# Reliability studies on uQDS, PDSU and PDSU-BIS interface for the IT protection

L. Felsberger, D. Westermann, D. Wollmann

Acknowledgements to R. Denz, C. Martin, T. Podzorny, I. Romera Ramirez, J. Steckert, J. Uythoven

# Introduction

## Universal Quench Detection System (uQDS):

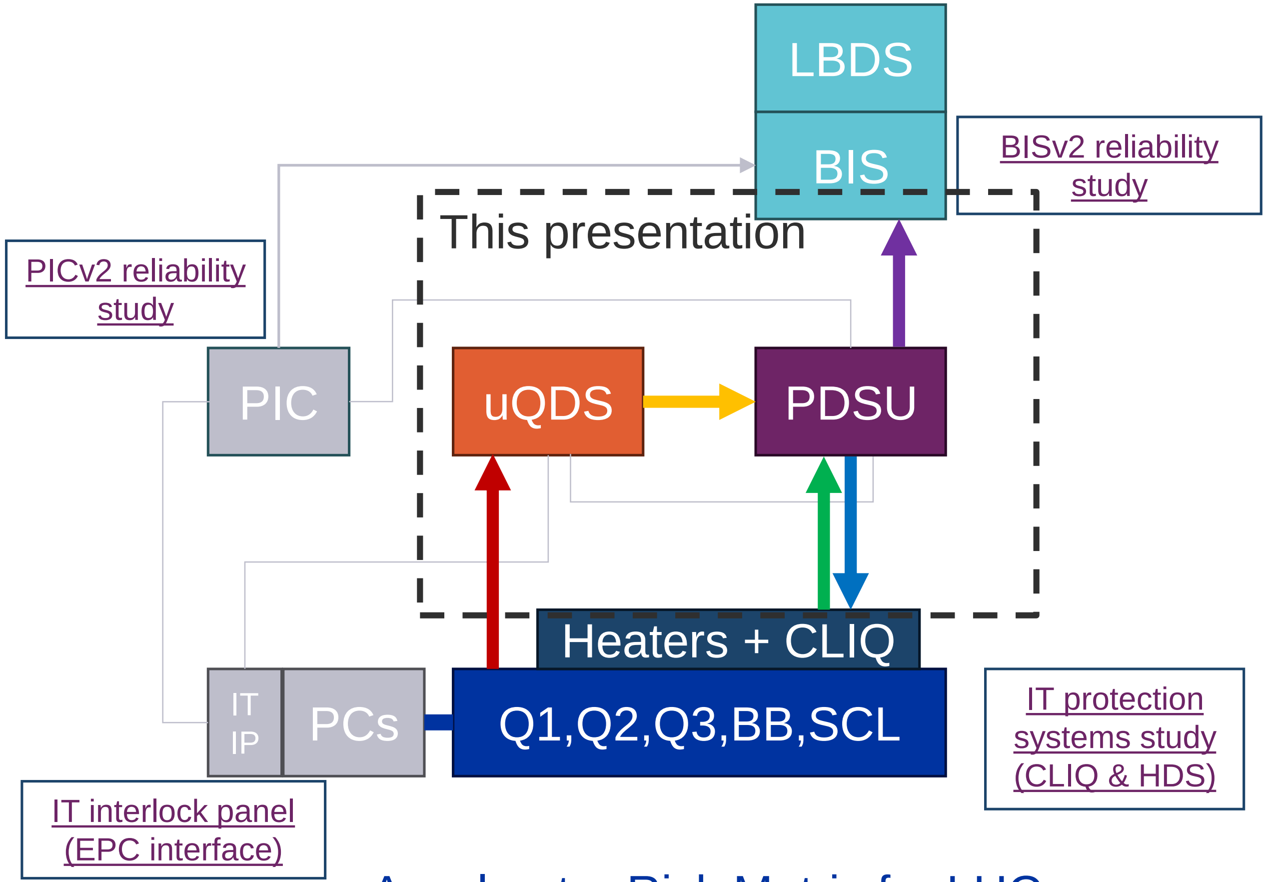
- Detect magnet quench
- Trigger PDSU
- Trigger FPA loop, Diagnostics

## Protection Device Supervision Unit (PDSU):

- (Re-)Trigger magnet protection systems
- Trigger beam dump
- Detect spurious magnet protection firing
- Trigger FPA loop, Diagnostics

## Beam Interlock System (BIS):

- Transmit beam dump request
- Diagnostics




Accelerator Risk Matrix for LHC:

| | [1m - 20m) | [20m - 1h) | [1h - 3h) | [3h - 6h) | [6h - 12h) | [12h - 24h) | [24h - 2d) | [2d - 1w) | [1w - 1M) | [1M - 1Y) | [1Y - 10Y) |
|---|---|---|---|---|---|---|---|---|---|---|---|
| 1/H | U | U | U | U | U | U | U | U | U | U | U |
| 1/Shift | U | U | U | U | U | U | U | U | U | U | U |
| 1/Day | A | U | U | U | U | U | U | U | U | U | U |
| 1/Week | A | A | A | ★ | U | U | U | U | U | U | U |
| 1/Month | A | A | A | A | A | A | U | U | U | U | U |
| 1/Year | A | A | A | ★ | A | A | A | A | U | U | U |
| 1/10Years | A | A | A | A | A | A | A | A | A | U | U |
| 1/100Years | A | A | A | A | A | A | A | A | A | ★ | U |
| 1/1000Years | A | A | A | A | A | A | A | A | A | ★ | A |

## Main failure modes:

- Missed magnet protection and beam dump (target for LHC systems - 1 in 1000 years)
- Spurious magnet protection and beam dump (target for LHC - 1 in 1 year)

→ Reliability analysis crucial

# Reliability Analysis Methodology

Risk identification and quantification

## Top-Level Failure Modes, Effects and Criticality Analysis (FMECA)

- Identify system, functions, associated risks and hazards and possible end-effects

## Accelerator Risk Matrix

- Quantify reliability requirements to mitigate risks and hazards

Risk estimation and mitigation

## Top-Down reliability model

- Capture system structure, redundancies, critical/non-critical parts, demand, inspection rates

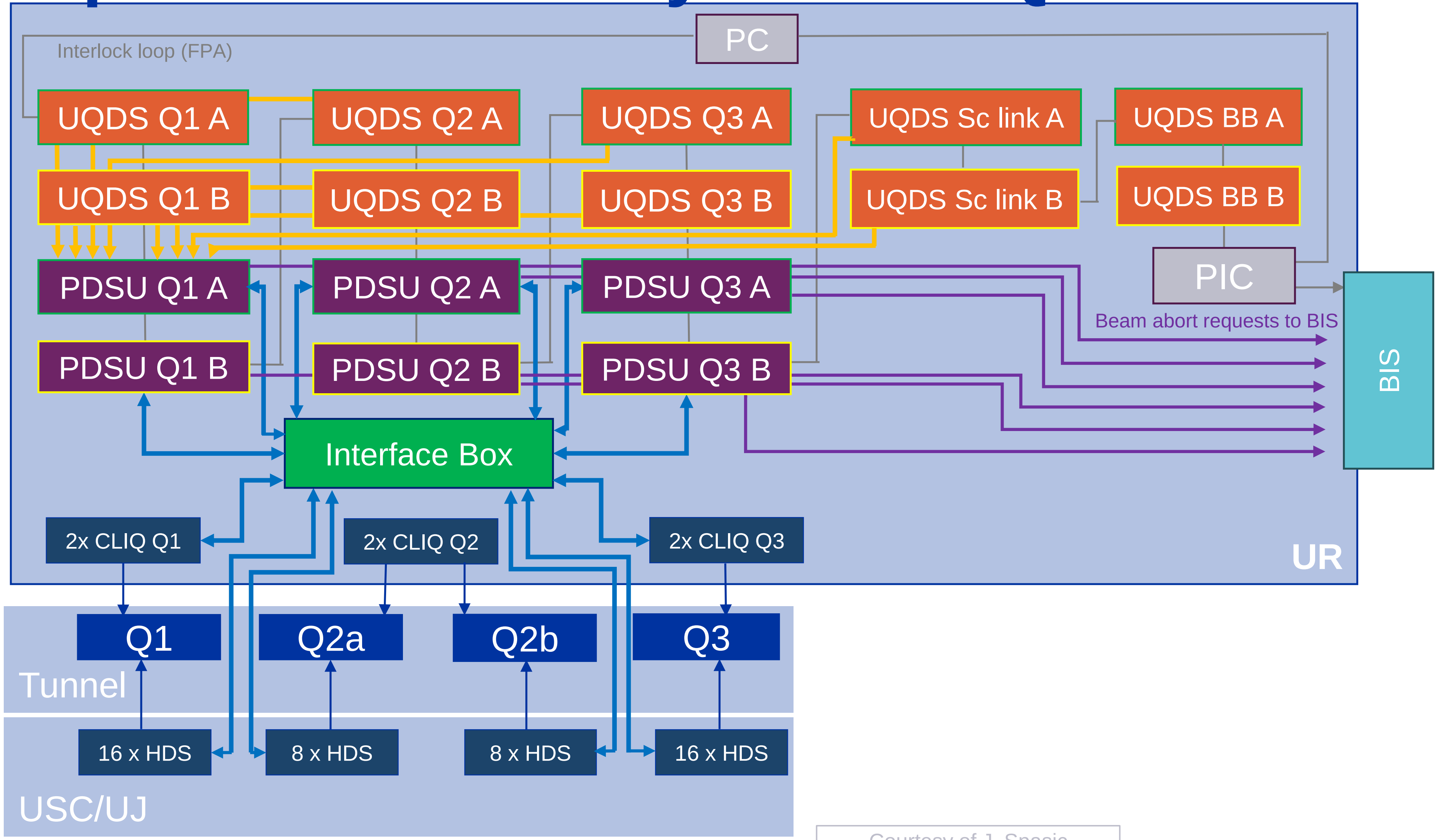
## Component-Level FMECA

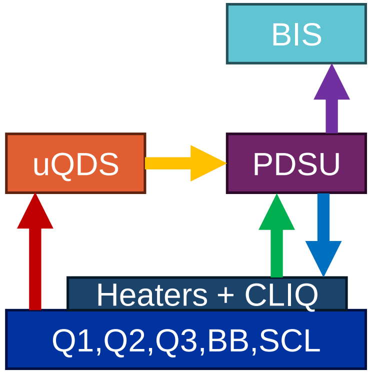
- Analyse detailed sub-system design to identify their failure probabilities for each end-effect

## → Design qualification

- Feed results from Component-Level FMECA into Top-Down FTA to qualify design or require design improvements

