SSG-UITF-BCM-STC-016	A summary of tests and results to exercise logic system functions at system level (derived from Simulink Model).	Detailed

Phase	Document Title	Basic Content	Version
	Inspection and Test Plans SSG-UITF-BCM-ITP-017	Inspection and Test Plans for bench, factory, integration, site installation and commissioning.	Detailed
	Material Schedules SSG-UITF-BCM-MTRL-018	A schedule of all material components not already listed on schematic diagrams (including cable and label schedules).	Detailed
	Operations, Maintenance and Disposal Manual SSG-UITF-BCM-OMDM-019	All user pertinent information required to manage the component throughout its lifecycle including required actions and completion times (including in case of dangerous failure in the SIF, instructions on placing outputs in a safe state) as well as preventive and corrective maintenance procedures.	Detailed
DDR	DDR Review Record SSG-UITF-BCM-DDRR-020	Review comments with disposition by DA on DDR Pack.	Final
Remaining Phases Including: Materials Receiving, Fabrication, FAT, SAT, Installation and Commissioning	Inspection and Test Records (Completed Inspection and Test Plans) SSG-UITF-BCM-ITR-021	Completion of bench, integration, environmental, installation and commissioning tests.	Final
	Safety Manual SSG-UITF-BCM-SM-022	A summary of the functional safety assessment results, validation results and user-relevant safety parameters including proof testing requirements, limitations of use, component lifetimes, SIF mode of operation, safe states, overrides, statement of systematic capability etc.	Final

Table 2: Document Schedule

Verification and Validation

Project development follows the V-Model as indicated below. Validation shall be assurance that test cases run on chip match those developed during simulation.

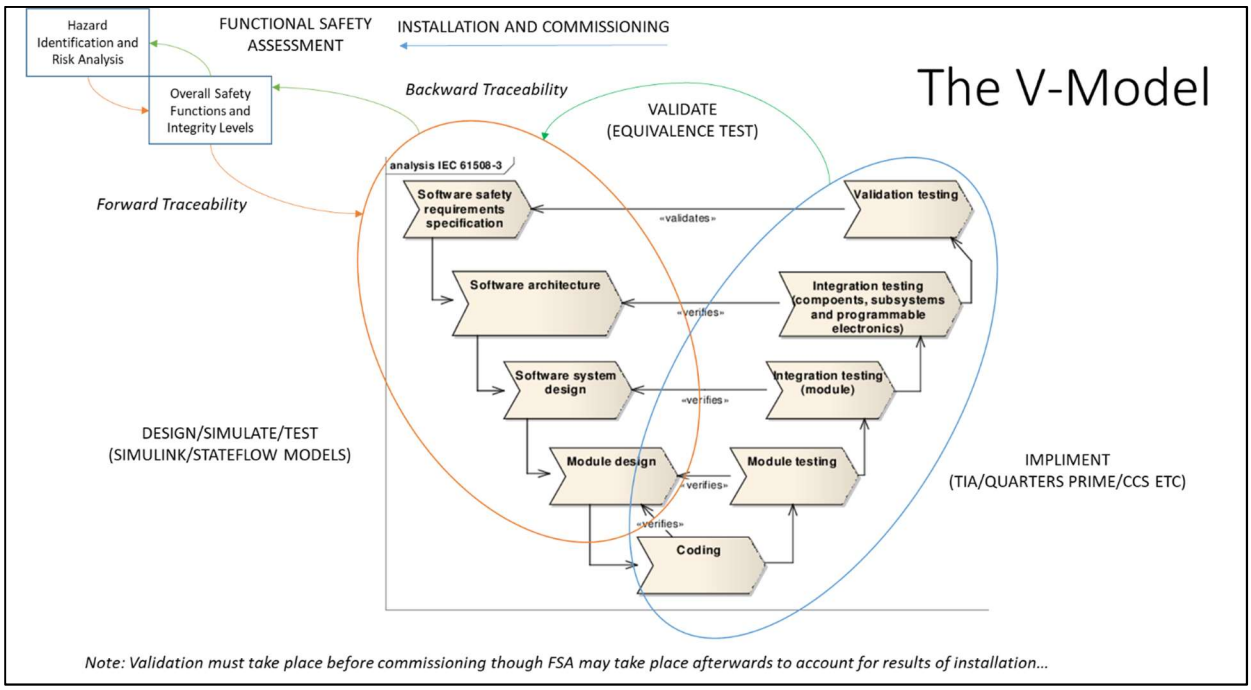

Figure 1: V-Model

Standards

The following standards were cited when formatting this specification. The two key standards in use are IEC 61508 (Functional, Reliability and Systematic Capability) and IEC 61131-2 (Environmental, Physical and Test).

