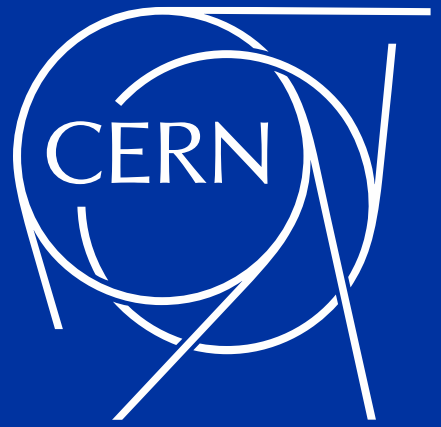


PhD research plan

Reliability assurance for highly-critical complex systems in particle accelerators

David Westermann

04.02.2025

Agenda

1. **Introduction**

2. **Objectives**

    1. Automated Assignment of End-Effects in the Component FMECA
    2. Integrating field & test data for improved reliability predictions
    3. Integrating Software assurance processes

3. **Summary**

1. Introduction

1. Introduction

For safety-critical systems, we ensure at the design stage that the frequency of

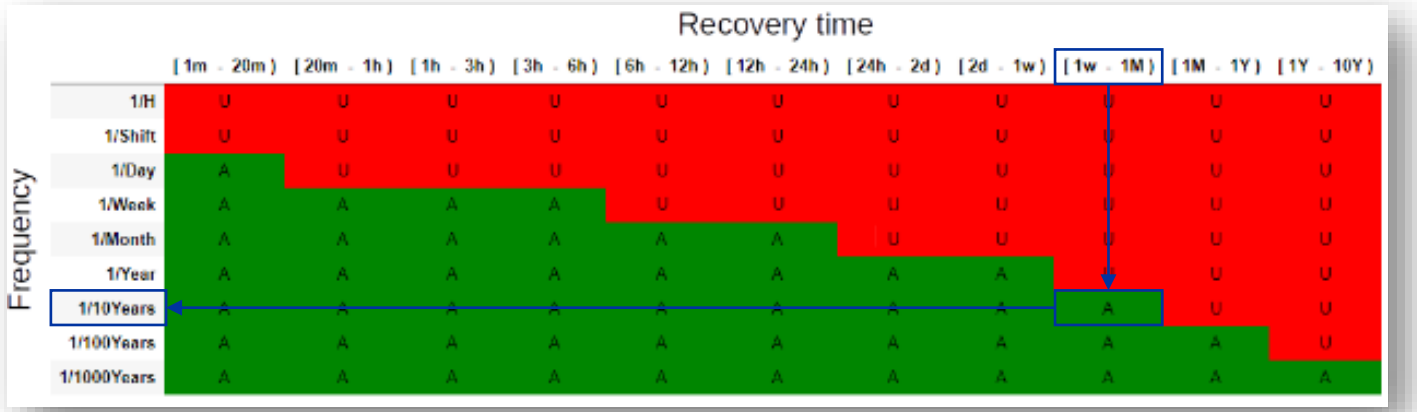
- undetectable failures that could lead to catastrophic damage in a demand situation, and
- failures that affect the availability of the accelerator (e.g. spurious execution of a protection function)

is within an accepted target and make recommendations based on the results.

Top-level FMECA

Identification and quantification of the risk

- Identify functions and corresponding failure modes
- Identify associated risks and hazards and possible end-effects
- Quantify reliability requirements to mitigate risks and hazards



1. Introduction

For safety-critical systems, we ensure at the design stage that the frequency of

- undetectable failures that could lead to catastrophic damage in a demand situation, and
- failures that affect the availability of the accelerator (e.g. spurious execution of a protection function)

is within an accepted target and make recommendations based on the results.