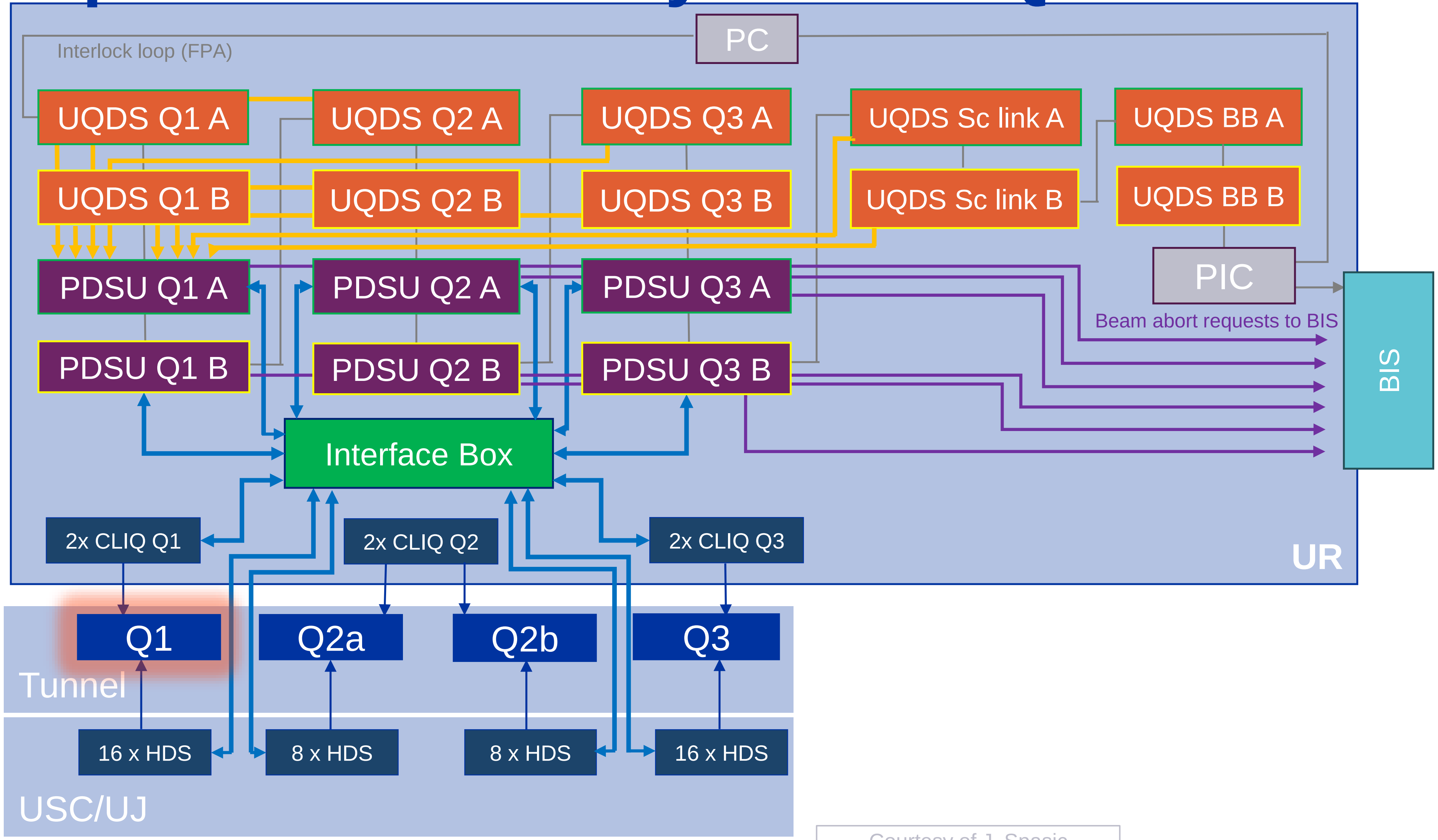
# Top-Down Reliability Model - Quench

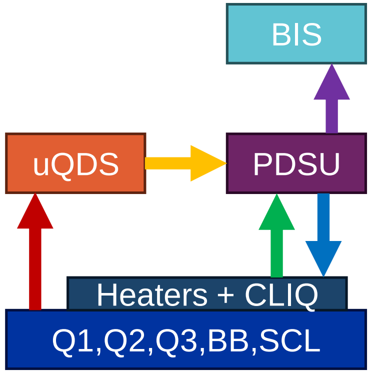



Courtesy of J. Spasic

# Top-Down Reliability Model - Quench

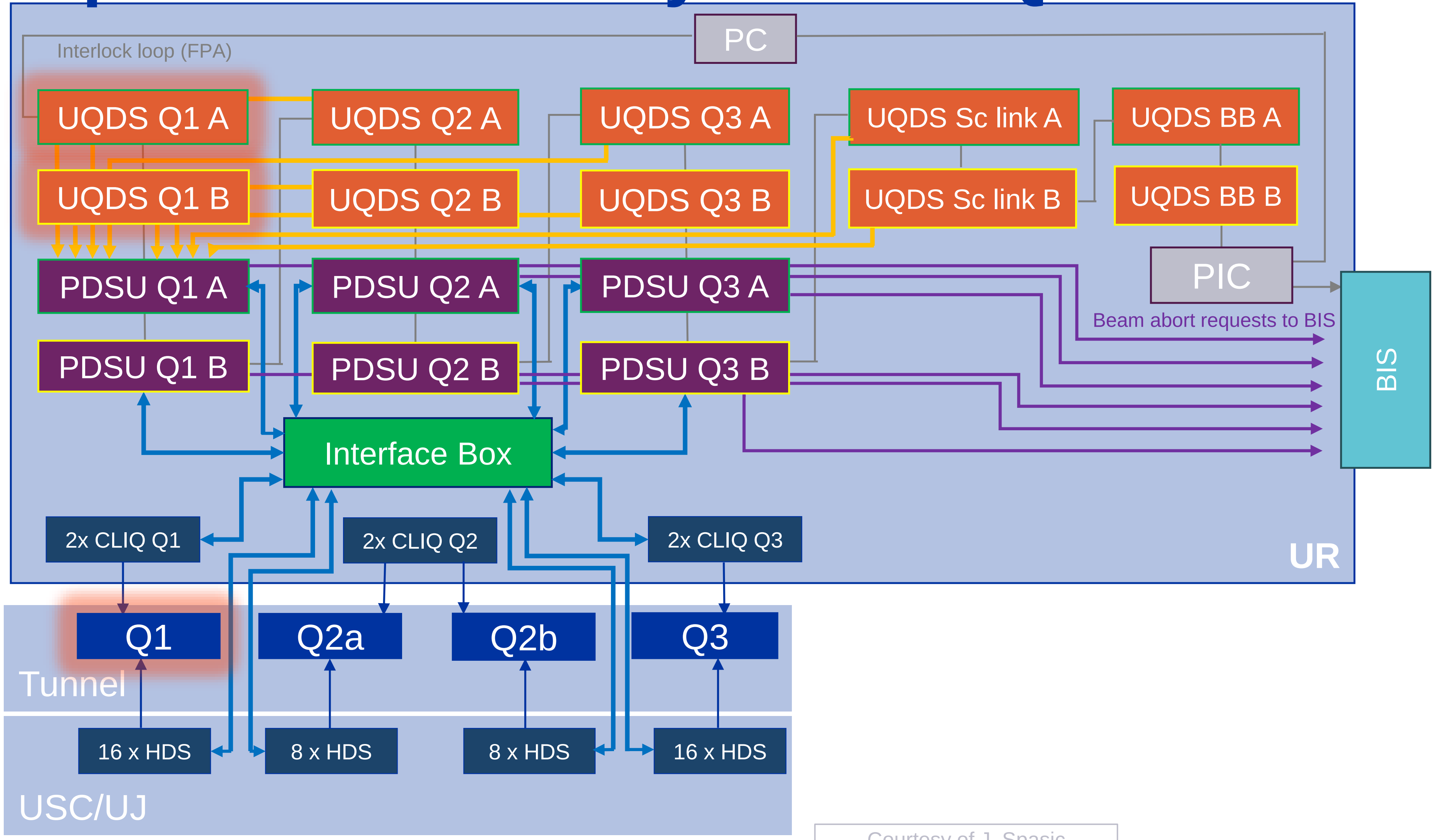


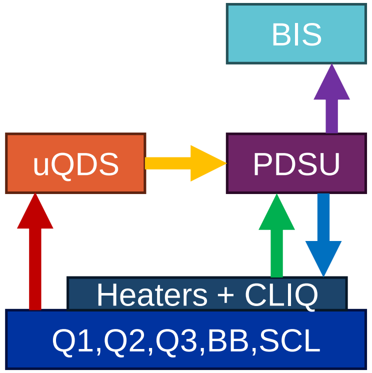

- Magnet quench

Courtesy of J. Spasic

# Top-Down Reliability Model - Quench

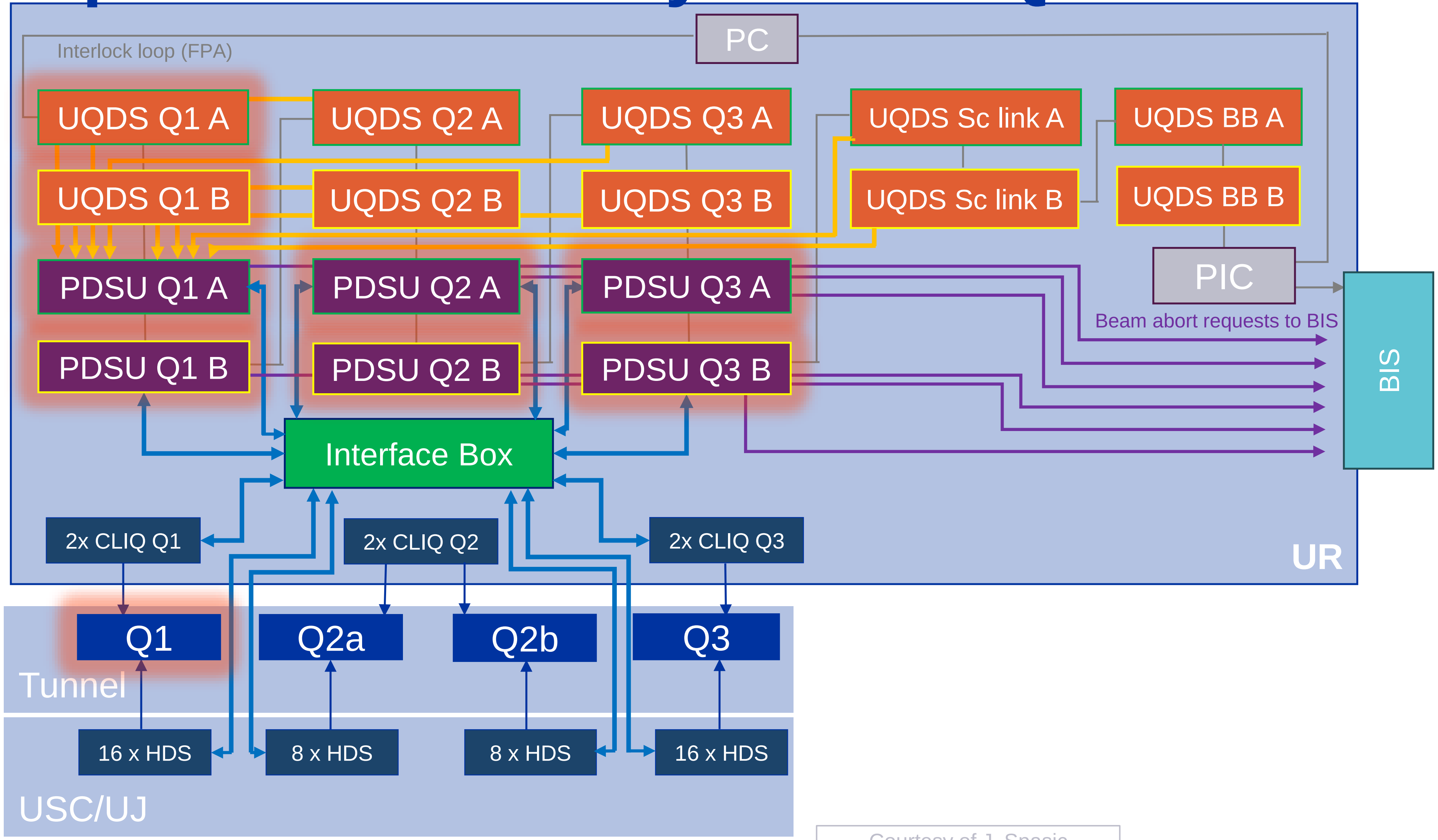



Courtesy of J. Spasic

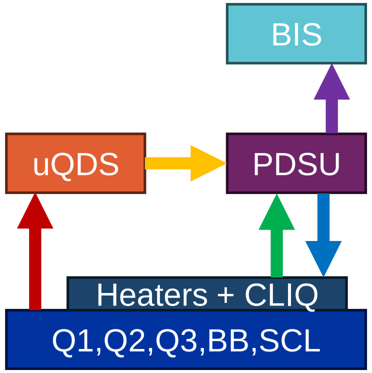



- Magnet quench
- uQDS detection

# Top-Down Reliability Model - Quench

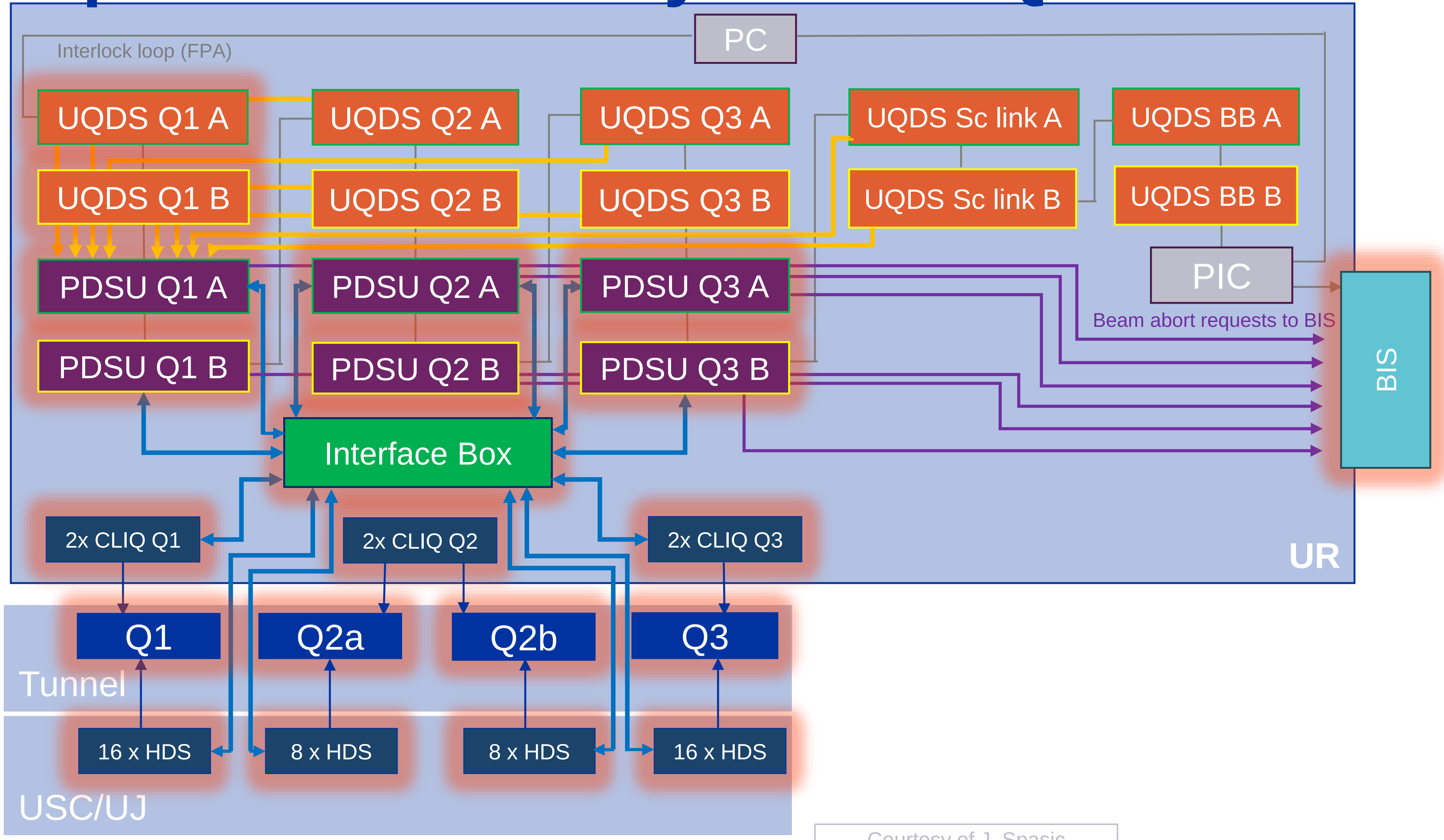


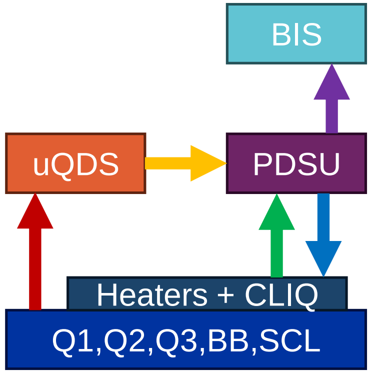

Courtesy of J. Spasic




- Magnet quench
- uQDS detection
- 6 PDSUs triggered

# Top-Down Reliability Model - Quench

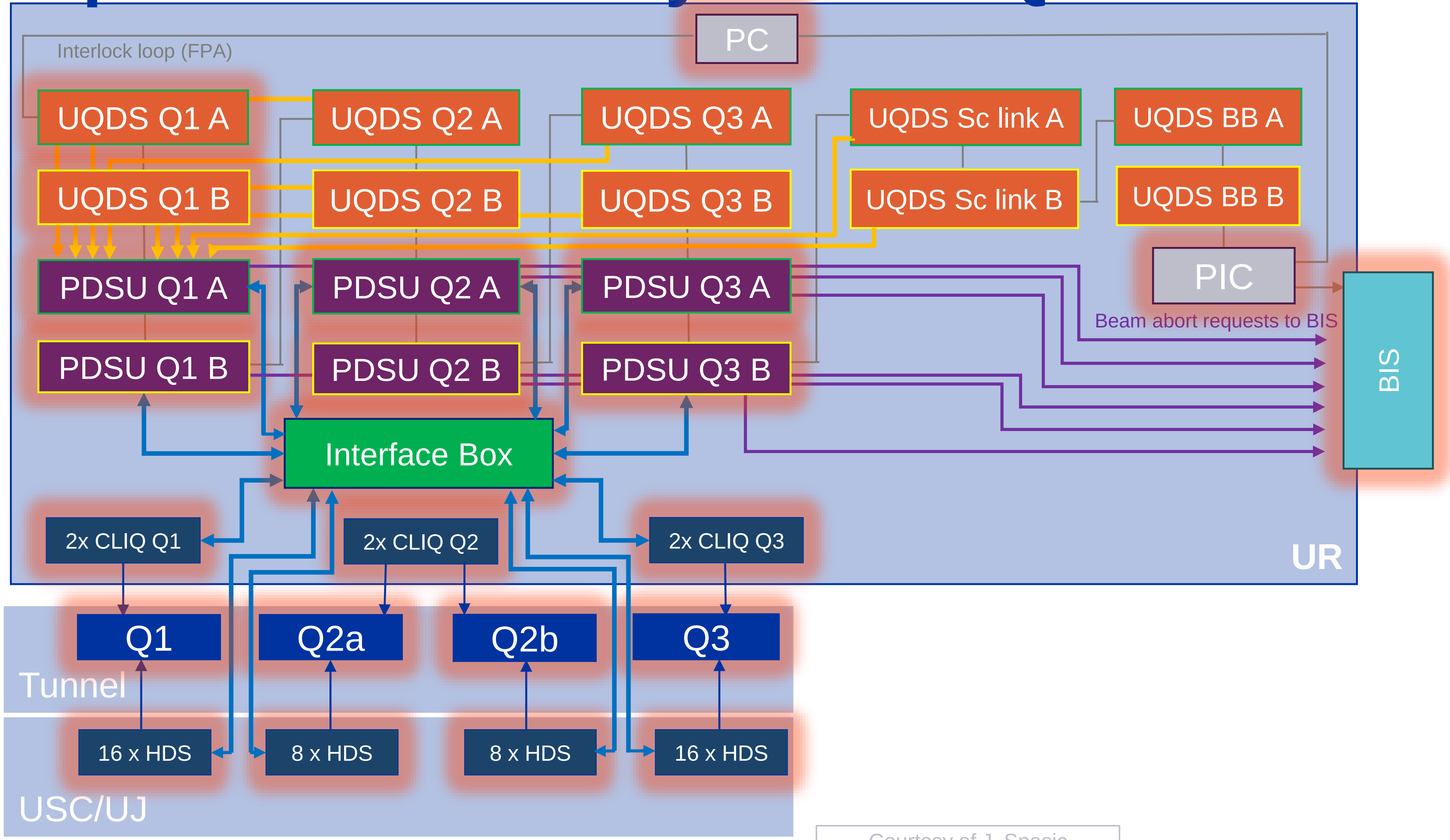


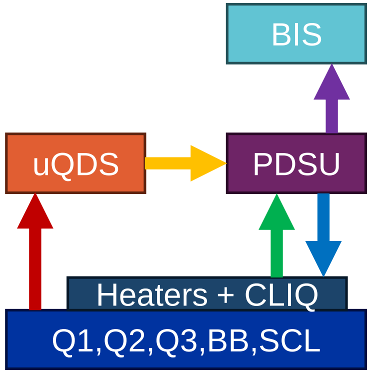

- Magnet quench
- uQDS detection
- 6 PDSUs triggered
- Beam dump & magnet protection activated