Standard	Description
IEC 60529	Degrees Of Protection Provided By Enclosures
IEC 60812	Failure Mode and Effects Analysis (FMEA)
IEC 61000	Electromagnetic Compatibility (EMC)
IEC 61078	Analysis Techniques for Dependability - Reliability Block Diagram and Boolean Methods
IEC 61131	Programmable Logic Controllers (PLC)
IEC 61165	Application Of Markov Techniques
IEC 61499	Function Blocks
IEC 61508	Functional Safety - Electrical, Electronic and Programmable Electronic Safety Related Systems
IEC 61703	Mathematical Expressions For Reliability, Availability, Maintainability and Maintenance Support Terms
IEC 61784	Industrial Communication Networks - Profiles
IEC 62262	Degrees Of Protection Provided By Enclosures For Electrical Equipment Against External Mechanical Impacts
IEC 62308	Equipment Reliability - Reliability Assessment Methods
IEC 62380	Reliability Data Handbook - Universal Model For Reliability Prediction Of Electronics Components, PCBs and Equipment
IEC 62528	Standard Testability Method for Embedded Core-based Integrated Circuits
IEC 62685	Industrial Communication Networks - Profiles - Assessment Guideline for Safety Devices using IEC 61784-3 Functional Safety Communication Profiles
IEC 62987	Nuclear Power Plants - Instrumentation and Control Important to Safety - Use of Failure Mode and Effects Analysis (FMEA) And Related Methods To Support The Justification Of Systems
MAAB	Mathworks Automotive Advisory Board Guidelines For High Integrity Software Development
SN 29500	Siemens AG Standard For The Reliability Prediction of Electronic and Electromechanical Components

Table 3: Standards

Risk Matrix

A qualitative risk matrix is used to determine initial (no function available) and final (safety functions installed) risk levels. This is used to assess compliance with international standards and ensure the safety system provides the necessary level of risk reduction. Note that JSA may have more conservative design standards in place which will also be followed. Likelihoods refer to the demand on the function, not of the hazardous event occurring. Consequences refer to the nature of the hazardous event if the Safety Function is not available or fails.

	Severity				
Likelihood	5 Minor	4 Moderate	3 Major	2 Critical	1 Catastrophic
A Continuous	1 x SIL 2 2 x SIL 1*	1 x SIL 3 2 x SIL 2*	1 x SIL 4 2 x SIL 3*	Single Function Not Sufficient	Single Function Not Sufficient
B Frequent	1 x SIL 1	1 x SIL 2 2 x SIL 1*	1 x SIL 3 2 x SIL 2*	1 x SIL 4 2 x SIL 3*	Single Function Not Sufficient
C Occasional	SIL 0	1 x SIL 1	1 x SIL 2 2 x SIL 1*	1 x SIL 3 2 x SIL 2*	1 x SIL 4 2 x SIL 3*
D Possible	SIL 0	SIL 0	1 x SIL 1	1 x SIL 2 2 x SIL 1*	1 x SIL 3 2 x SIL 2*
E Improbable	SIL 0	SIL 0	SIL 0	1 x SIL 1	1 x SIL 2 2 x SIL 1*
F Rare	SIL 0	SIL 0	SIL 0	SIL 0	1 x SIL 1
G BDB	SIL 0				

Figure 2: Risk Matrix

Likelihood	Demand Rate (W) Per Year	Description
A Continuous	W ≥ 10	Demand expected many times per year (e.g. monthly), or loss of the function leads directly to the hazardous event occurring.
B Frequent	1 ≤ W < 10	Demand event expected to occur one or more times per year.
C Occasional	0.1 ≤ W < 1	Demand expected several times during the plant lifetime but not every year.
D Possible	0.01 ≤ W < 0.1	Demand on function could occur during the plant lifetime (although not guaranteed to occur).
E Improbable	0.001 ≤ W < .01	Demand on function unlikely to occur (although feasibly could occur) during the plant lifetime.
F Rare	0.0001 ≤ W < 0.001	Demand on function very unlikely to occur during the plant lifetime but is not considered to be beyond the design basis.
G BDB	W < 0.0001	Either it is impossible for the event to occur or the event is considered to be beyond the design basis.

Figure 3: Likelihood Ratings

Severity	People Injury	People (Acute Dose) D**	Plant Repair Cost C	Tolerable Event Rate E (Per Year)
1 Catastrophic	Multiple Fatalities	>1 Person: D ≥ 100 rem	Loss of Asset C ≥ $10M	E < 0.0001
2 Critical	Single Fatality, Permanent Partial Disability or Multiple Injuries with Severity Major	1 Person: D ≥ 100 rem >1 Person: 10 ≤ D < 100 rem	Significant Downtime (Months) Suspension of Operating License $1M ≤ C < $10M	0.0001 ≤ E < 0.001
3 Major	Temporary Disability, Hospitalization/Surgery and Rehabilitation or Multiple Injuries with Severity Moderate	1 Person: 10 ≤ D < 100 rem >1 Person: 1 ≤ D < 10 rem	Major downtime (Weeks) Reportable event without loss of license $100k ≤ C < $1M	0.001 ≤ E < 0.01
4 Moderate	Injury requiring medical treatment including Lost Time Injury without Surgery or Rehab	1 Person: 1 ≤ D < 10 rem >1 Person: 0.1 ≤ D < 1 rem	Moderate downtime (days) $10k ≤ C < $100k	0.01 ≤ E < 0.1
5 Minor	Minor Injury Self healing with minor first aid and no lost time.	1 Person: D < 1 rem >1 Person: D < 0.1 rem	Minimal (hours) or no downtime C < $10k	0.1 ≤ E < 1

Figure 4: Consequence Levels

**Note that pregnant worker dose limits are less than those listed in Figure 4. These dose limits are used to rank acute accident scenarios for the probabilistic safety case. They do not represent dose limits for managing non-acute (cumulative) exposure, nor do they replace the need to practice ALARA in every day operations. Again note that Likelihoods refer to the likelihood of demand on the function, not the likelihood of the hazardous event occurring. The likelihood of the hazardous event occurring is described by Tolerable Event Rate (E). For example, the probabilistic design target for a moderate injury is 1 in 50 years of operation…