Component FMECA

Analysis of a sub-system

- Determine the failure rate & failure modes for each component
- Assign system level end effects to each component failure mode
- Derive design improvements

AlternatePN	CategoryDescription	Failure Rate	failure_mode	Alpha	FailureModeRate	EndEffect
C1A	Capacitor	0.350	Open	6	0.021	Degraded protection
C1A	Capacitor	0.350	Parameter change	61	0.213	
C1A	Capacitor	0.350	Short	30	0.105	Spurious protection
C1A	Capacitor	0.350	Other	3	0.010	
C1B	Capacitor	0.350	Open	6	0.021	Degraded protection
C1B	Capacitor	0.350	Parameter change	61	0.213	
C1B	Capacitor	0.350	Short	30	0.105	Spurious protection
C1B	Capacitor	0.350	Other	3	0.010	
C3A	Capacitor	0.350	Open	6	0.021	Degraded protection
C3A	Capacitor	0.350	Parameter change	61	0.213	
C3A	Capacitor	0.350	Short	30	0.105	Spurious protection
C3A	Capacitor	0.350	Other	3	0.010	

1. Introduction

For safety-critical systems, we ensure at the design stage that the frequency of

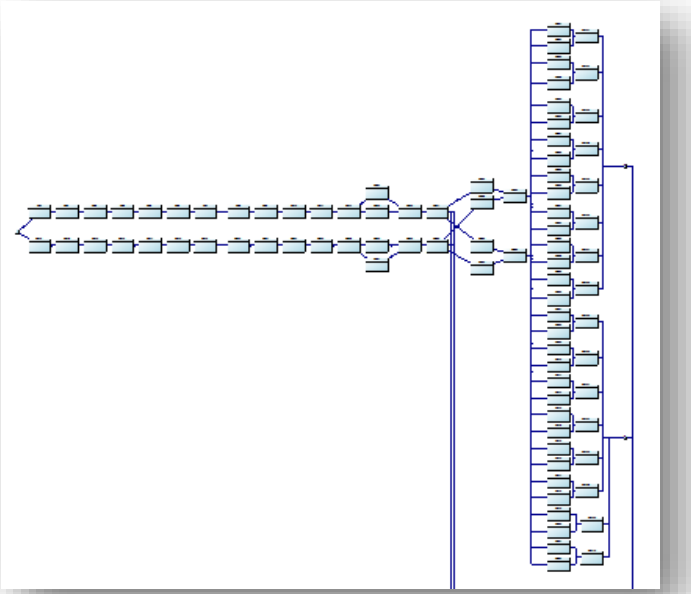
- undetectable failures that could lead to catastrophic damage in a demand situation, and
- failures that affect the availability of the accelerator (e.g. spurious execution of a protection function)

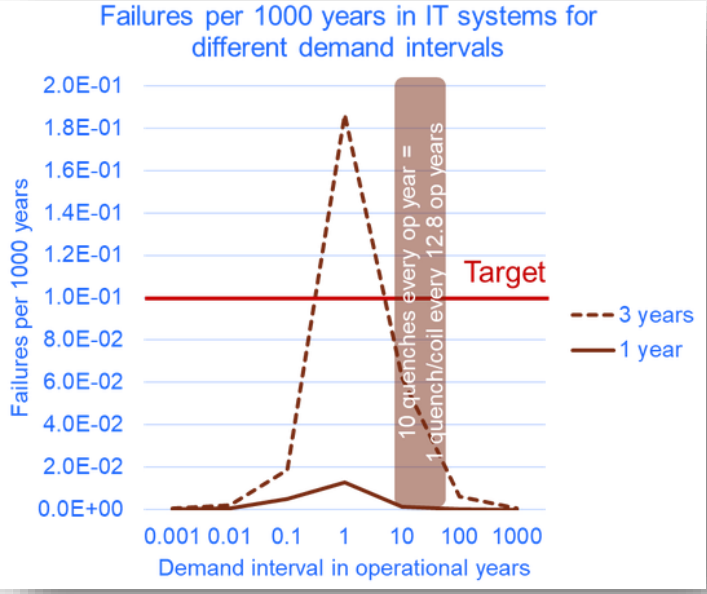
is within an accepted target and make recommendations based on the results.