Courtesy of J. Spasic

# Top-Down Reliability Model - Quench

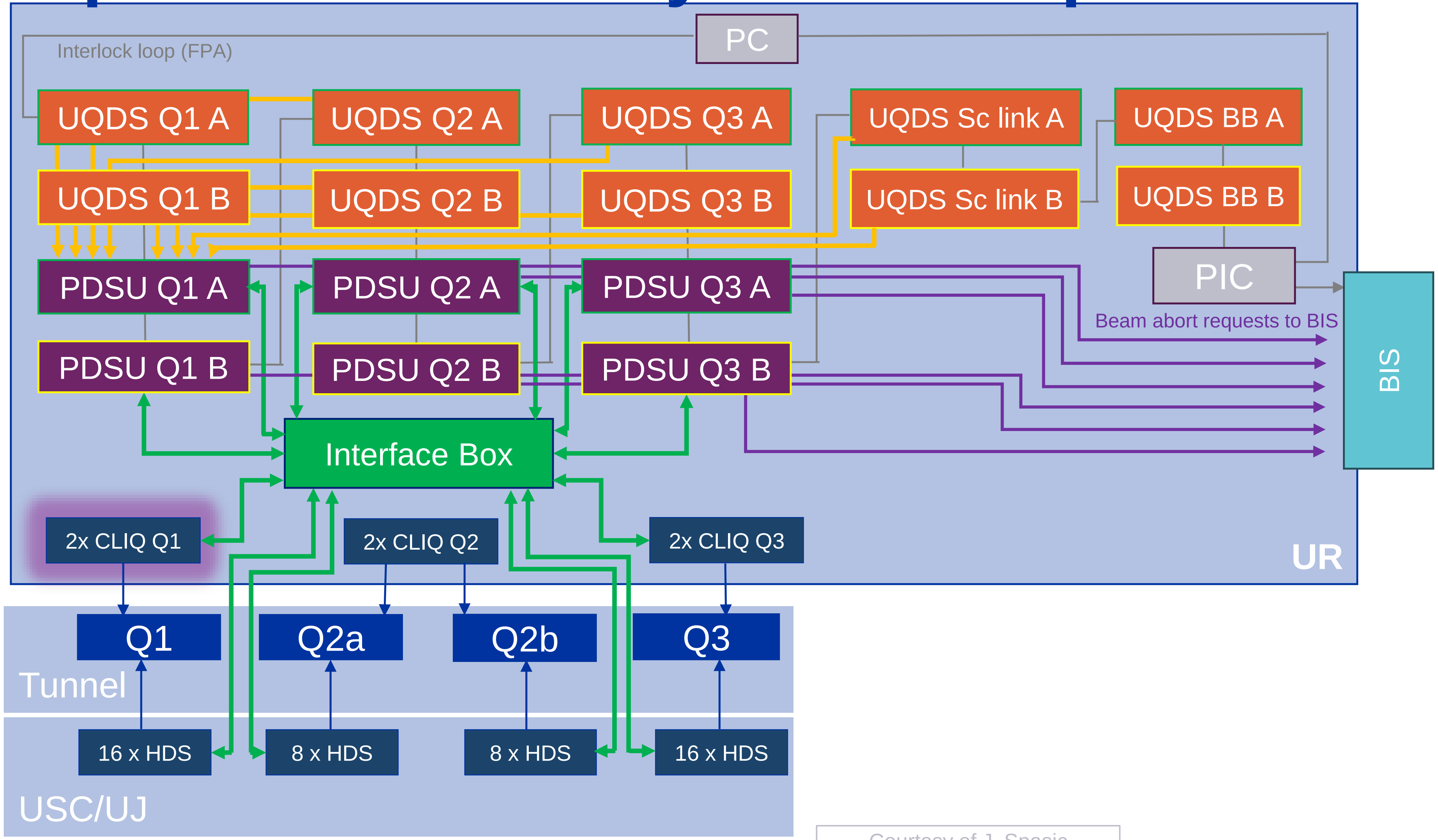



Courtesy of J. Spasic

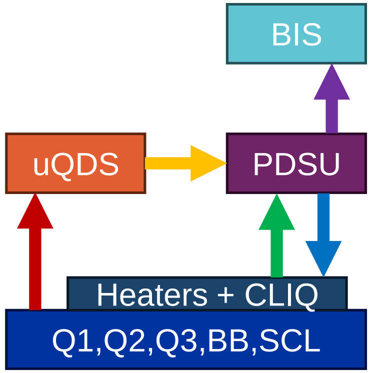



- Magnet quench
- uQDS detection
- 6 PDSUs triggered
- Beam dump & magnet protection activated
- PC stopped (beam dump via PIC not fast enough)

# Top-Down Reliability Model – Spurious Firing

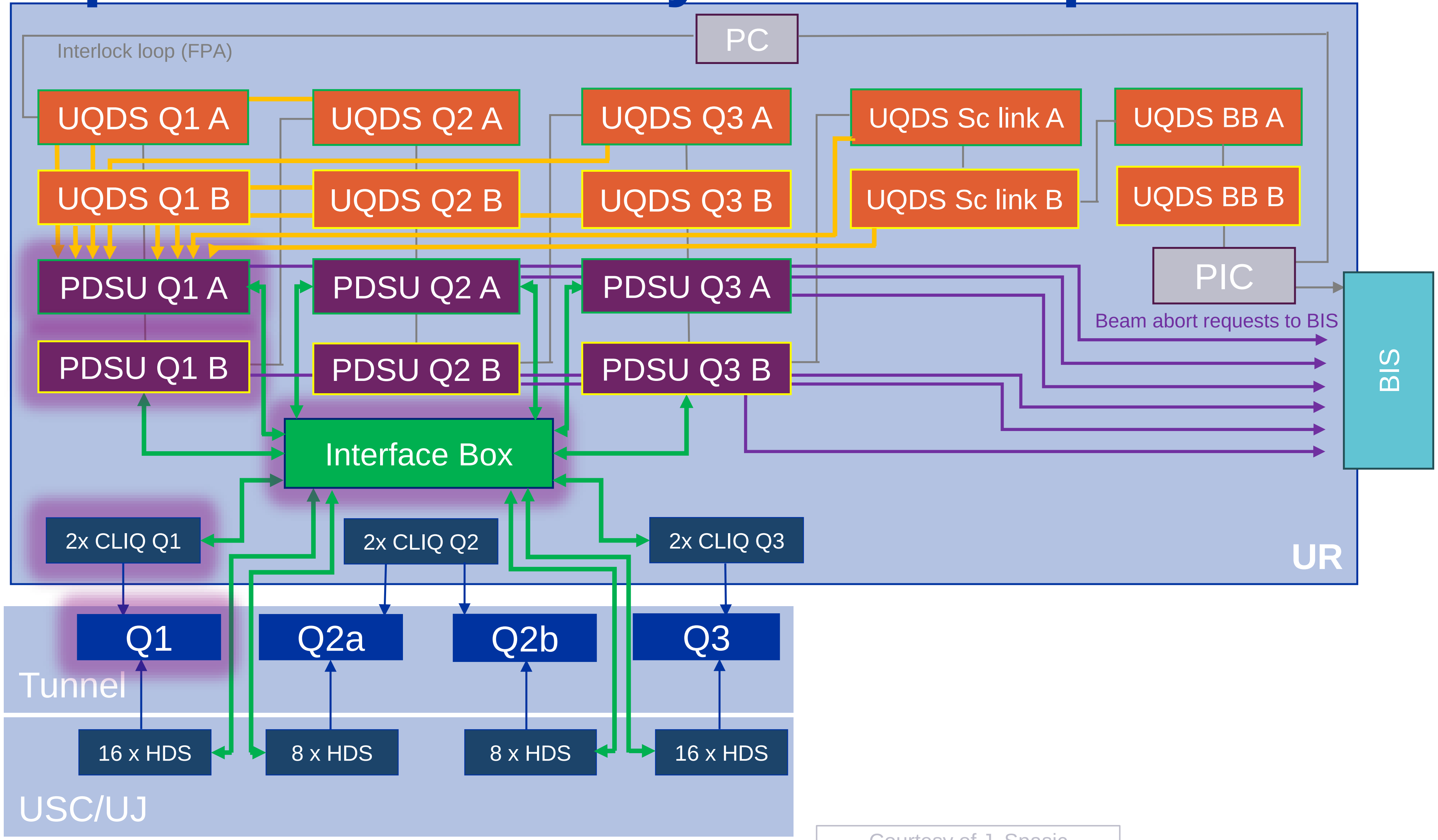



Courtesy of J. Spasic

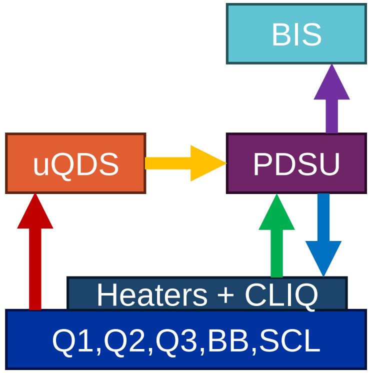



- Spurious CLIQ/HDS firing

# Top-Down Reliability Model – Spurious Firing

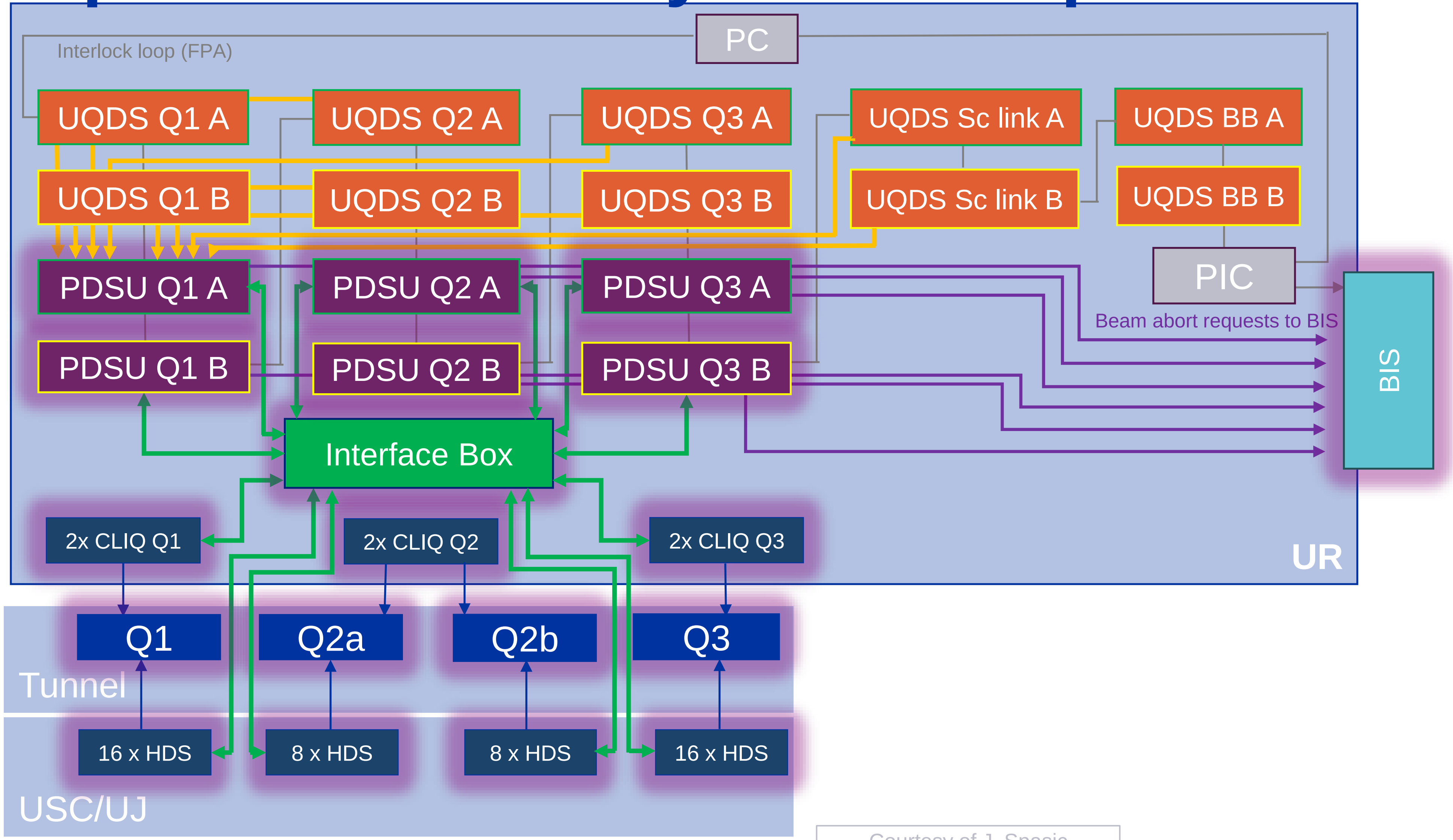



Courtesy of J. Spasic

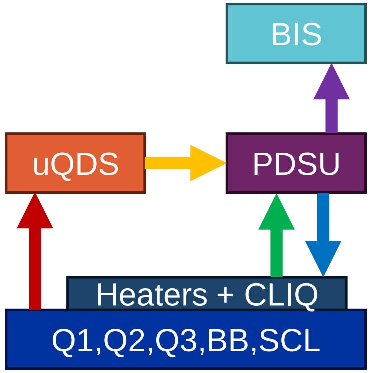



- Spurious CLIQ/HDS firing
- PDSU detects

# Top-Down Reliability Model – Spurious Firing

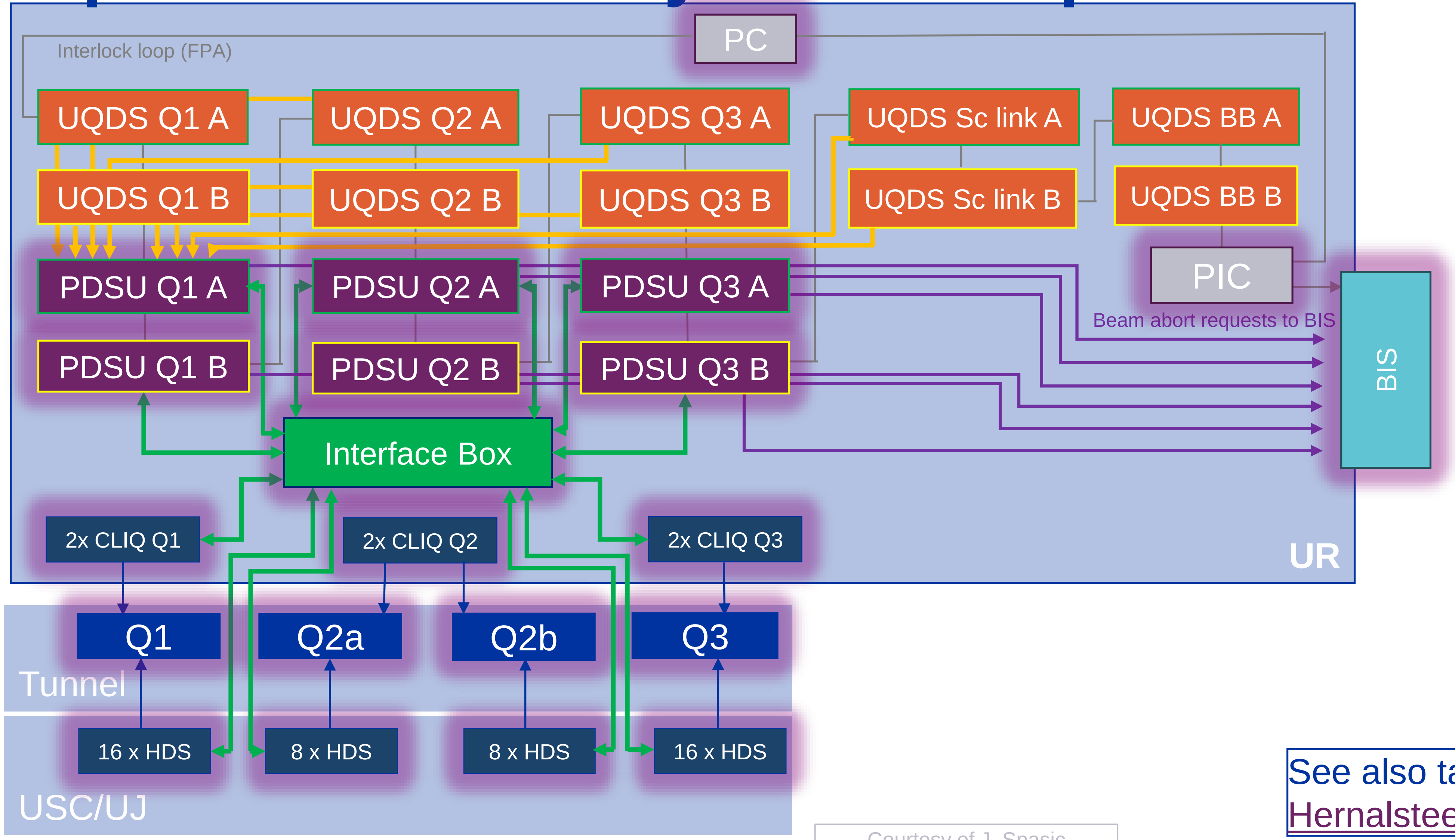



Courtesy of J. Spasic

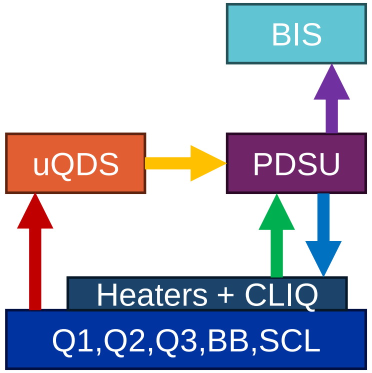



- Spurious CLIQ/HDS firing
- PDSU detects
- PDSU A/B retriggering
- Beam dump and magnet protection request