Demand Likelihood	Event Consequence	Risk	Required RRF
Continuous or Very High	Catastrophic	Extreme LOPA Mandatory	100,000 – 1,000,000
High	Catastrophic		
Continuous or Very High	Critical		
Occasional	Catastrophic	Very High LOPA Highly Recommended	10,000 – 100,000
High	Critical		
Continuous or Very High	Major		
Possible	Catastrophic	High	1,000 - 10,000x
Occasional	Critical		
High	Major		
Continuous or Very High	Moderate		
Improbable	Catastrophic	Medium	100 – 1,000x
Possible	Critical		
Occasional	Major		
High	Moderate		
Continuous or Very High	Minor		
Rare	Catastrophic	Low	10 - 100x
Improbable	Critical		
Possible	Major		
Occasional	Moderate		
High	Minor		
Beyond Design Basis	Catastrophic	Safety System Not Required	None
Rare	Critical		
Improbable	Major		
Possible	Moderate		
Occasional	Minor		
Beyond Design Basis	Critical		
Rare	Major		
Improbable	Moderate		
Possible	Minor		
Beyond Design Basis	Major		
Rare	Moderate		
Improbable	Minor		
Beyond Design Basis	Moderate		
Rare	Minor		
Beyond Design Basis	Minor		

Table 5: Initial Risk Levels and Required Risk Reduction Factor (RRRF)

Terminology

Several key terms are used throughout the safety document as described below:

Term	Definition
Operable	A safety function is OPERABLE when it is capable of performing its designed Safety Function if and when required.
Safety Critical	A Safety Function with a SIL of 3 or 4.
Safety Related	A Safety Function with a SIL of 1 or 2. Failure of the safety system should not result in loss of life or significant injury including paralysis.
Non-Safety Related	A Safety Function with a SIL of zero (aka no SIL required).
Safe Fault	A fault that causes the channel to move to its safe state or remain stuck in its safe state. When a safe faults occurs it is often called a “spurious” trip.
Dangerous Fault	A fault that prevents the channel from being capable of performing its intended safety function. Dangerous faults are either detectable (by diagnostics) or not detectable.
Dangerous Undetected Fault	A dangerous fault that is undetectable by channel diagnostics and requires administrative proof testing or maintenance in order to detect. Often referred to as a hidden fault or unrevealed fault.
Dangerous Detected Fault	A dangerous fault that is detectable by channel diagnostics, provided the diagnostics are operable. Once detected, the fault may either be isolated or controlled.
Isolated Fault	A fault that is detected by channel diagnostics and an alarm issued but no further action is taken until the channel is repaired by maintenance. The channel system is allowed to continue operation with the fault isolated (only applicable to multi-channel architectures).
Controlled Fault	A fault that is detected by channel diagnostics and then controlled by means of the channel diagnostics opening a fault relay. In many architectures the fault relay is monitored by the redundant channel or external/supervisory system because a fault should never be controlled by the sub-system in which the fault was detected. Depending on the implementation of the fault control system, the safety system may allow time limited operation (temporary isolation) to allow the fault to be recovered, or the safety system may change its voting pattern depending on the presence of faults.
Inoperable	A safety function is INOPERABLE when it is not capable of performing its designed Safety Function if required. Channels which possess Safe Faults should be considered INOPERABLE even though they have failed to a safe detectable state.
Channel Tripped	The channel is tripped when it has successfully performed its safety function due to external demand. Not to be confused with Safe Fault or Spurious Trip.
Allowable Value	The maximum physical limit that cannot be exceeded. For example the pressure at which a tank ruptures.
Safety Setting	The Safety Setting ensures that the Allowable Value is never exceeded. The margin between the Safety Setting and Allowable Value must consider channel drift, oscillation, response time, calibration interval, accuracy and various other parameters.

Term	Definition
Demand	A demand on the safety function occurs when the process exceeds its safe limit and intervention by the safety system is required.
Fault	Any fault in the channel that means it is not operating as intended.
Failure	A Functional Failure occurs if there is a demand on the channel when it has a Dangerous Fault present and hence does not perform its intended function. If there is only one channel and function providing safety, the Failure may result in the occurrence of a hazardous event/accident.