System-level reliability model

Risk estimation and mitigation

- Build a model that captures the system structure, redundancies, critical/non-critical parts, demand and inspection rates
- Use simulations or analytic models to determine the expected failure frequency
- Give recommendations based on the results





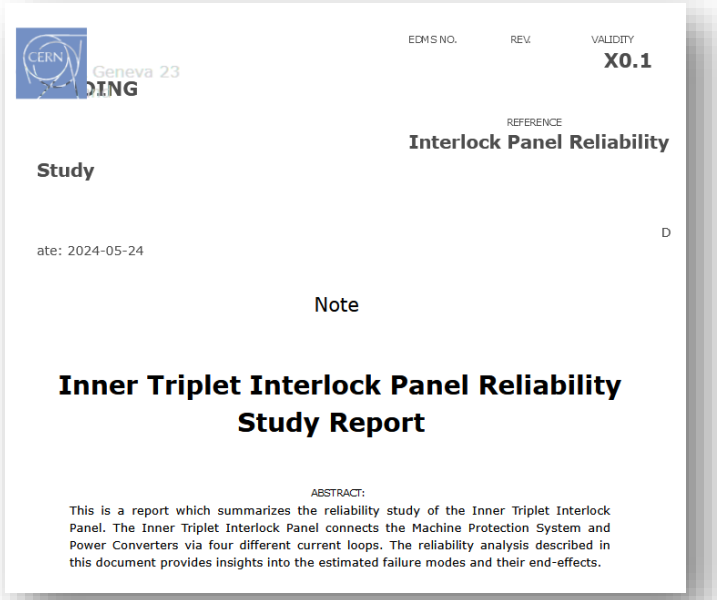
1. Introduction

For safety-critical systems, we ensure at the design stage that the frequency of

- undetectable failures that could lead to catastrophic damage in a demand situation, and
- failures that affect the availability of the accelerator (e.g. spurious execution of a protection function)

is within an accepted target and make recommendations based on the results.

Inner Triplet Interlock Panel



EDMS NO. REV. VALIDITY
X0.1

REFERENCE
Interlock Panel Reliability

Study

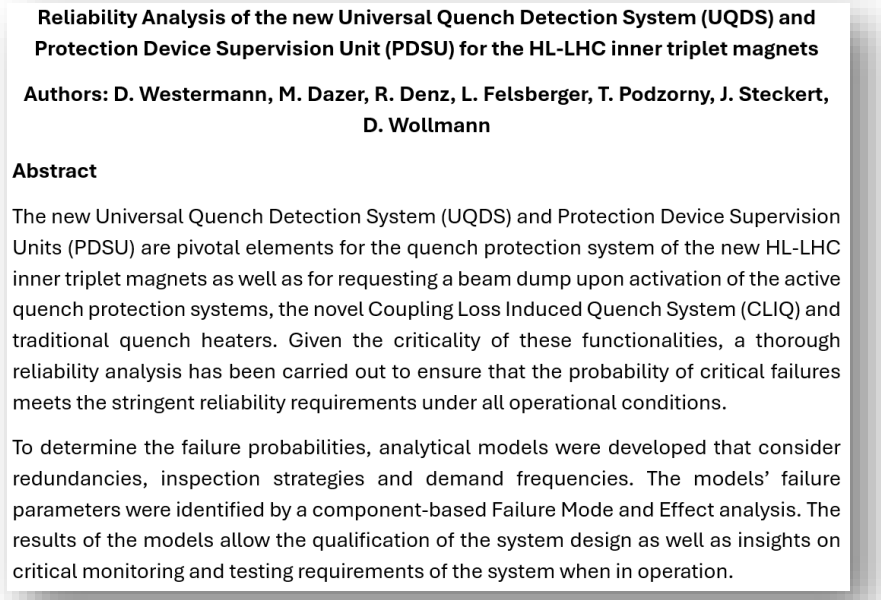
ate: 2024-05-24

Note

Inner Triplet Interlock Panel Reliability Study Report

ABSTRACT:
This is a report which summarizes the reliability study of the Inner Triplet Interlock Panel. The Inner Triplet Interlock Panel connects the Machine Protection System and Power Converters via four different current loops. The reliability analysis described in this document provides insights into the estimated failure modes and their end-effects.