# Top-Down Reliability Model – Spurious Firing



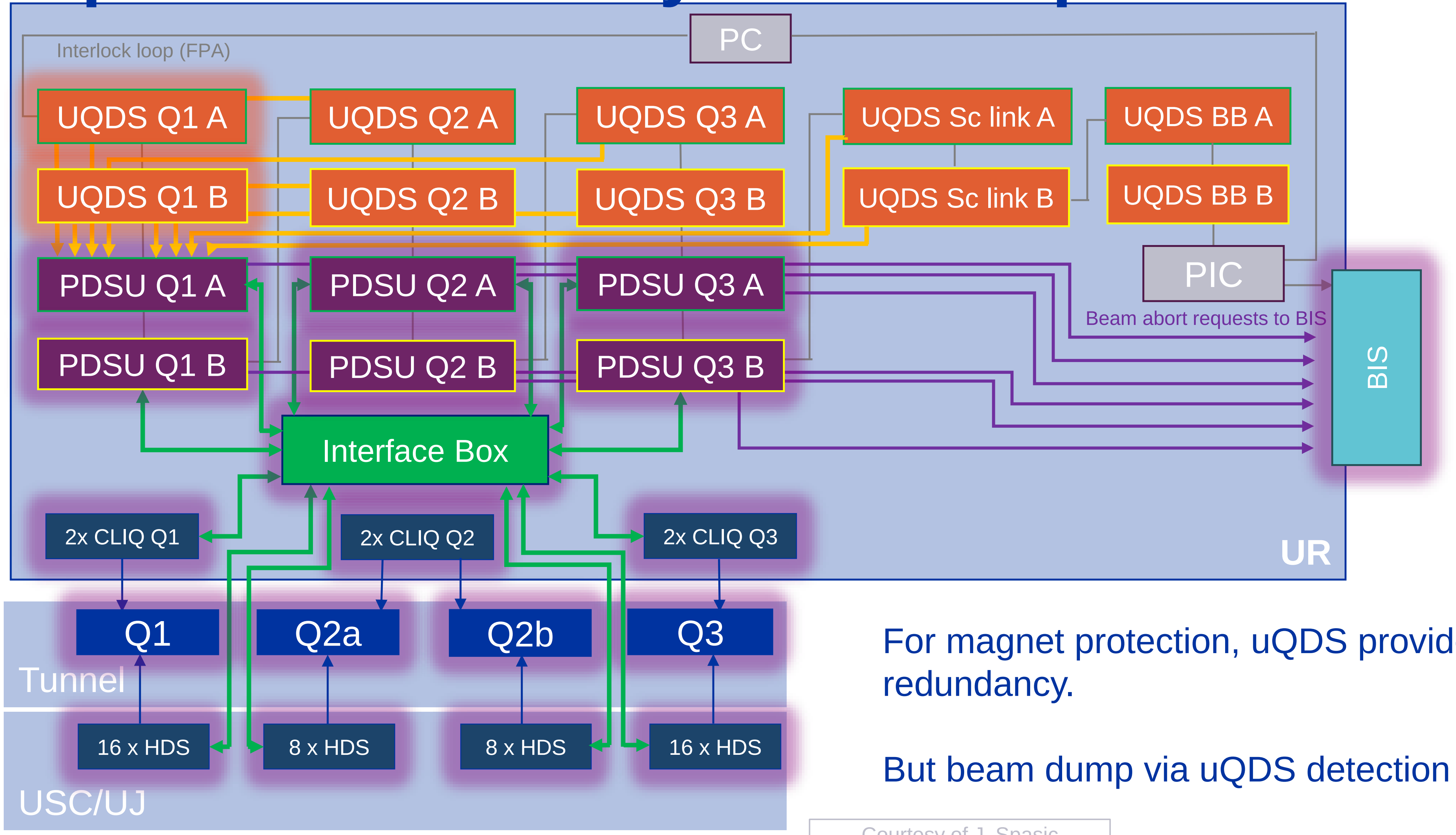

Courtesy of J. Spasic

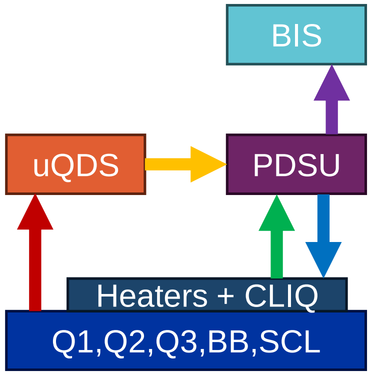



- Spurious CLIQ/HDS firing
- PDSU detects
- PDSU A/B retriggering
- Beam dump and magnet protection request
- PC stopped (beam dump via PIC not fast enough)

See also talks by C. Hernalsteens and T. Podzorny

# Top-Down Reliability Model – Spurious Firing




- Spurious CLIQ/HDS firing
- PDSU detects
- PDSU A/B retriggering
- Beam dump and magnet protection request

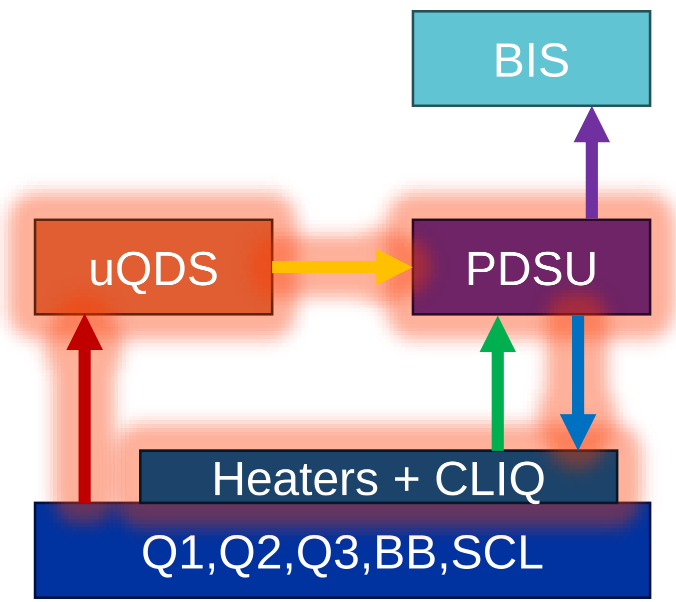
For magnet protection, uQDS provides additional redundancy.

But beam dump via uQDS detection not fast enough!

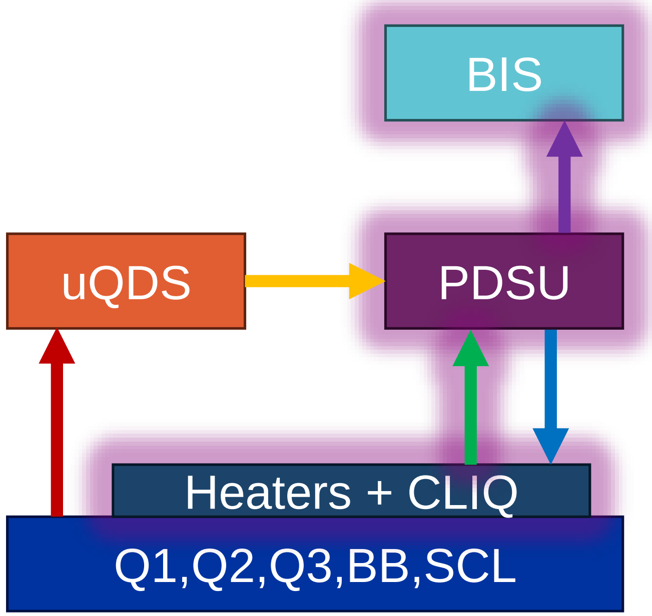
Courtesy of J. Spasic

# Top-Down Reliability Models

## Magnet Protection



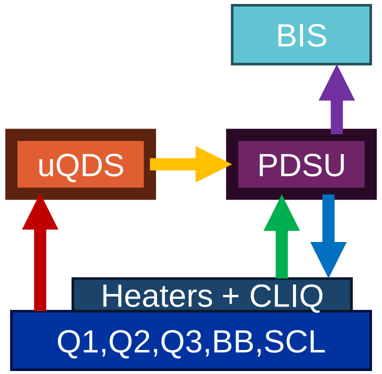

## Beam Dump/Spurious Firing

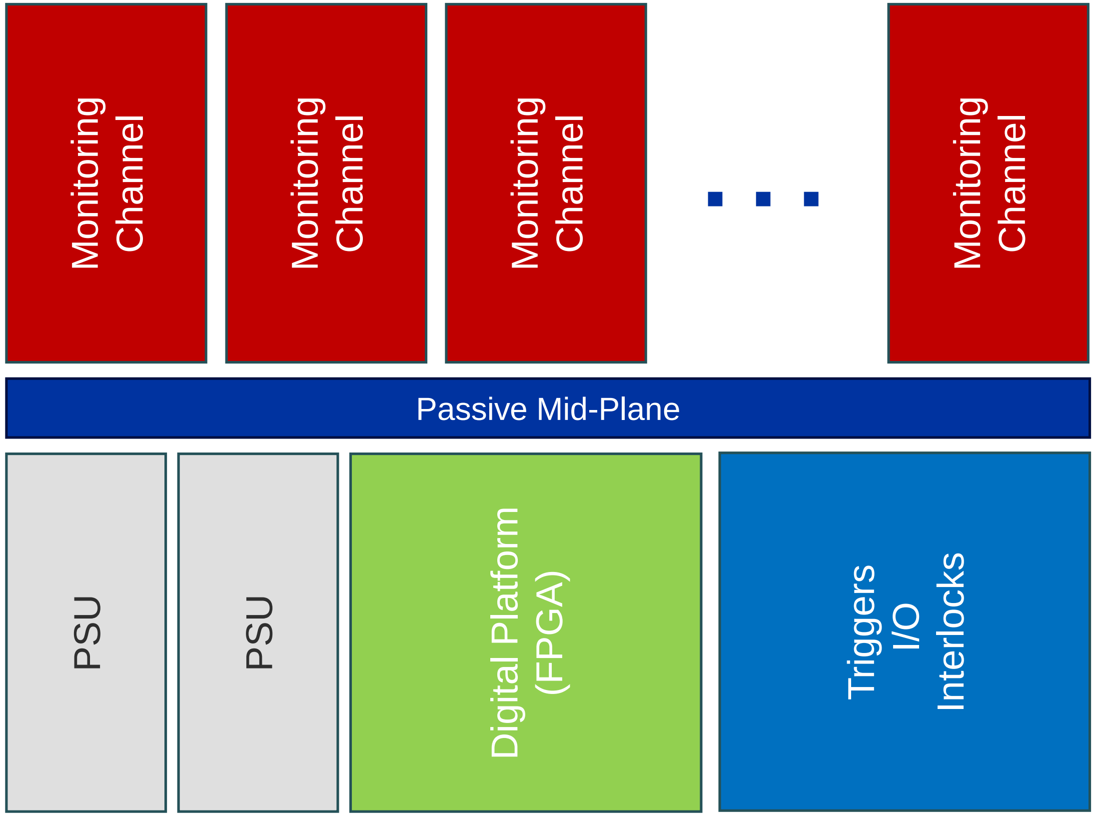



Magnet protection model ignores beam dump functionality (covered in spurious firing model)
Spurious firing model ignores magnet protection functionality (covered in magnet protection model)

# uQDS & PDSU Hardware

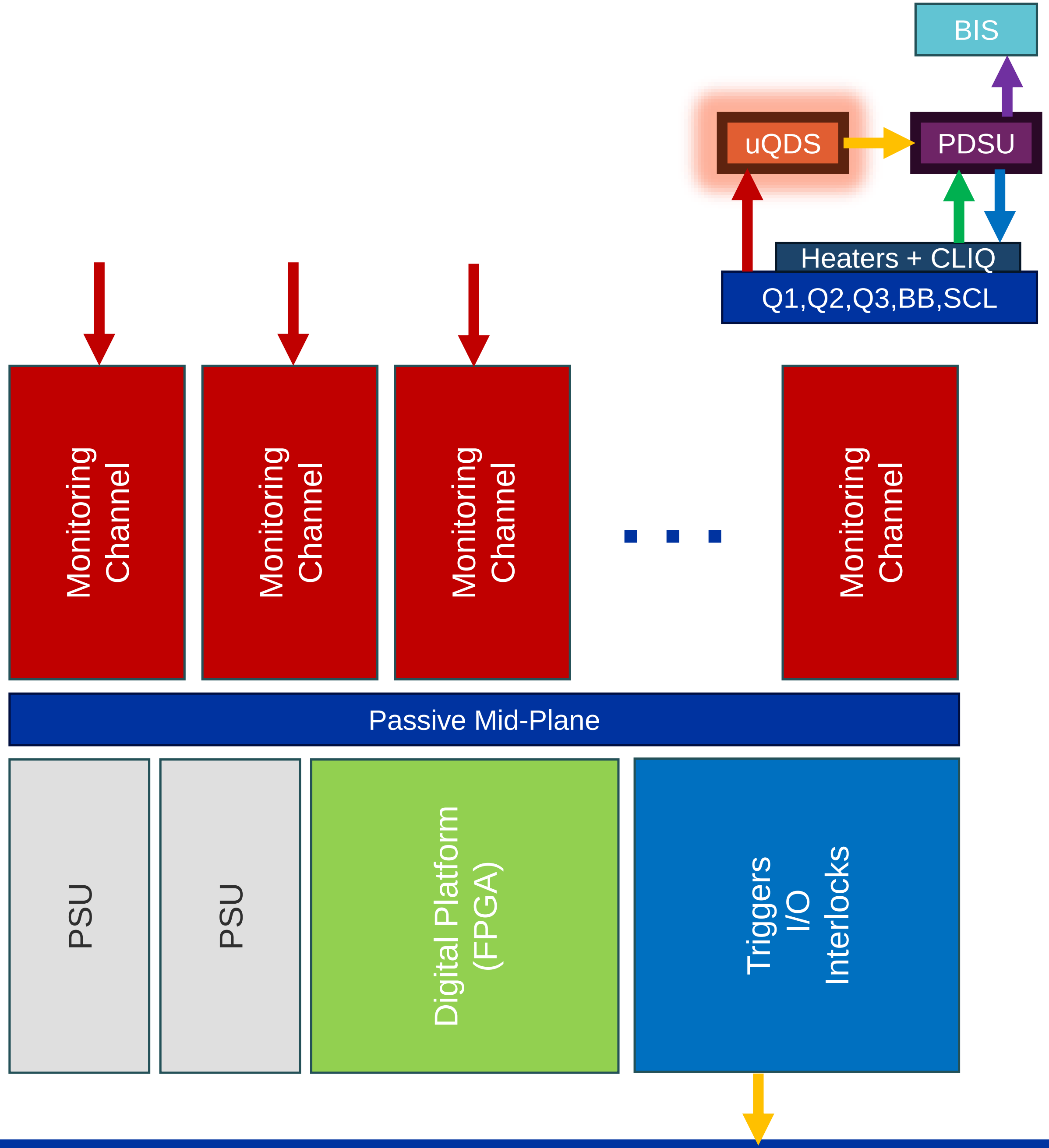
- **uQDS and PDSU share designs of hardware modules**