Table 4: Safety Terms

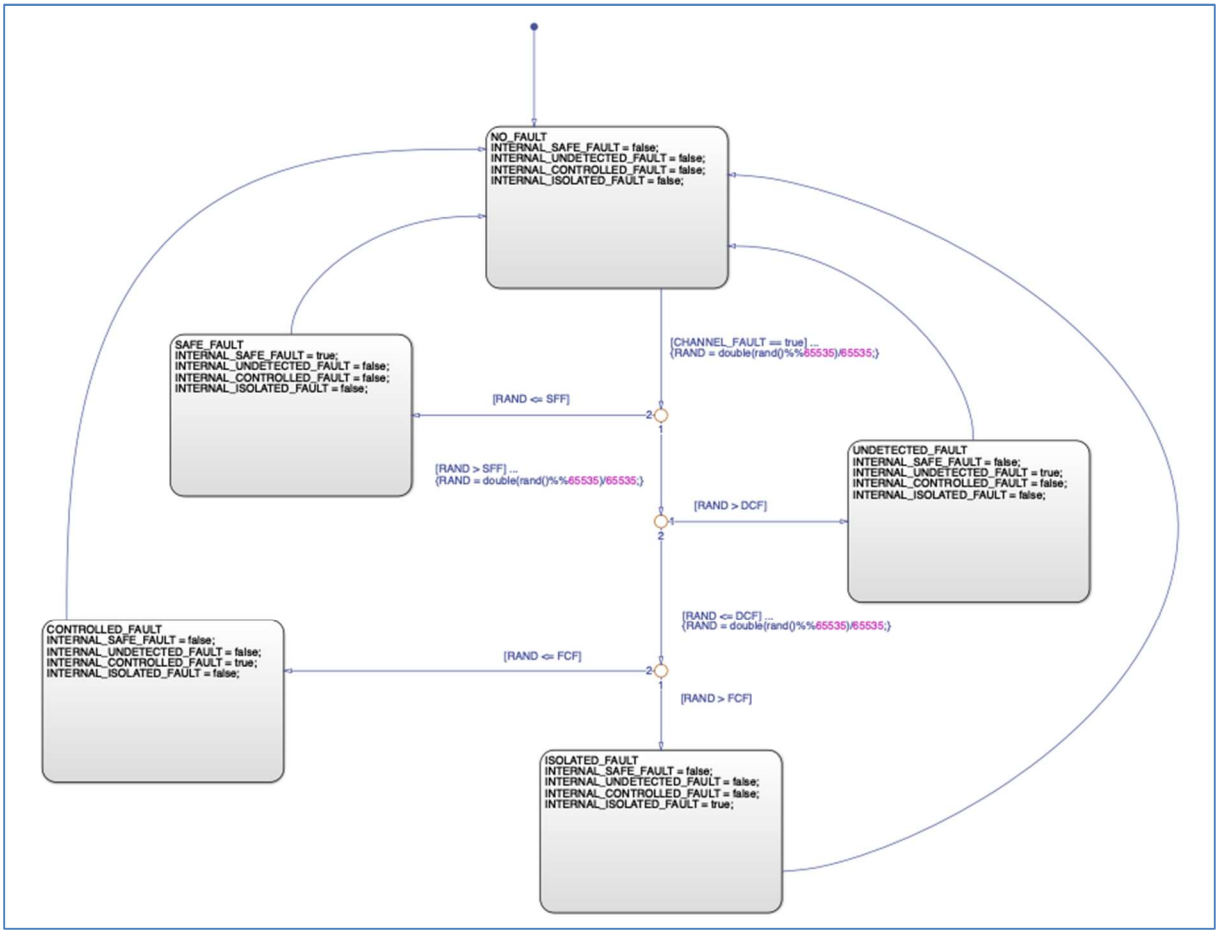

Figure 4: Types of Faults Demonstrating SFF/DCF/FCF in SSG Reliability Model

The Safe Failure Fraction (SFF), Diagnostic Coverage Fraction (DCF) and Fault Control Fractions (FCF) are shown in relation to the above definitions in the equations below. An FMEDA is required to determine the value of these parameters however targets have been specified in the Overall Specifications.

$$SFF = \frac{\Sigma\lambda_S + \Sigma\lambda_{D_d}}{\Sigma\lambda_S + \Sigma\lambda_{D_d} + \Sigma\lambda_{D_u}}$$

$$DCF = \frac{\Sigma\lambda_{D_d}}{\Sigma\lambda_{D_d} + \Sigma\lambda_{D_u}}$$

$$FCF = \frac{\Sigma\lambda_{D_{d,c}}}{\Sigma\lambda_{D_{d,c}} + \Sigma\lambda_{D_{d,i}}}$$

Equations: Safety Fractions

Design Basis Initiating Events

Note that the BCM and BLA system is not considered a mitigation for the hazard of Personnel Access Violation. Hazards are therefore acute radiation dose to staff residing outside the shielding of the UITF enclosure during the following beam malfunction initiating event scenarios. *Initial risk levels are draft since final radiation modelling is not yet available. Note that design basis initiating events represent the worst case but credible accident scenarios and should consider the physical limits of each energy source such as power supply ratings etc. If it is not clear that a potential accident scenario is bound by another, then it should be included as a separate line.

DBIE	Acute Radiation Accident Initiating Event	Hazard	Initial Risk*
1	Malfunction of the beam source at injector (e.g. laser intensity or frequency) causes total beam current to rise to 3mA for a 200keV beam without the QCM in operation (power supply limited). Condition exists for 30 minutes before being manually interrupted by operator and/or building being evacuated.	Acute Radiation Dose	DX
2	Malfunction of the beam source at injector (e.g. laser intensity or frequency) causes total beam current to rise to 300µA for a 10MeV beam with the QCM in operation (SRF cavity limited). Condition exists for 30 minutes before being manually interrupted by operator and/or building being evacuated.	Acute Radiation Dose	DX
3	Malfunction of beam acceleration or steering during low current operation causes total beam loss of 100nA for the 10MeV beam. Condition exists for 30 minutes before being manually interrupted by operator and/or building being evacuated.	Acute Radiation Dose	AX
4	Malfunction of beam acceleration or steering during high current operation causes total beam loss of 100uA for the 10MeV beam. Condition exists for 30 minutes before being manually interrupted by operator and/or building being evacuated.	Acute Radiation Dose	AX

Table 4: Design Basis Initiating Events (Initial Risk, No Safety System)

Note that DBIE4 bounds DBIE3 hence DBIE3 will be removed when the UITF moves into high current operation. DBIE1 may not be credible hence further input is sought from end users.

In each of the four DBIE listed above, RADCON shall first estimate the dose rate to staff outside the shielding of the UITF assuming no BCM/BLA/PSS functions are available (to inform Initial Risk levels). RADCON shall then also estimate the dose levels to staff working near the exterior of the UITF shielding when the same DBIE events occur and this time are successfully controlled by the BCM/BLA Safety Functions. For the later analysis, RADCON may need to know the response times of the PSS as shown in the sequences below. However, rather than model these beam shutdown sequences, RADCON may find it easier to assume that no current or potential limiting occurs until the laser shutters are fully inserted at 500ms after the demand.