Universal Quench Detection System (UQDS) & Protection Device Supervision Unit (PDSU) (IPAC paper 2025)



Reliability Analysis of the new Universal Quench Detection System (UQDS) and Protection Device Supervision Unit (PDSU) for the HL-LHC inner triplet magnets

Authors: D. Westermann, M. Dazer, R. Denz, L. Felsberger, T. Podzorny, J. Steckert, D. Wollmann

Abstract

The new Universal Quench Detection System (UQDS) and Protection Device Supervision Units (PDSU) are pivotal elements for the quench protection system of the new HL-LHC inner triplet magnets as well as for requesting a beam dump upon activation of the active quench protection systems, the novel Coupling Loss Induced Quench System (CLIQ) and traditional quench heaters. Given the criticality of these functionalities, a thorough reliability analysis has been carried out to ensure that the probability of critical failures meets the stringent reliability requirements under all operational conditions.

To determine the failure probabilities, analytical models were developed that consider redundancies, inspection strategies and demand frequencies. The models' failure parameters were identified by a component-based Failure Mode and Effect analysis. The results of the models allow the qualification of the system design as well as insights on critical monitoring and testing requirements of the system when in operation.

2. Objectives

2. Objectives –
Automated Assignment of End-Effects in the Component FMECA

In our current process, for each failure mode of each component, the system expert determines the end effect at the system level.

AlternatePN	CategoryDescription	Failure Rate	failure_mode	Alpha	FailureModeRate	EndEffect
C1A	Capacitor	0.350	Open	6	0.021	Degraded protection
C1A	Capacitor	0.350	Parameter change	61	0.213	
C1A	Capacitor	0.350	Short	30	0.105	Spurious protection
C1A	Capacitor	0.350	Other	3	0.010	
C1B	Capacitor	0.350	Open	6	0.021	Degraded protection
C1B	Capacitor	0.350	Parameter change	61	0.213	
C1B	Capacitor	0.350	Short	30	0.105	Spurious protection
C1B	Capacitor	0.350	Other	3	0.010	
C3A	Capacitor	0.350	Open	6	0.021	Degraded protection
C3A	Capacitor	0.350	Parameter change	61	0.213	
C3A	Capacitor	0.350	Short	30	0.105	Spurious protection
C3A	Capacitor	0.350	Other	3	0.010	

2. Objectives –
Automated Assignment of End-Effects in the Component FMECA

In our current process, for each failure mode of each component, the system expert determines the end effect at the system level.

Problems

- The expert can make mistakes when assigning the end effects.
- We do only consider single component failures.

2. Objectives –
Automated Assignment of End-Effects in the Component FMECA

In our current process, for each failure mode of each component, the system expert determines the end effect at the system level.

Problems

- The expert can make mistakes when assigning the end effects.
- We do only consider single component failures.

We need to

- Simulate single-component failures as well as multi-component failures and degraded components and determine from the results whether they need to be included in the analysis.

➢ No recommendation yet in the literature about the simulation of multi-component failure scenarios.

Project: Contactor Controls Board

Paper for ICSRS 2025

Topic

Simulation of single and multi-component electronic failure scenarios, including random and degradation failures

Aim

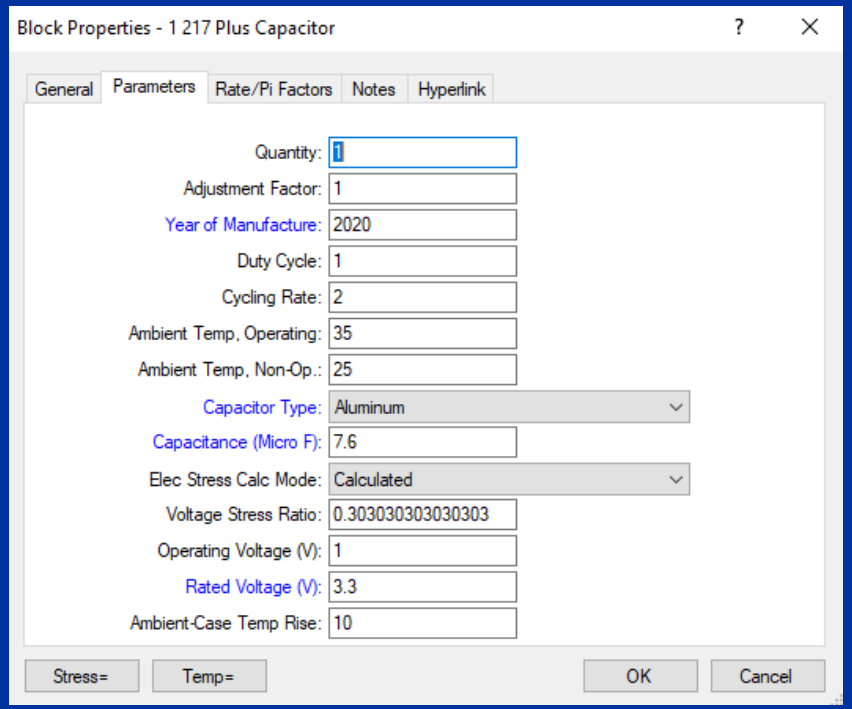
- Review the results of the manual examination
- Determine the failure of not considering multi-component failures in the analysis
- Determine the effect of degradation failures