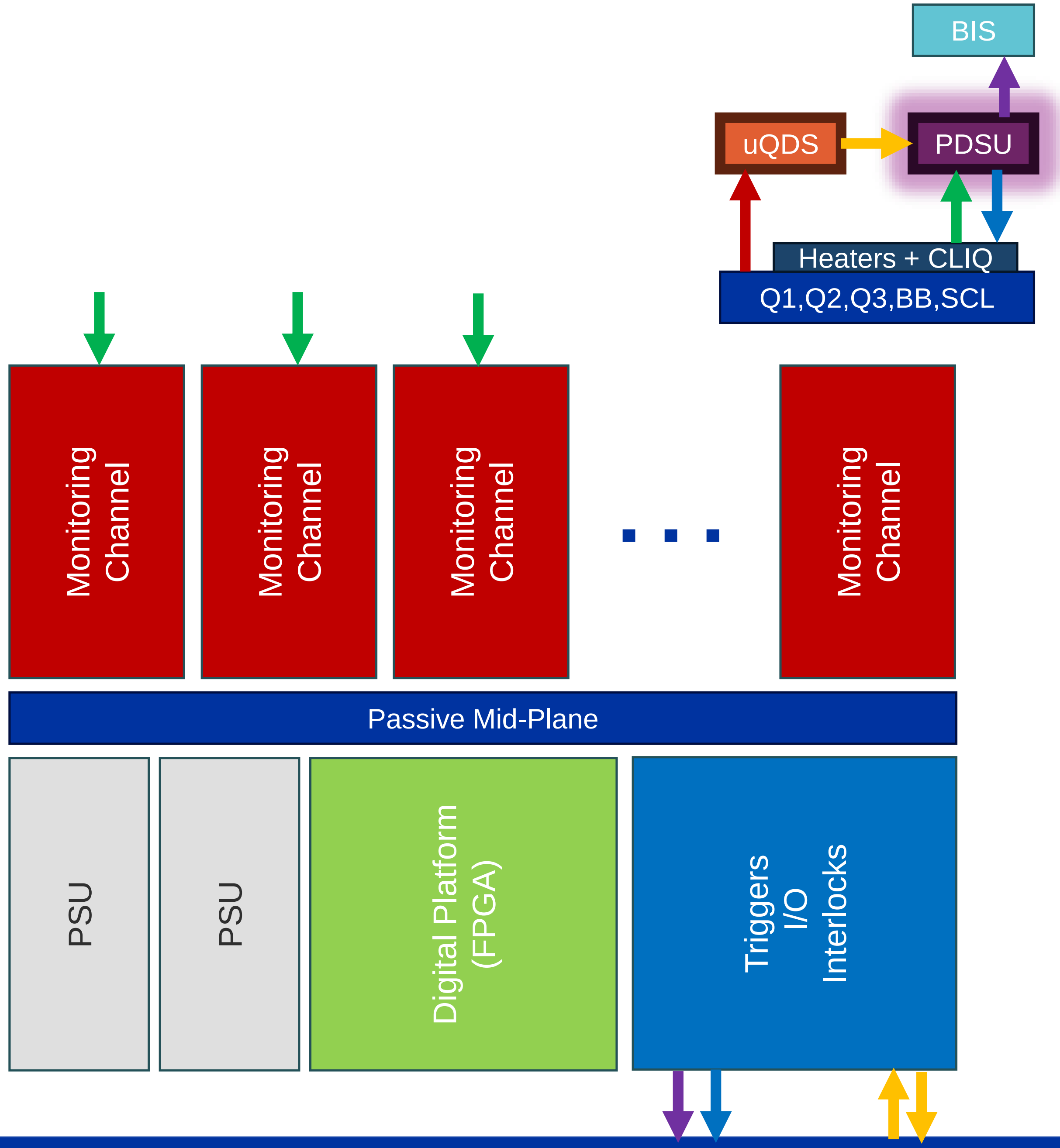
# uQDS & PDSU Hardware

- **uQDS and PDSU share designs of hardware modules**



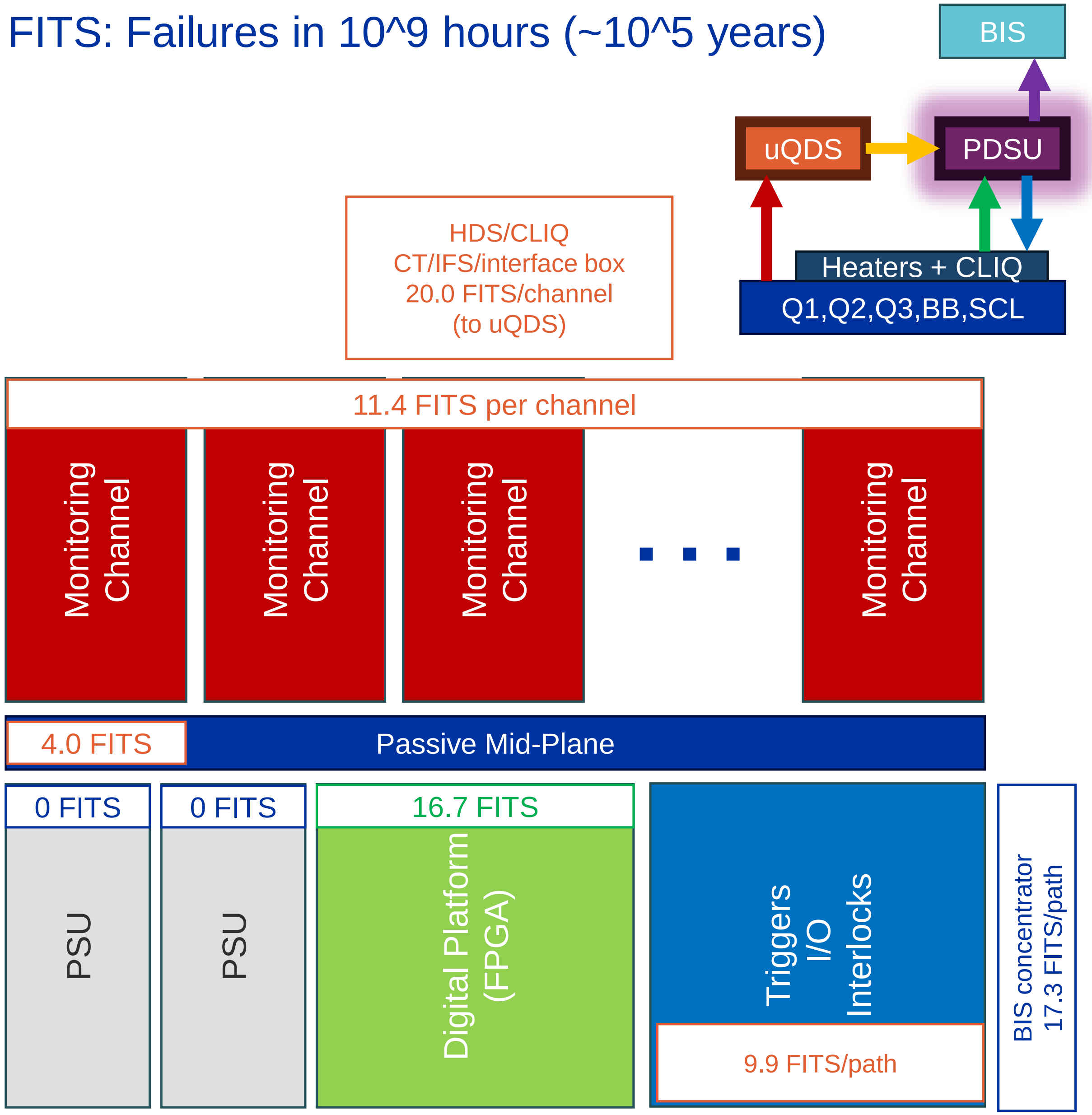
# uQDS & PDSU Hardware

- **uQDS and PDSU share designs of hardware modules**



# uQDS & PDSU FMECA

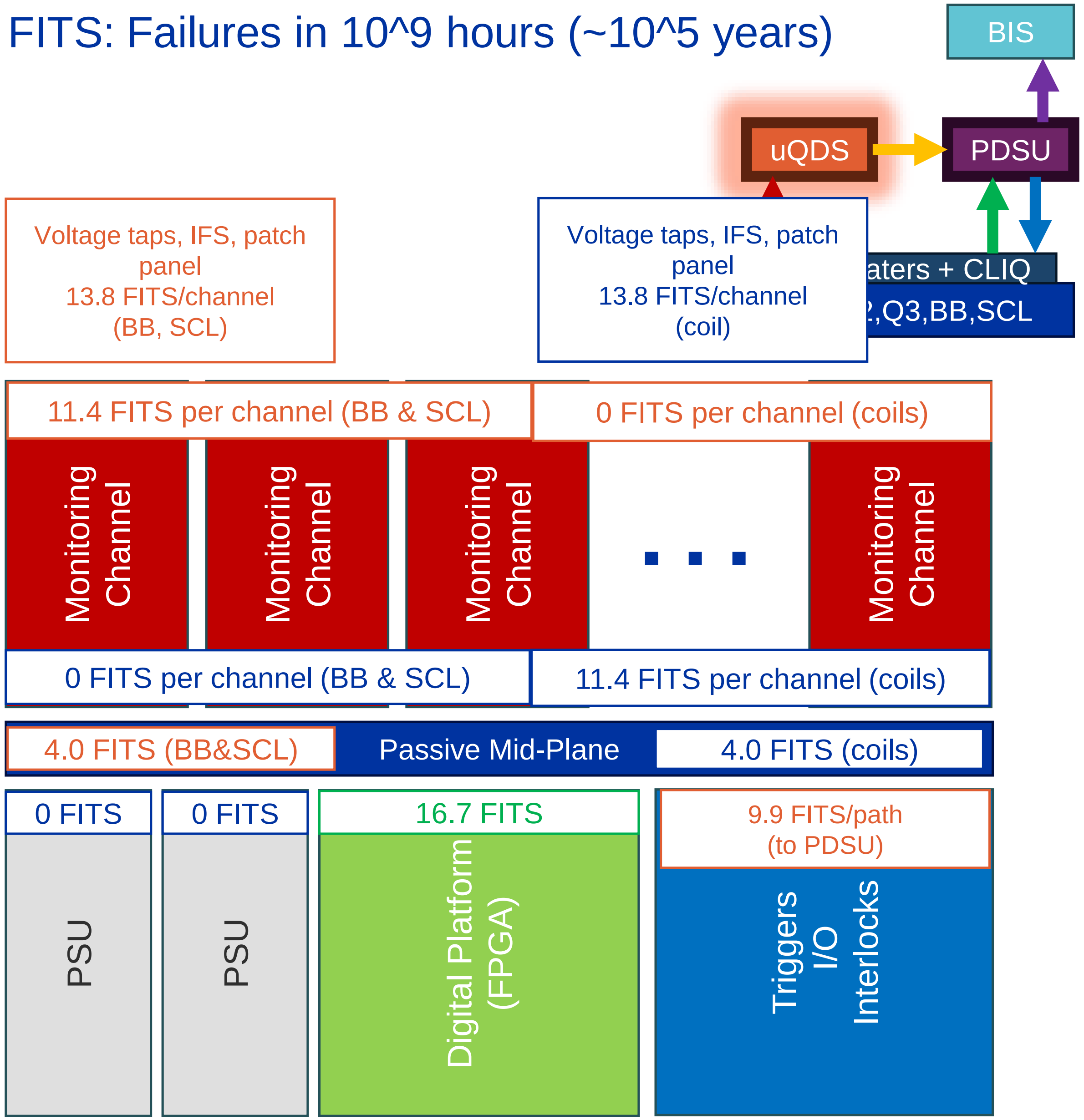
- **uQDS and PDSU share designs of hardware modules**
- **Detailed FMECA carried out for**
  - Analogue monitoring channels (similar between uQDS and PDSU)
  - Digital Platform (identical between uQDS and PDSU)
  - Approximate (pessimistic) FMECA for other modules & interfaces
- **Relevant failure mode types for magnet protection & beam dump**
  - Blind unsafe failure (detected upon commissioning or demand)
  - Blind unsafe failure (detected every fill/ramp)
  - Detected unsafe failure (visible in supervision)



# uQDS & PDSU FMECA

- **uQDS and PDSU share designs of hardware modules**
- **Detailed FMECA carried out for**
  - Analogue monitoring channels (similar between uQDS and PDSU)
  - Digital Platform (identical between uQDS and PDSU)
  - Approximate (pessimistic) FMECA for other modules & interfaces
- **Relevant failure mode types for magnet protection & beam dump**
  - Blind unsafe failure (detected upon commissioning or demand)
  - Blind unsafe failure (detected every fill/ramp)
  - Detected unsafe failure (visible in supervision)

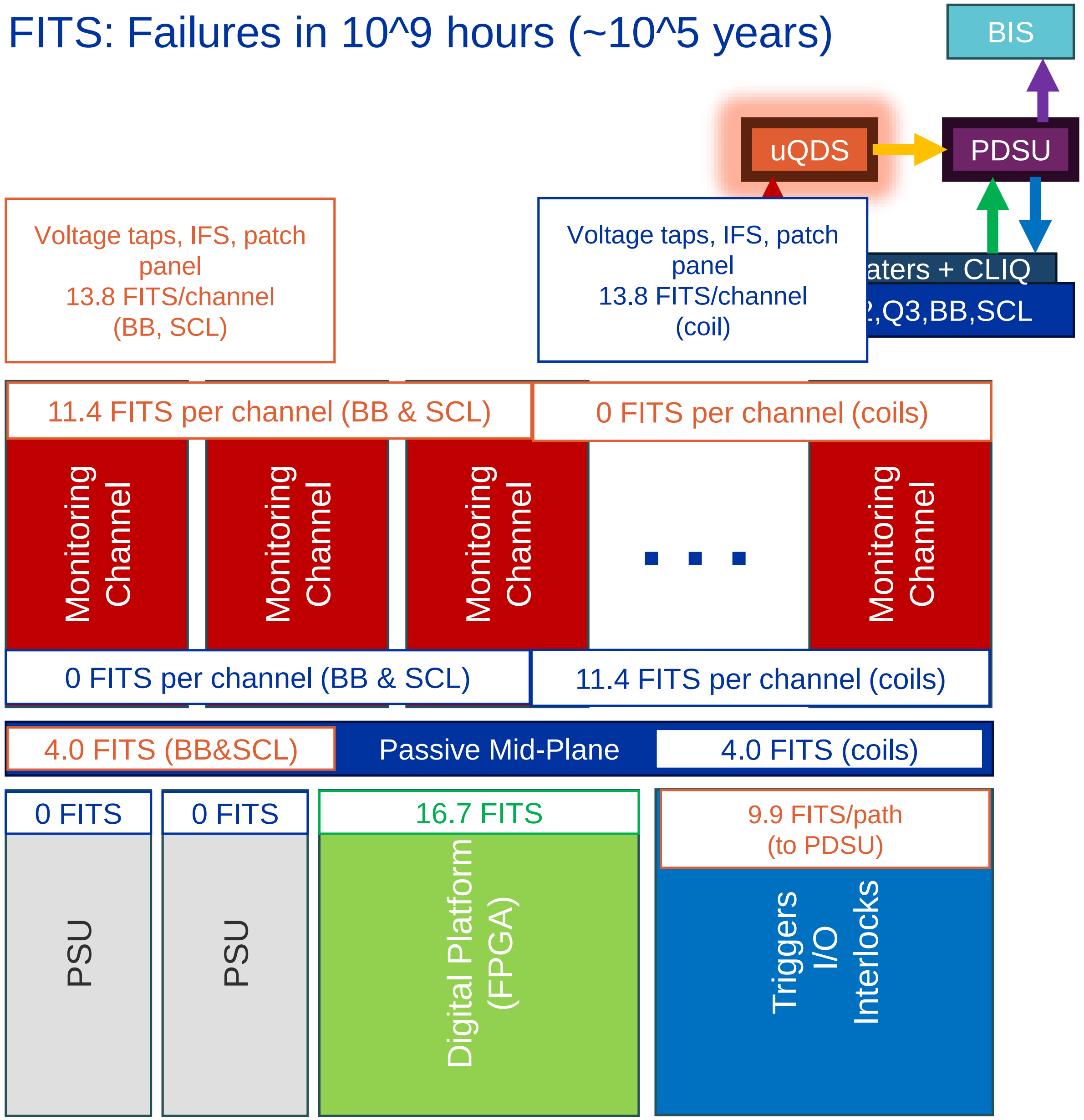
FITS: Failures in 10^9 hours (~10^5 years)