DBIE	Acute Radiation Accident Initiating Event (PSS Controlled)	Hazard	Final Risk*
5	Malfunction of the beam source at injector (e.g. laser intensity or frequency) causes total beam current to rise to 3mA for a 200keV beam without the QCM in operation (power supply limited). The safety system functions and current is reduced to 600µA at 40ms after demand, then 1nA at 500ms after demand.	Acute Radiation Dose	DX
6	Malfunction of the beam source at injector (e.g. laser intensity or frequency) causes total beam current to rise to 300µA for a 10MeV beam with the QCM in operation (SRF cavity limited). The safety system functions and current is reduced to 60µA at 40ms after demand, potential is reduced to 200keV at 200ms after demand, and finally current is reduced to 1nA at 500ms after demand.	Acute Radiation Dose	DX
7	Malfunction of beam acceleration or steering during low current operation causes total beam loss of 100nA for the 10MeV beam. The safety system functions and current is reduced to 20nA at 40ms after demand, potential is reduced to 200keV at 200ms after demand, and finally current is reduced to 1nA at 500ms after demand.	Acute Radiation Dose	AX
8	Malfunction of beam acceleration or steering during high current operation causes total beam loss of 100uA for the 10MeV beam. The safety system functions and current is reduced to 20µA at 40ms after demand, potential is reduced to 200keV at 200ms after demand, and finally current is reduced to 1nA at 500ms after demand.	Acute Radiation Dose	AX

Table 4: Design Basis Initiating Events (Final Risk Analysis with Safety System Installed)

Again note that DBIE8 bounds DBIE7 hence DBIE7 will be removed when the UITF moves into high current operation phase. Note that the PSS is not able to control its Response Time, only its Safety Settings. Hence depending on radiation levels calculated, Final Risk Levels will mainly depend on the agreement of Allowable Values/Safety Settings to be discussed between SSG/UITF/RADCON.

As shown above, the proposed end-to-end process safety time will be targeted at 500ms which is mainly limited by the insertion time of laser shutters. The PSS design includes the capability to measure the end-to-end response time and this will be done automatically by the Safety PLC (which is then able to store trend data for offline analysis and failure prediction). Hence all response time assumptions will be validated during cold commissioning.

Two sets of RADCON analysis are therefore required to validate that the PSS safety system provides the necessary level of risk reduction. Pending these results, the safety functions have been conservatively set at SIL 2 level to hopefully cover all conceivable use case scenarios the system may encounter, including outside the UITF. It is assumed that highest dose rates will occur behind the shielding wall at the rear of the end station.

Although it is not required for the safety case, the UITF may also wish to estimate damage to equipment during the DBIE listed above. Anecdotally complete overhaul of a QCM due to loss of vacuum and burn through would exceed $1M hence the consequence to plant and operations could be categorized as “Critical” for the Beam Loss Accounting function. It is not currently known the consequence to plant equipment for failure of the BCM Safety Functions.

Currently, Safety Settings/Allowable Values have assumed a fixed set-point for BCM/BLA trips. However since beam power / radiation is proportional to the square of the beam current, and users have expressed a desire to have a mode of time-limited over-current operation, we propose defining the safety limit using a time-current curve as described below.

Safety Limit

It is proposed to represent the current/time safety limit using the following safety parameters and equations. The safety limit is also indicated graphically further below. Because the BCM only measures current, there is no safety limit referencing beam energy in this specification.

$$\Delta t = \frac{\left(\frac{I_{max}^2}{I^2} - 1\right) \times (t_{max} - t_{min})}{\left(\frac{I_{max}^2}{I_{min}^2} - 1\right)} + t_{min}$$

$$x = \frac{1}{I^2}$$

$$a = \frac{I_{max}^2 \times (t_{max} - t_{min})}{\left(\frac{I_{max}^2}{I_{min}^2} - 1\right)}$$

$$b = t_{min} - \frac{(t_{max} - t_{min})}{\left(\frac{I_{max}^2}{I_{min}^2} - 1\right)}$$

Equations 3: Safety Limit Curve

When the current falls below IMIN, the state of the integrator (S) should decay exponentially according to the following equation. This ensures that short duration dips below IMIN do no reset the integrator and invalidate the safety limit.

$$S(t) = S(0) \times exp^{(\lambda.t)}$$

$$\lambda = \frac{ln\left(\frac{1}{t_{max}}\right)}{t_{max}}$$

Equations 4: Decay of Safety Limit

The equations above are governed by 4 safety parameters: TMAX, TMIN, IMAX and IMIN:
IMAX: The current or loss, above which an instantaneous trip should occur.
IMIN: The current or loss, below which indefinite operation is allowed.
TMAX: The maximum amount of time the beam will operate at IMIN before being shut down.
TMIN: The maximum amount of time the beam will operate above IMAX before being shut down.

The final value of these parameters will be set in consultation with the user (UITF/RADCON) to ensure the safety limit curve is clearly defined and agreed. The same safety limit equation is valid for both the BCM and BLA functions (though different parameter values will apply to each function).