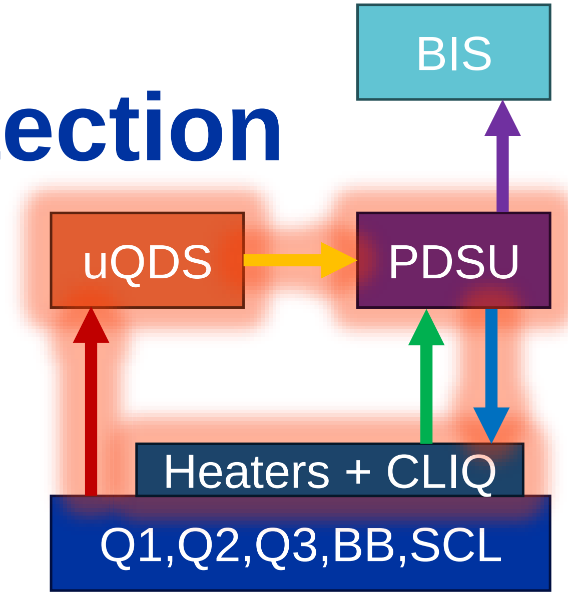
# uQDS & PDSU FMECA

- **Component failure rate source is 217+ electronics reliability prediction & FMD91/2016 standard**
  - Values apply for indoor, stationary mission profile during useful lifetime
- **If end effect unclear, pessimistic choice taken**
- **Certain end effect assignments should be validated by functional tests in hardware**
  - E.g. behavior under 3.3V voltage rail drift, ADC behavior under reference voltage drift
- **FMECA process identified parts of design that may be optimized further for QDS CONS design for main dipole magnets**
  - E.g. placement of additional pull up/down lines in channel

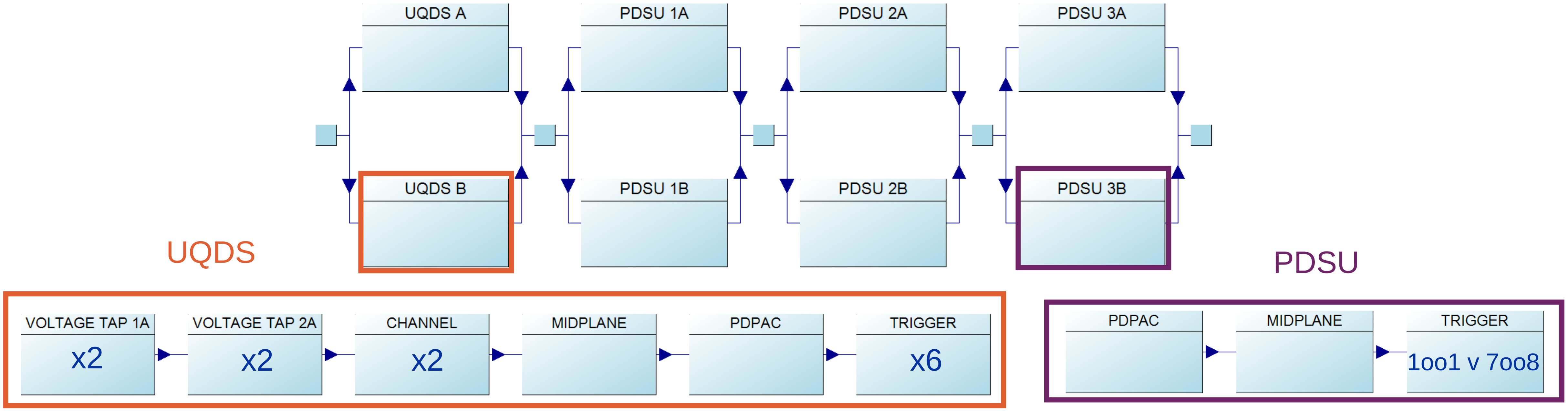
FITS: Failures in 10^9 hours (~10^5 years)



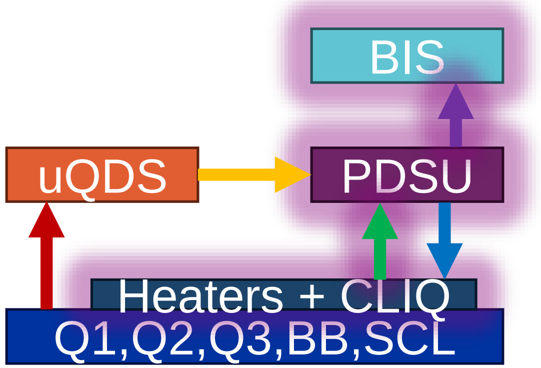
# Top-Down Reliability Model – Magnet Protection



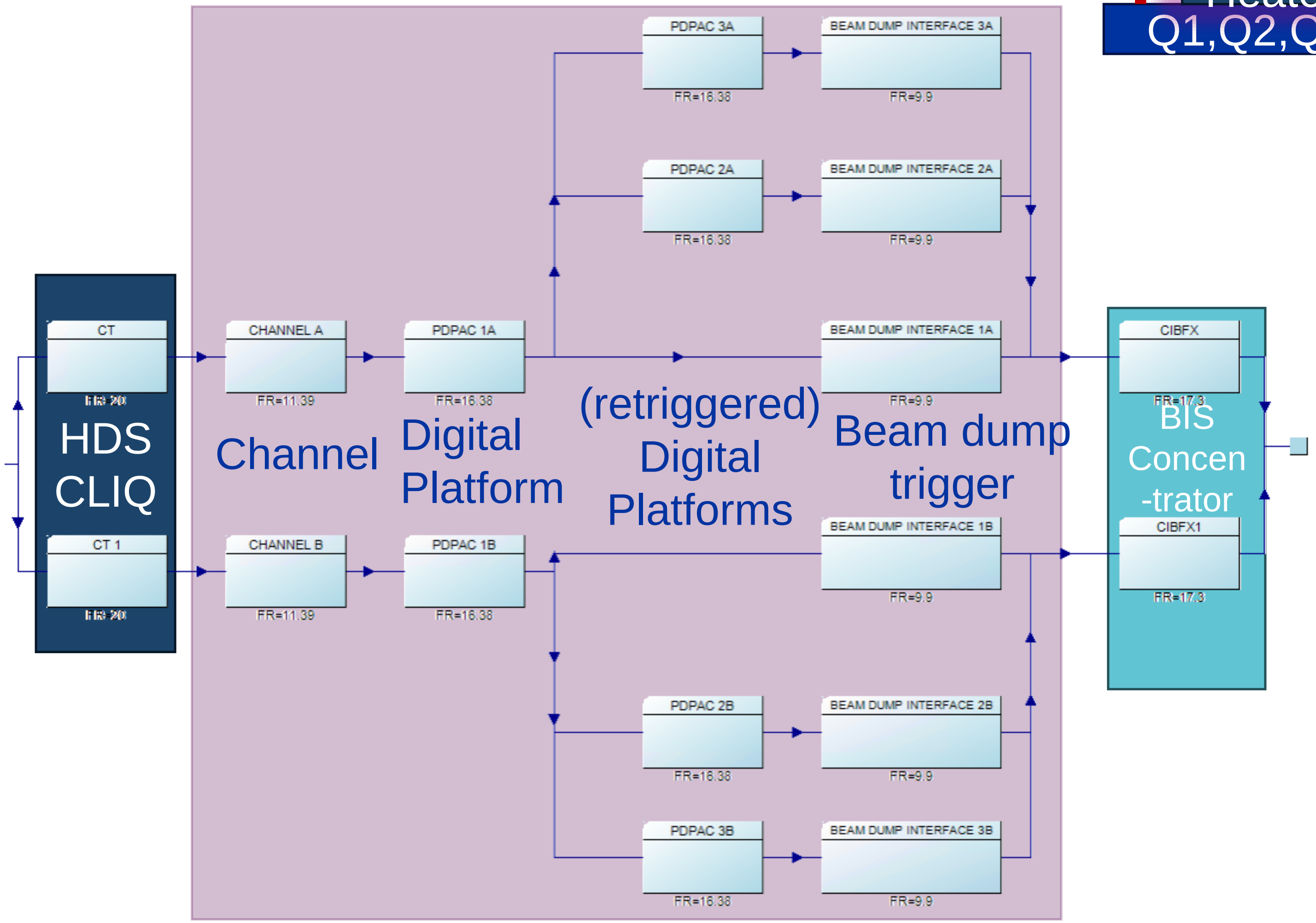

- **Complexity of model required making pessimistic simplifications**
  - Comparison with full redundancy structure confirmed that error is tolerable
- **Heaters & CLIQ modeled previously in IT protection systems study**



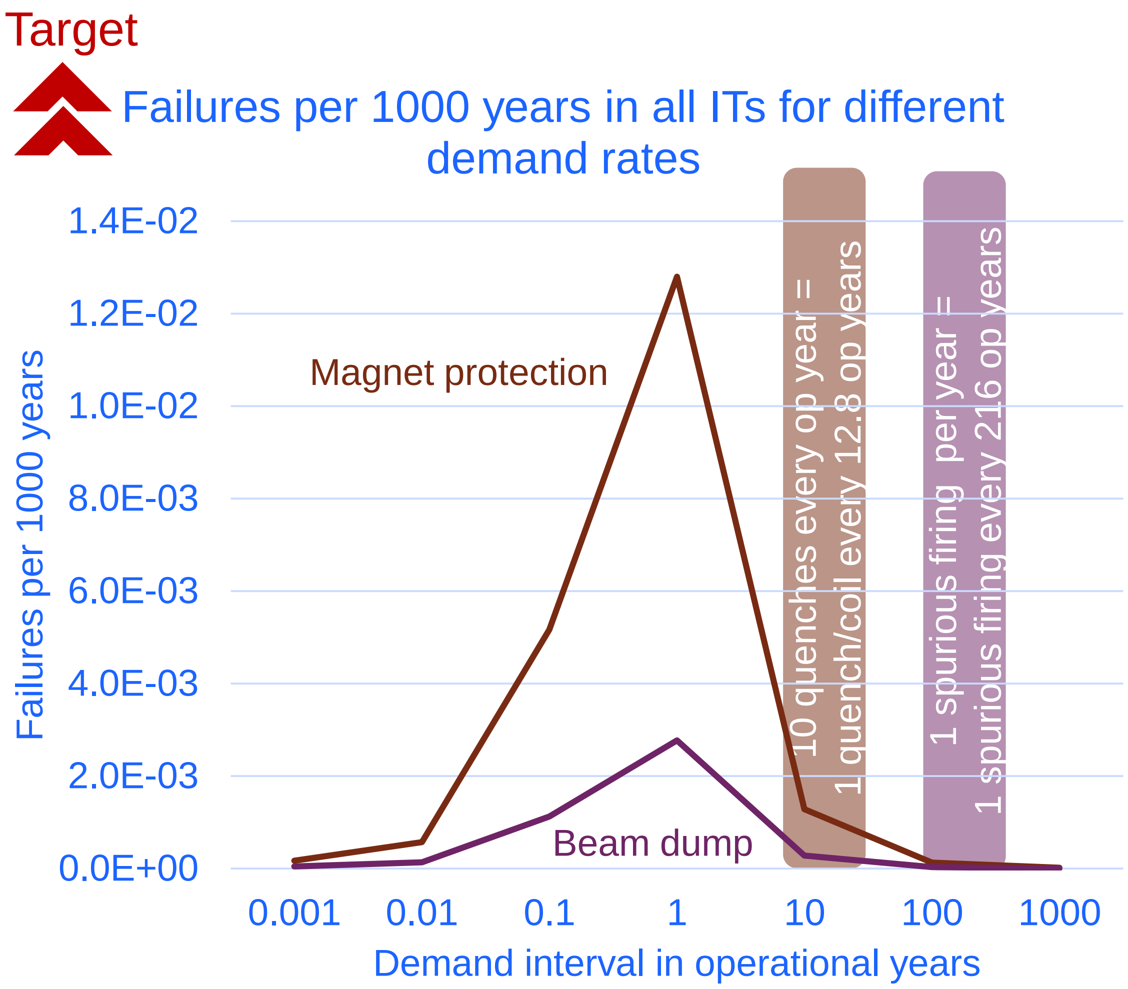
# Top-Down Reliability Model – Beam Dump/Spurious Firing




- **Few pessimistic simplifications required**
- **HDS case shown, as CLIQ has additional redundancy in read-out**
  - Clear separation of redundant paths as PDSU retriggering does not re-trigger between paths A & B
- **BIS concentrator**
  - New CIBFX design
  - Originally developed for EPC use cases
  - Reliability study as part of [BISv2 reliability study]



# Results – Failure Rates




**Repair/Inspection Policy:**

- **Commissioning: 1 operational (op) year = 7200 hours/300 days**
- **Ramp detection interval: 12 hours**
- **Reaction to Supervision: 12 hours**

**Magnet protection: 128 instances that can have a single quench**

**Beam dump: 216 instances that can have a spurious trigger**

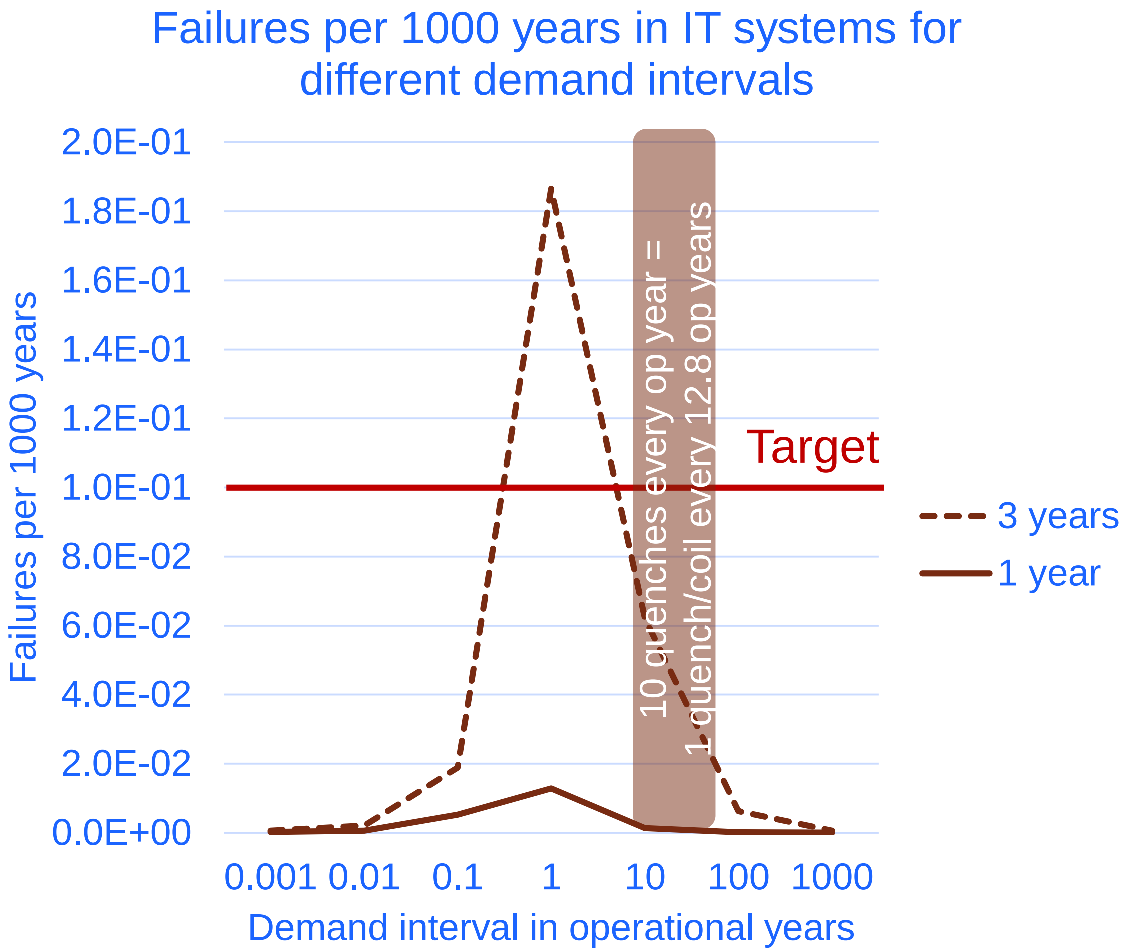
- **Maximum number of failures when the demand interval approaches the commissioning interval**
  - Magnet protection less reliable, mainly due to longer chain of systems in critical path

→ **For both protection functions the reliability target is comfortably met.**

→ But under the condition of regular systematic testing

# Commissioning interval

## Magnet protection




**Repair/Inspection Policy:**

- **Commissioning:** ***1 or 3*** **operational years**
- **Ramp detection interval:** **12 hours**
- **Reaction to Supervision:** **12 hours**

**Magnet protection: 128 instances that can have a single quench**

**Beam dump: 216 instances that can have a spurious trigger**

- **With a commissioning interval of 3 years instead of 1 year, the number of failures increase**
  - Mainly due to the probability of blind failures accumulating that are only visible in commissioning or on demand.
    - Difference smaller if demand rate is higher

→ **With 3-year intervals, the reliability target is not met**

→ **Yearly quench test is recommended**

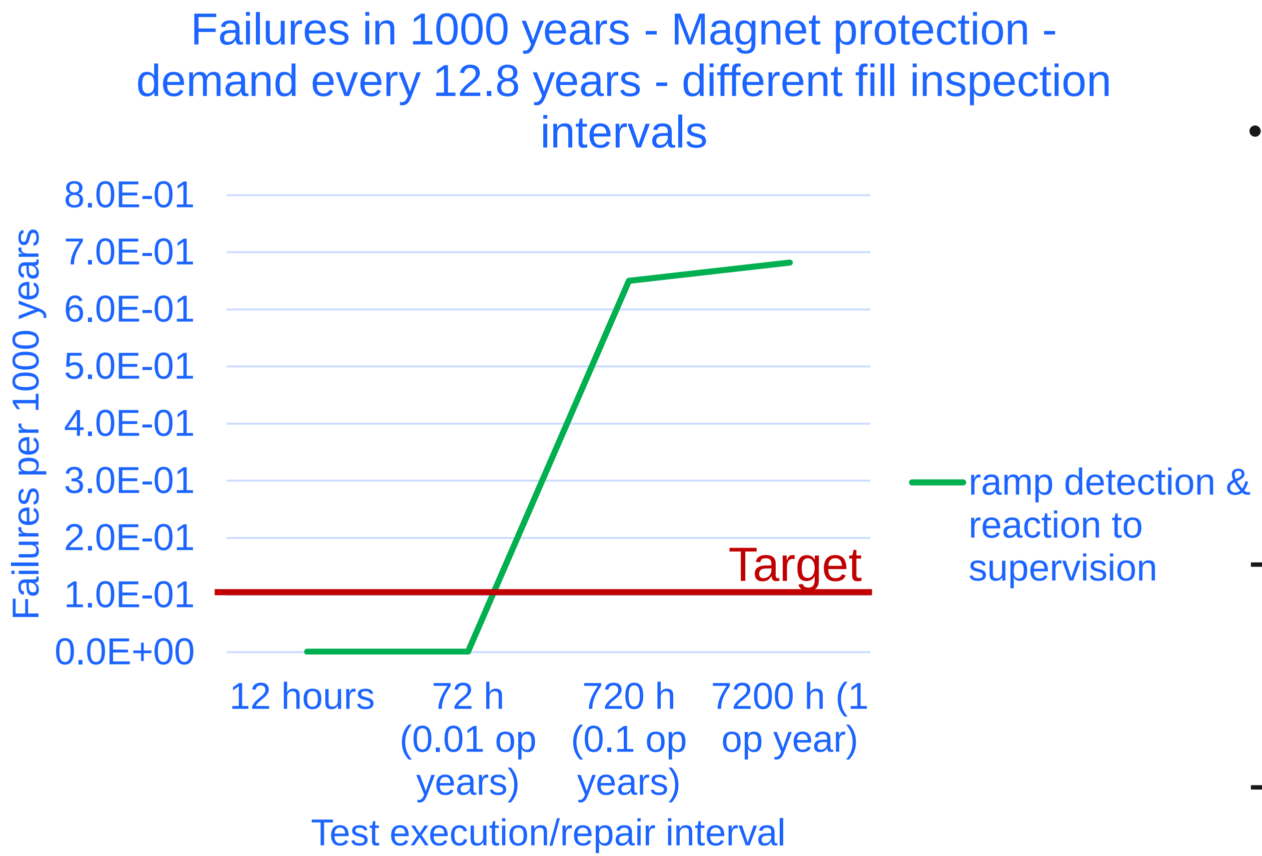
# System Monitoring & Testing
## Magnet protection

**Repair/Inspection Policy:**

- **Commissioning: 1 operational (op) year**
- **Ramp detection interval: 12 hours → 7200 hours**
- **Reaction to Supervision: 12 hours → 7200 hours**

**Magnet protection: 128 instances that can have a single quench**

**Beam dump: 216 instances that can have a spurious trigger**




- **Strong impact of less frequent/imperfect testing**
  - Only a small increase of about 1.1E-05, if the failures are detected and repaired after 72 hours.
  - Maximum of 6.8E-01 failures if the failures are detected for the first time during yearly commissioning.
    - This assumes an interlock of operation (SIS) if both critical paths lose supervision.

→ **Monitoring & ramp testing is crucial for protection function!**

→ Extending coverage yields additional reliability margins

→ **Detected problems can be fixed after fill**

→ Do not need to stop operations

# Conclusions & Next Steps

- **A reliability model for the quench protection and beam dump functions of the IT shows**
  - The foreseen uQDS, PDSU and BIS concentrator hardware design conforms with the reliability requirements
  - This is under the condition that
    - yearly commissioning tests are performed (IST) to check the integrity of the system and all interfaces
    - an automated test during ramp is executed every LHC fill as part of a sequencer task to check integrity of the system
- **Follow-up of the study**
  - The uQDS/PDSU FMECA analysis results should be validated by selected HW functional tests/simulations
  - Availability aspects of the system to be quantified and checked against operational data
  - An analysis of critical firm- and software and configuration management should complement the hardware study
- **In view of the consolidation of the LHC main dipole QDS system**
  - The reliability model should be adapted, and pessimistic assumptions refined
  - Design improvements triggered by uQDS/PDSU FMECA analysis should be implemented if possible

# Protection System Life Cycle

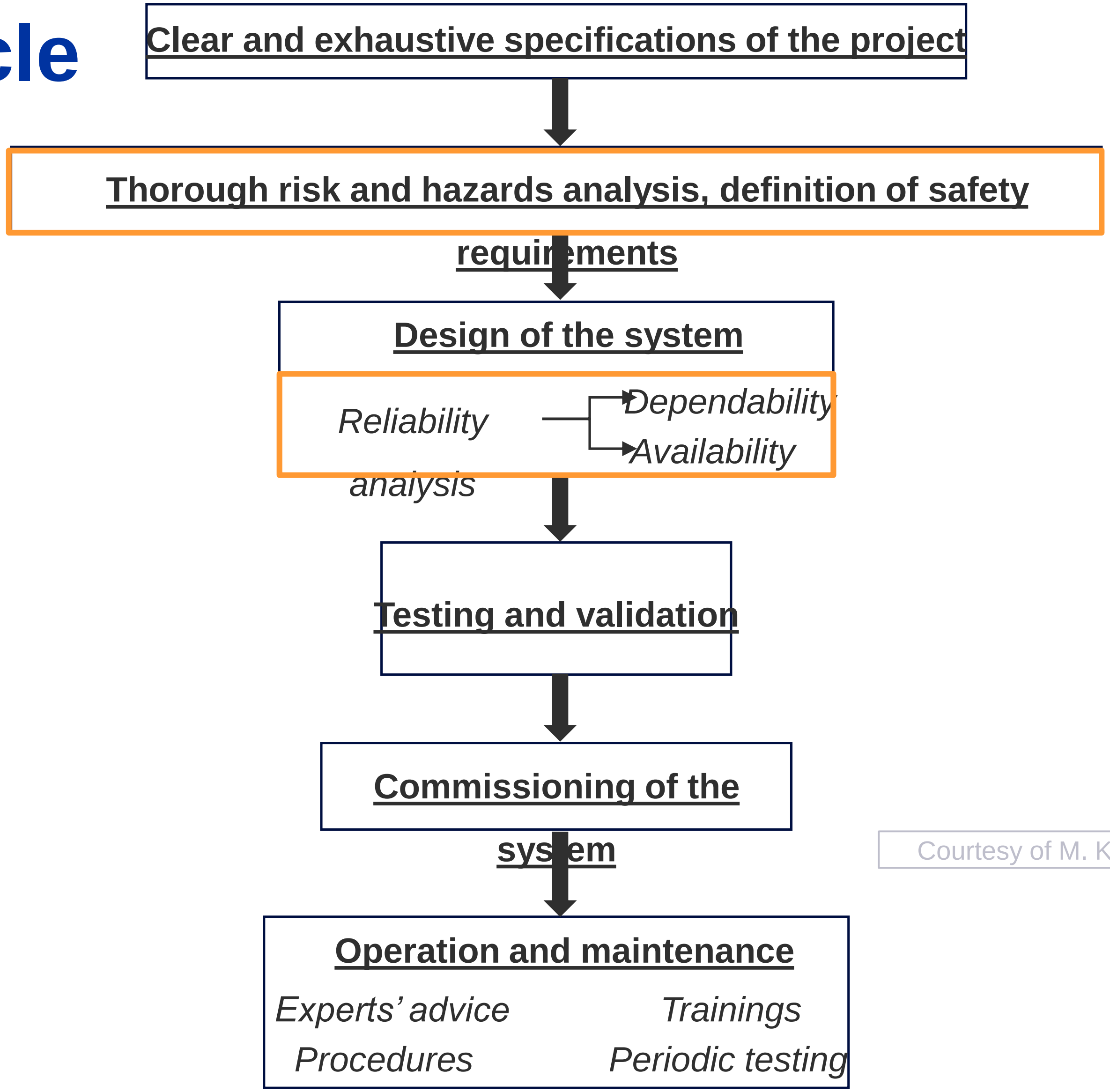
**Machine Protection systems development follows defined life-cycle**

**Ensures that risks are mitigated**

**Inspired by IEC 61508 and adapted for CERN context**

**The scope of the uQDS & PDSU reliability analysis is to**

- Identify risks and hazards and quantify requirements for their mitigation
- Qualify the detailed hardware design according to the defined requirements




Courtesy of M. Kalinowski

# Component-Level FMECA - Introduction

**Failure Modes, Effects, and Criticality Analysis** (FMECA)

**Purpose:** identify potential failure modes of individual components within a system & quantify failure impact at system level

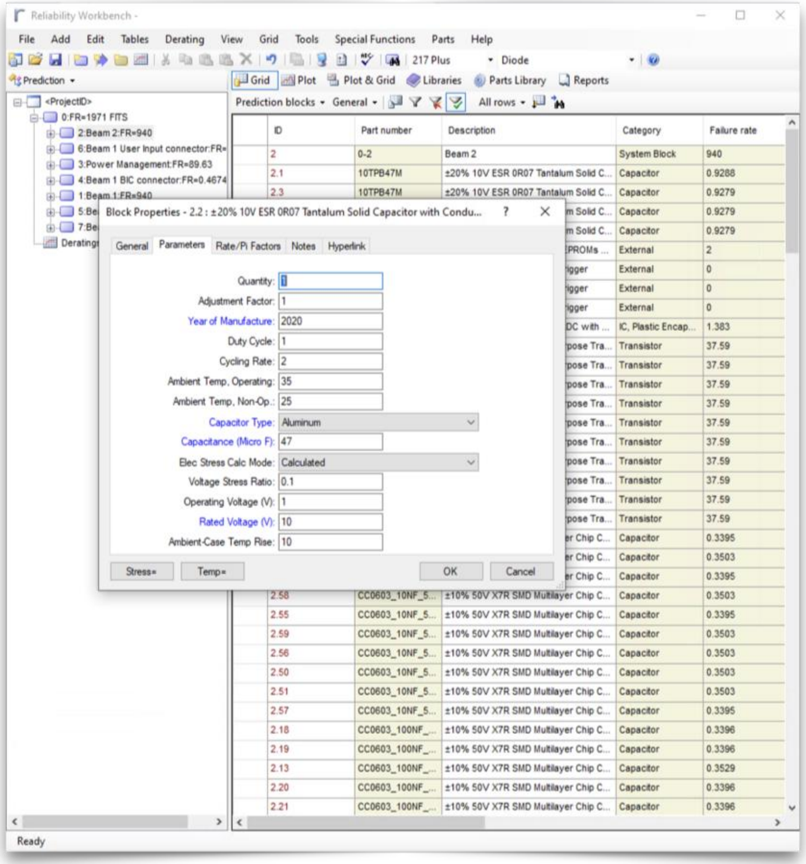
| Id | Component | Description | failure_mode | Alpha | Component Failure Rate | Failure Mode Rate | End Effect |
|---|---|---|---|---|---|---|---|
| 1.1 | C2 | ¬±10% 50V X7R SMD Multilayer Chip Ceramic Capacitor | Open | 9 | 0.357 | 0.032 | Spurious Protection |
| 1.1 | C2 | ¬±10% 50V X7R SMD Multilayer Chip Ceramic Capacitor | Parameter change | 61 | 0.357 | 0.218 | No effect |
| 1.1 | C2 | ¬±10% 50V X7R SMD Multilayer Chip Ceramic Capacitor | Short | 30 | 0.357 | 0.107 | Blind channel |

# FMECA Process
## Key steps

1. **Using Bill of Materials, do a component-wise Failure Rate Prediction.**
   - Mainly based on 217Plus standard (2015/RIAC, but also available: Telcordia TR/SR, MIL-217, NSWC). Completed by manufacturer and test data.
   - Requires definition of mission profile/environment as well as operating conditions for individual components

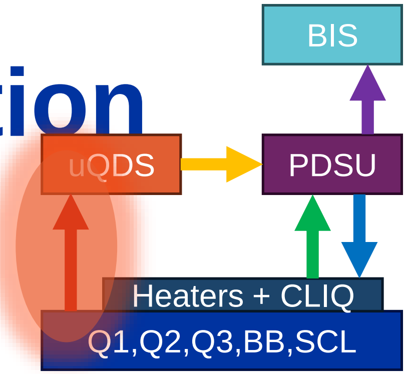
2. **Identification & apportionment of component failure modes**
   - i.e., capacitor -> {open, param. change, short}.
   - Based on handbooks (MIL-HDBK338, FMD2016).

3. **Assigning end-effects to each failure mode of every component of the system.**
   - i.e., Capacitor C1: open -> no effect, short -> false dump, param. change -> blind failure.

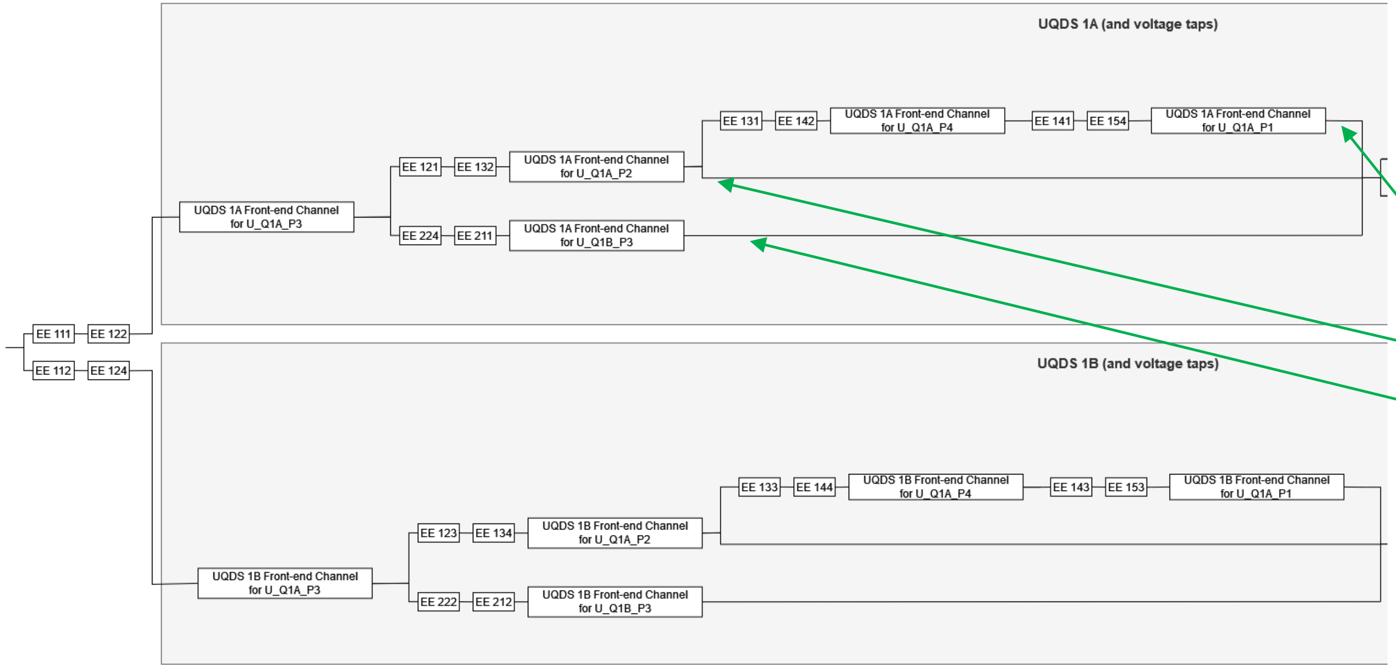


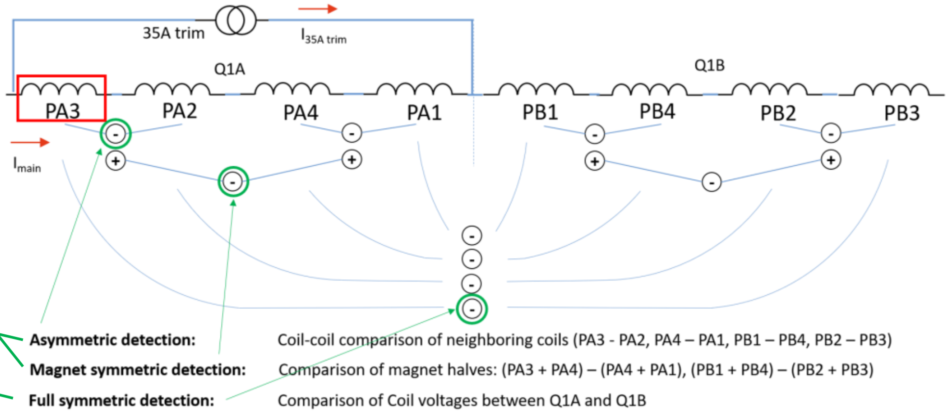

Screenshot of Isograph Reliability Workbench (tool used for FMECA analysis)