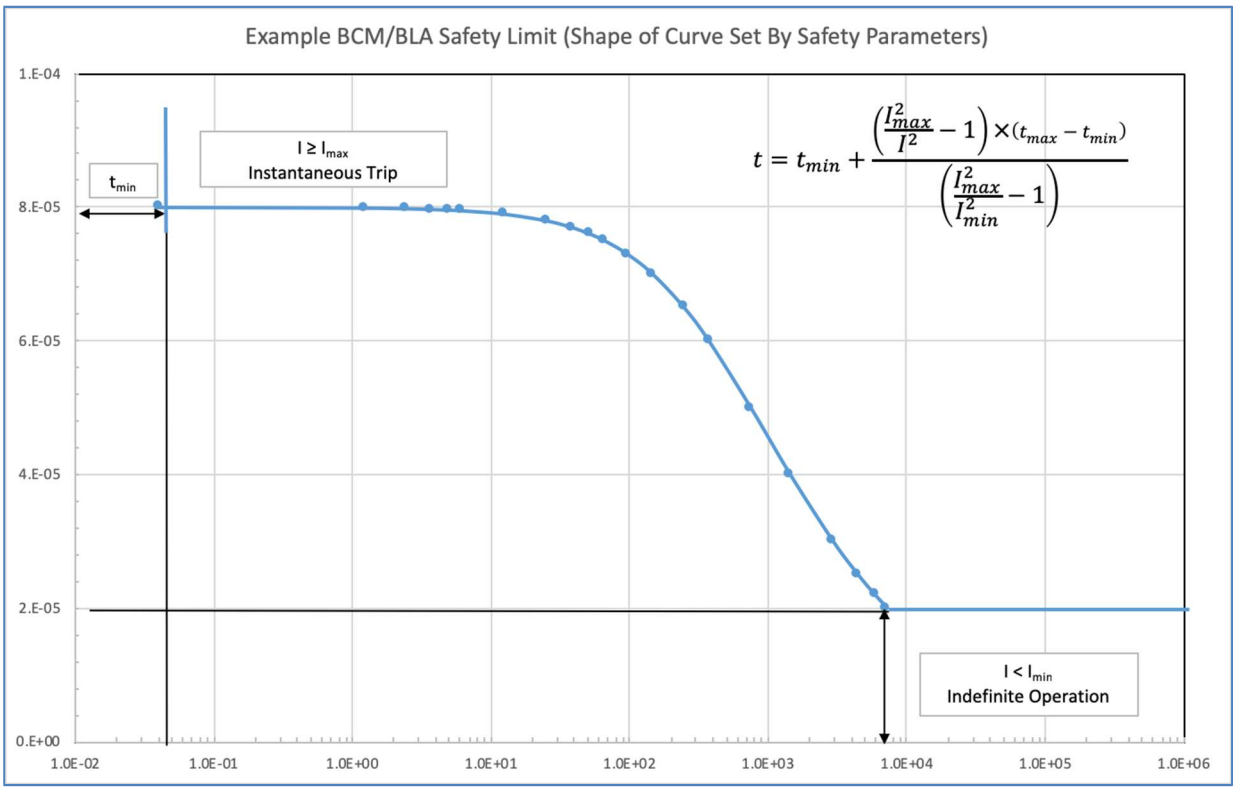

Figure 8: Generic Safety Limit Curve

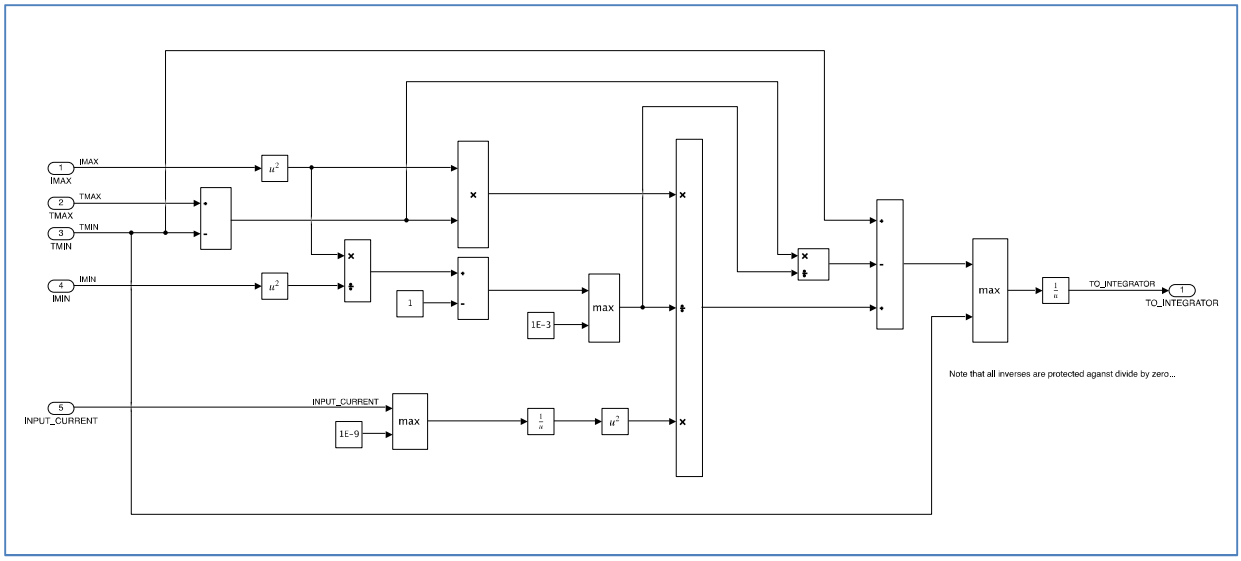

Figure 7: Simulink Representation of Safety Limit Equation Input to Integration

The implementation of the trip processing function within the FPGA will be performed in a fashion that does not violate this curve (with suitable margin to account for channel response time, drift and oscillation).

Reliability

Basic reliability modelling of the BCM has been completed using the TÜV simplified equations from IEC 61508 as shown below:

$$PFD_{avg} = \frac{\lambda_{d_u}\beta T}{2} + \frac{\lambda_{d_u}^2(1-\beta)^2T^2}{3} + \frac{\lambda_{d_D}\beta_D T_D}{2} + \frac{\lambda_{d_D}^2(1-\beta_D)^2T_D^2}{3}$$

Equation 2: Simplified Equation for PFD_{avg}

The required/target per-Channel Mean-Time-To-Any-Failure (Plot 1) and Mean-Time-To-Dangerous-Undetected-Failure (Plot 2) curves for each BCM Input Channel are shown below. An advanced Monte-Carlo driven Markov model has been developed within SSG and is currently being tested. This model will be used to provide more accurate (and potentially more flexible) reliability data and targets for the final safety case when the FMEDA is completed.

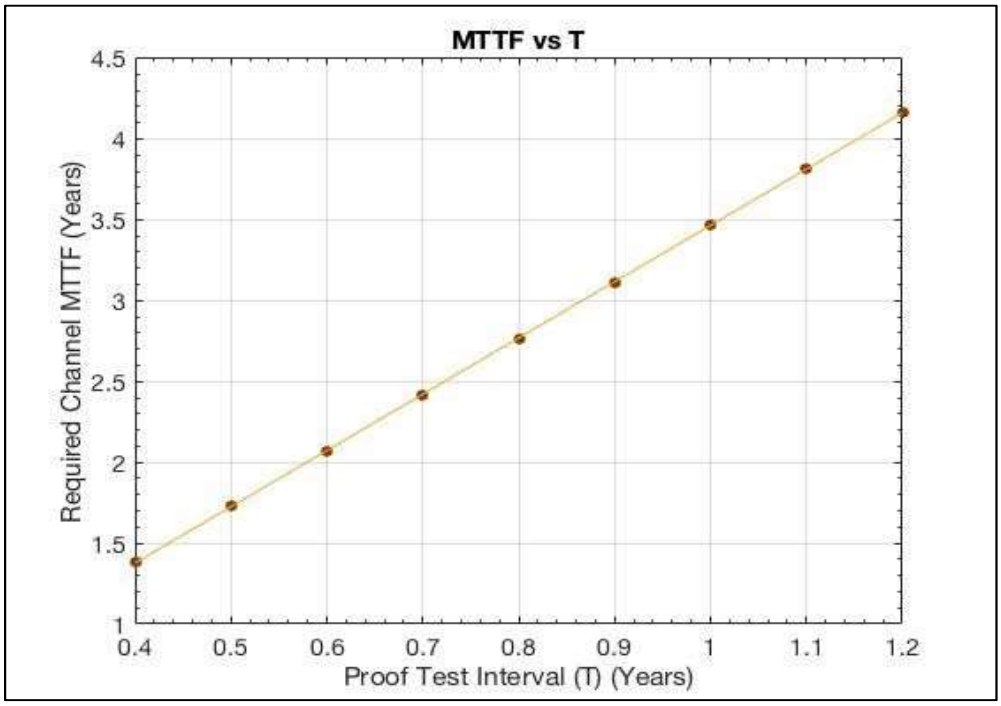

Figure 5: MTTF versus Proof Test Interval

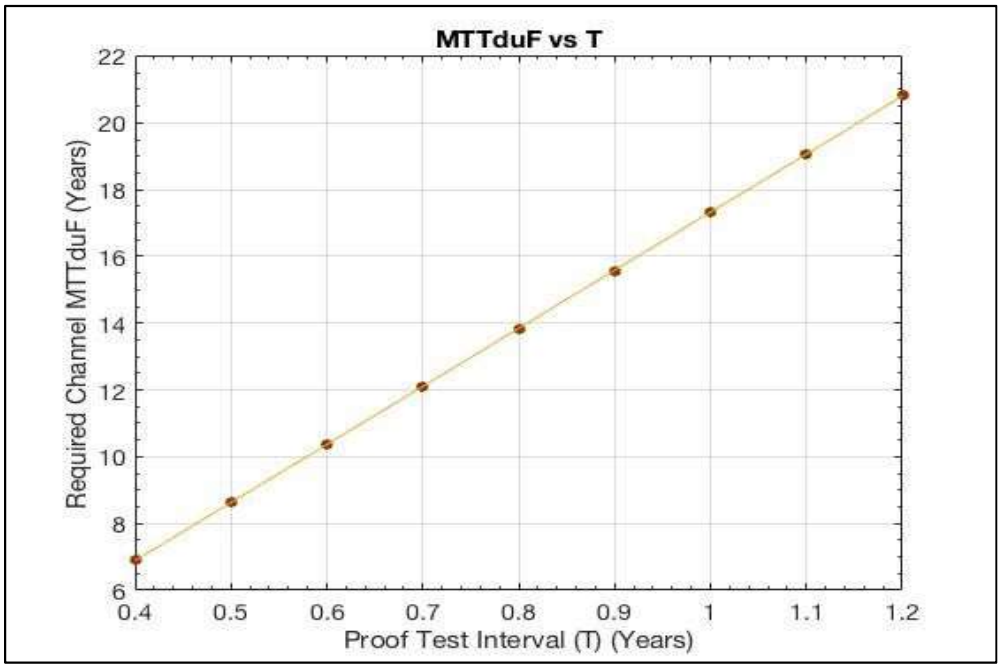

Figure 6: $MTT_{du}F$ versus Proof Test Interval

Note that ideally an FMEDA "Failure Modes, Effects and Diagnostic Analysis" will need to be completed by ICG and SSG on the finalized hardware to verify that these targets have been met. This analysis would use both component level reliability handbook data complemented by "Stuck-At" fault modelling to build the system Reliability Block Diagram (RBD) and verify that the target MTTF has been met.