# Top-Down Reliability Model – Magnet Protection



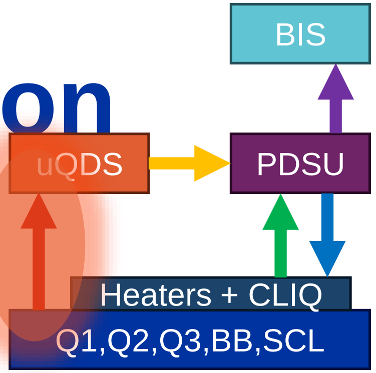

- Quench protection strategy is inherently redundant
- For single coil quench, triple redundant detection method & each of them redundant in hardware



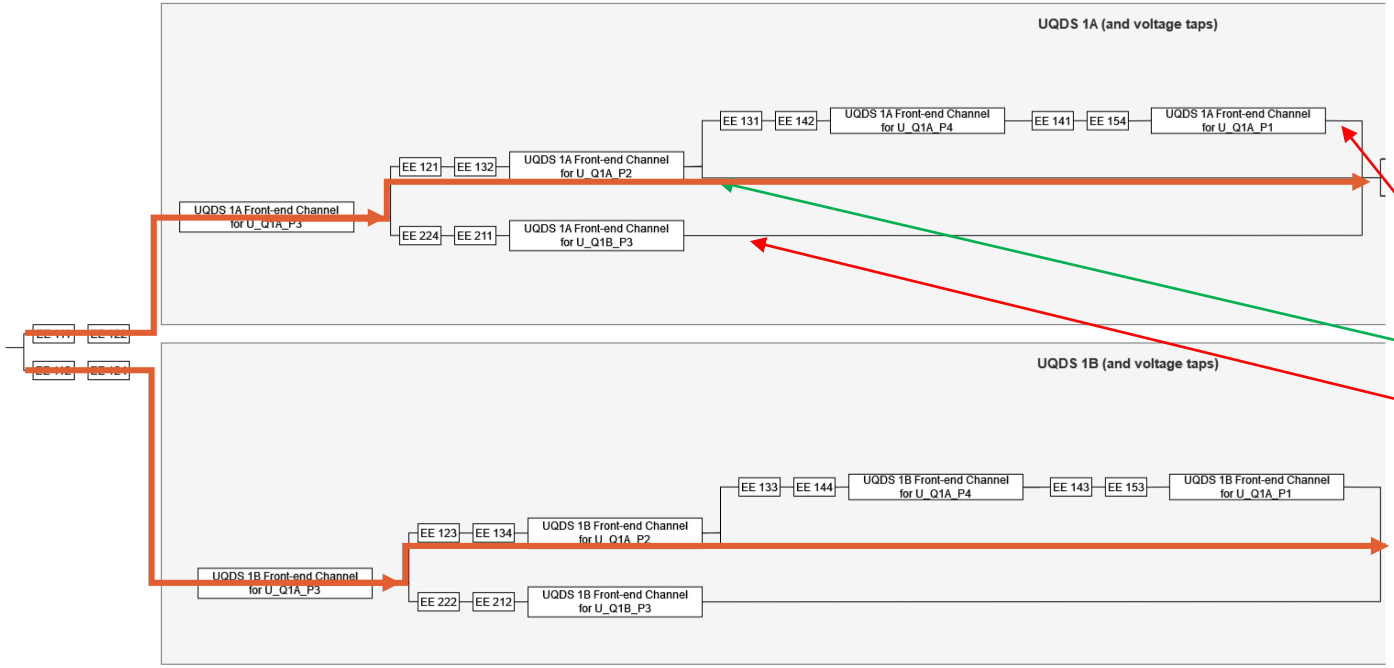



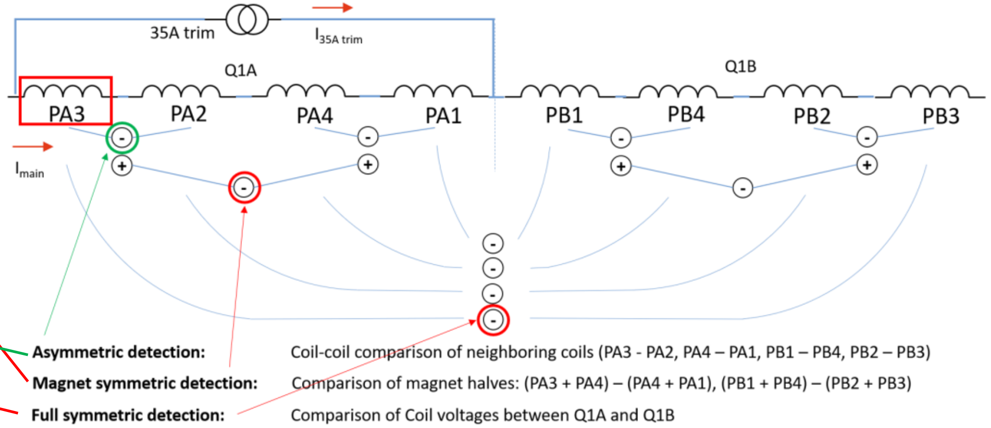

- Reliability model assumes single coil quench

# Top-Down Reliability Model – Magnet Protection




- **Quench protection strategy is inherently redundant**
- **For single coil fault, triple redundant detection method & each of them redundant in hardware**

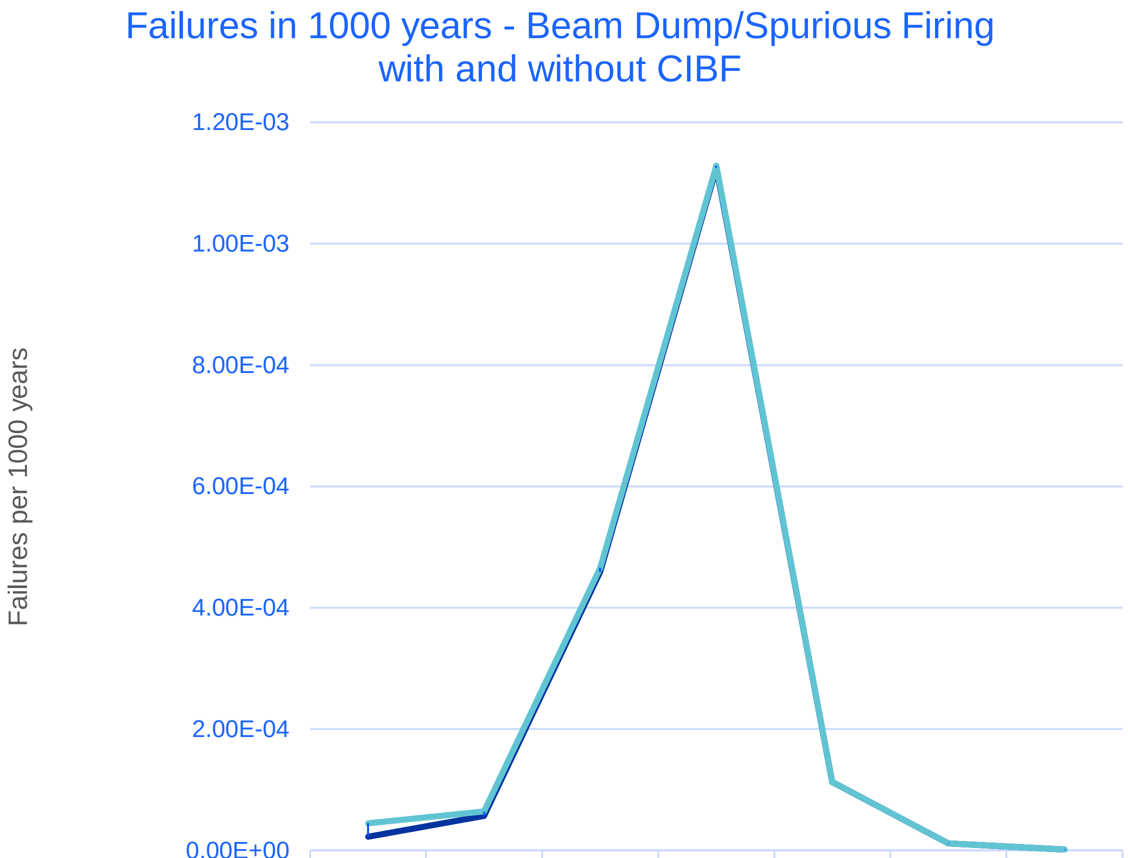



**Pessimistic scenario**

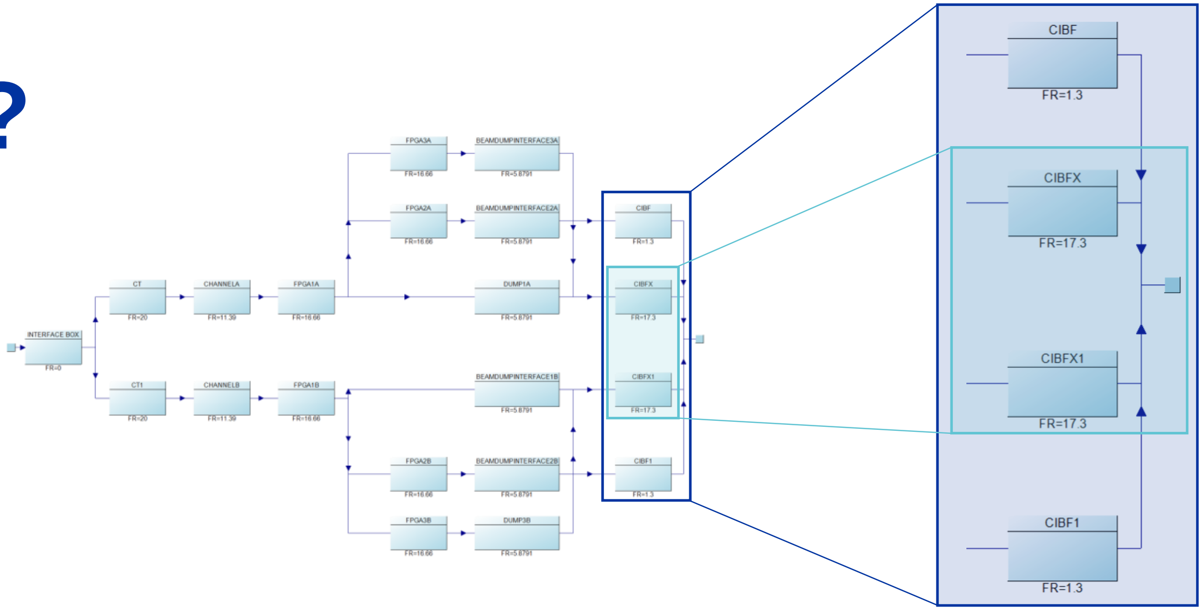
- Reliability model assumes single coil quench
- To reflect that symmetric quenches can occur, which have reduced redundancy, two of three redundant paths are omitted.

# CIBFx+CIBF or only CIBFx?



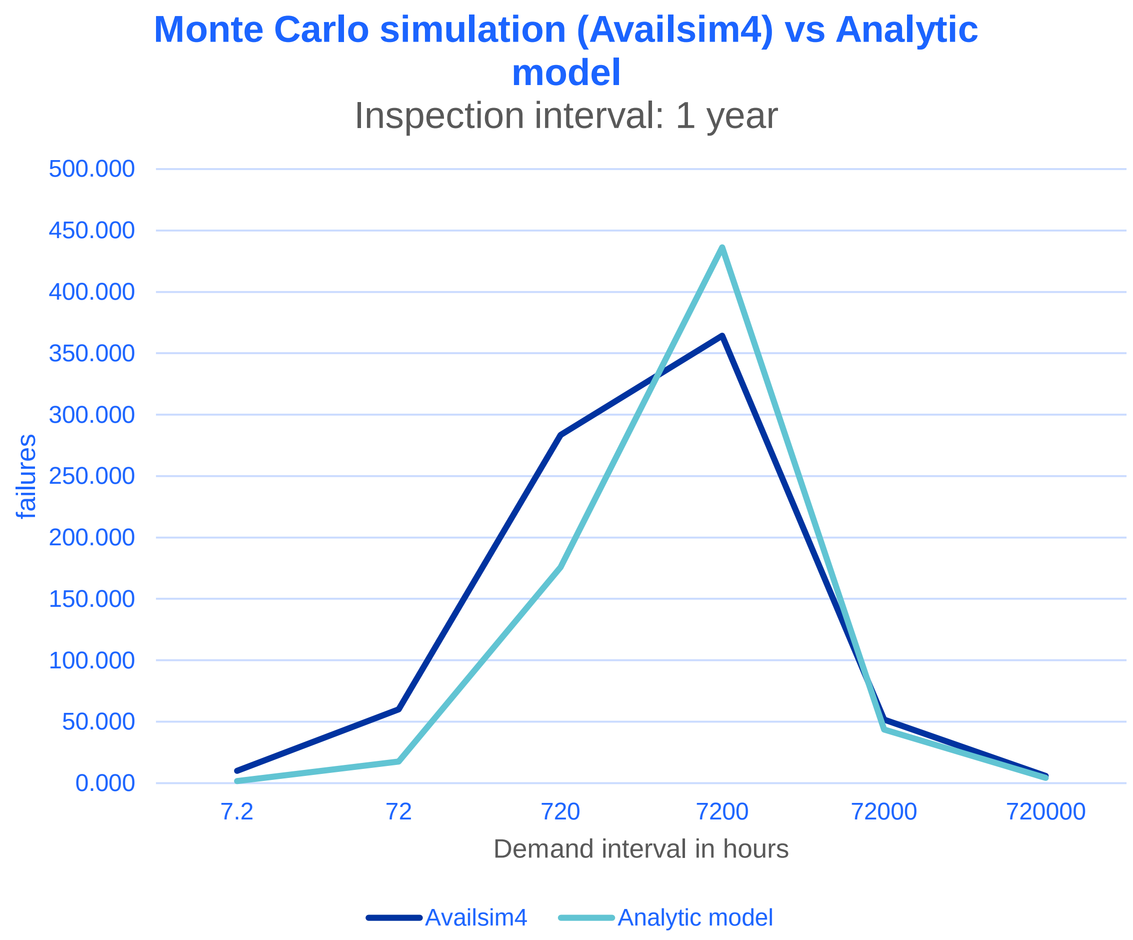

| | 0.001 | 0.01 | 0.1 | 1 | 10 | 100 | 1000 |
|---|---|---|---|---|---|---|---|
| with CIBFx and CIBF | 2.27E-05 | 5.65E-05 | 4.59E-04 | 1.13E-03 | 1.13E-04 | 1.13E-05 | 1.13E-06 |
| only CIBFX | 4.47E-05 | 6.40E-05 | 4.66E-04 | 1.13E-03 | 1.13E-04 | 1.13E-05 | 1.13E-06 |

Demand interval




- Depending on the demand rate, the additional CIBF reduces the number of faults per 1000 years by **0 to 2.20E-05**.
- In the relevant range of 0.0046 spurious firings per year per HDS/CLIQ (1 spurious firing per year), the influence is with a difference of about 3.24E-08 to 3.24E-09 almost negligible.

# Design qualification – Analytic Approach – Magnet Protection




- **An analytical approach was chosen over a simulation approach for time reasons and results are consistent**
- **The minimal cut set method was used to consider various inspection intervals and repair actions**