Note: For the UITF, the reliability targets (SIL 2) are likely to be extremely conservative as the application likely falls closer to SIL 1 requirements.

Overall Safety Functions

Overall safety functions for the UITF are listed below. The probabilistic safety case should be able to demonstrate that the UITF Safety Case for beam current/energy as it relates to equipment damage and radiation dose limits can be met by either the availability of the Laser Shutter Actuators *or* the availability of both the Pockel Cell Actuator and RF Power Supply Actuator functions. However only the insertion of laser shutters is able to stop all beam transport hence it is considered mandatory required functionality.

ID	Description
SF1	If the UITF total beam current exceeds 100nA during low power operation then the beam shall be shut down within 0.5 seconds by insertion of a laser shutter. The SIL of this function shall be SIL 2.
SF2	If the UITF total beam current exceeds 100nA during low power operation then beam current shall be reduced by at least 80% within 0.04 seconds by disabling power to a Pockel Cell. The SIL of this function shall be SIL 2.
SF3	If the UITF total beam current exceeds 100nA during low power operation then beam potential shall be limited to 200keV within 0.2 seconds by disabling power to RF power supplies of the quarter cryogenic module. The SIL of this function shall be SIL 2.
SF4	If the UITF total beam current exceeds 100µA during high power operation then the beam shall be shut down within 0.5 seconds by insertion of a laser shutter. The SIL of this function shall be SIL 2.
SF5	If the UITF total beam current exceeds 100µA during high power operation then beam current shall be reduced by at least 80% within 0.04 seconds by disabling power to a Pockel Cell. The SIL of this function shall be SIL 2.
SF6	If the UITF total beam current exceeds 100µA during high power operation then beam potential shall be limited to 200keV within 0.2 seconds by disabling power to RF power supplies of the quarter cryogenic module. The SIL of this function shall be SIL 2.
SF7	If the UITF current to the target exceeds XµA during low power operation then the beam shall be shut down within 0.5 seconds by insertion of a laser shutter. The SIL of this function shall be SIL 2.
SF8	If the UITF current to the target exceeds XµA during low power operation then beam current shall be reduced by at least 80% within 0.04 seconds by disabling power to a Pockel Cell. The SIL of this function shall be SIL 2.
SF9	If the UITF current to the target exceeds XµA during low power operation then beam potential shall be limited to 200keV within 0.2 seconds by disabling power to RF power supplies of the quarter cryogenic module. The SIL of this function shall be SIL 2.

ID	Description
SF10	If the UITF current to the target exceeds XμA during high power operation then the beam shall be shut down within 0.5 seconds by insertion of a laser shutter. The SIL of this function shall be SIL 2.
SF11	If the UITF current to the target exceeds XμA during high power operation then beam current shall be reduced by at least 80% within 0.04 seconds by disabling power to a Pockel Cell. The SIL of this function shall be SIL 2.
SF12	If the UITF current to the target exceeds XμA during high power operation then beam potential shall be limited to 200keV within 0.2 seconds by disabling power to RF power supplies of the quarter cryogenic module. The SIL of this function shall be SIL 2.
SF13	If the UITF current on the beam dump exceeds XμA during low power operation then the beam shall be shut down within 0.5 seconds by insertion of a laser shutter. The SIL of this function shall be SIL 2.
SF14	If the UITF current on the beam dump exceeds XμA during low power operation then beam current shall be reduced by at least 80% within 0.04 seconds by disabling power to a Pockel Cell. The SIL of this function shall be SIL 2.
SF15	If the UITF current to the target exceeds XμA during low power operation then beam potential shall be limited to 200keV within 0.2 seconds by disabling power to RF power supplies of the quarter cryogenic module. The SIL of this function shall be SIL 2.
SF16	If the UITF current on the beam dump exceeds XμA during high power operation then the beam shall be shut down within 0.5 seconds by insertion of a laser shutter. The SIL of this function shall be SIL 2.
SF17	If the UITF current on the beam dump exceeds XμA during high power operation then beam current shall be reduced by at least 80% within 0.04 seconds by disabling power to a Pockel Cell. The SIL of this function shall be SIL 2.
SF18	If the UITF current to the target exceeds XμA during high power operation then beam potential shall be limited to 200keV within 0.2 seconds by disabling power to RF power supplies of the quarter cryogenic module. The SIL of this function shall be SIL 2.
SF19	If the UITF beam loss exceeds 100nA then the beam shall be shut down within 0.5 seconds by insertion of a laser shutter. The SIL of this function shall be SIL 2.
SF20	If the UITF beam loss exceeds 100nA then beam current shall be reduced by at least 80% within 0.04 seconds by disabling power to a Pockel Cell. The SIL of this function shall be SIL 2.

ID	Description
SF21	If the UITF beam loss exceeds 100nA then beam potential shall be limited to 200keV within 0.2 seconds by disabling power to RF power supplies of the quarter cryogenic module. The SIL of this function shall be SIL 2.

Table 5: Overall Safety Functions