Needed Results

- **Spice model**
- End effects with corresponding output signals
- Degradation mechanisms
- **Script to simulate failures and degraded components**
- End Effects for different failure scenarios
- Model to calculate the system failure rate for different scenarios
- Recommendations based on the comparison of the results

2. Objectives –
Integrating field & test data for improved reliability predictions

In our current process, failure rates are predicted at the design stage based on standard conditions (e.g. year of manufacture) using the Reliability Prediction Standard 217 Plus.

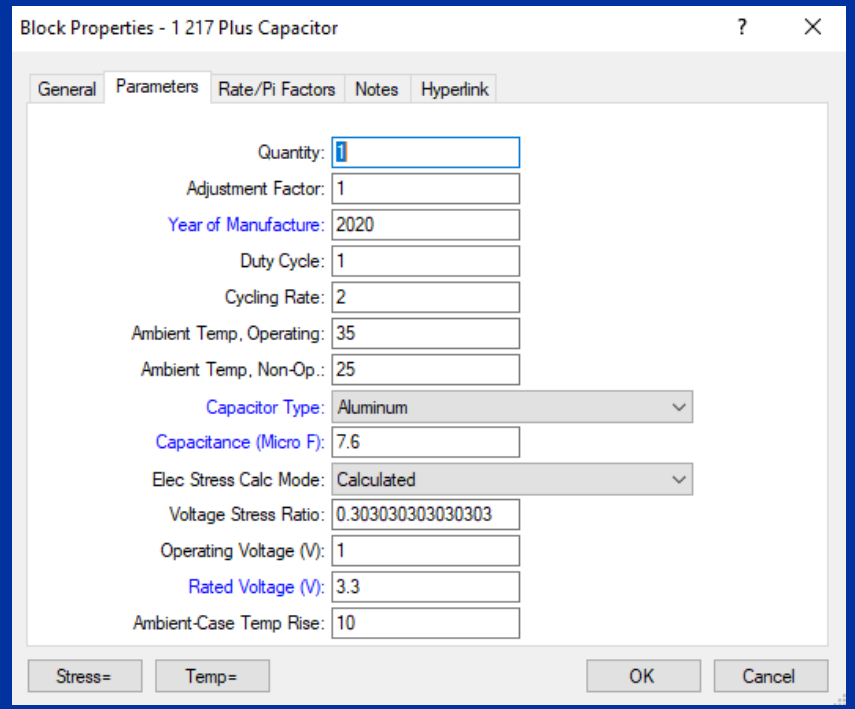


2. Objectives –
Integrating field & test data for improved reliability predictions

In our current process, failure rates are predicted at the design stage based on standard conditions (e.g. year of manufacture) using the Reliability Prediction Standard 217 Plus.

Problems

- The actual operating conditions are only partially taken into account (e.g. duty cycle).
- The use of prediction standards like 217 Plus can lead to predicted values deviating (significantly) from the actual values for various reasons.
- We do not determine the lifetime.
- The actual reliability of the systems is not checked during operation, so the predictions are not validated and updated.



2. Objectives –
Integrating field & test data for improved reliability predictions

We need *to better predict the reliability, by*

- Defining and including mission profiles that reflect the actual operational, environmental and other conditions.

➢ No reference mission profiles established for our application environments.

- Identifying prediction standards and data sources (monitoring data, data from manufacturers etc.) that reflect the failure rate of our components the best.

➢ No benchmarking of prediction standards with actual field data in our operating environments done yet.

Project: BIS - Analysis of failure data		
Machine	CIBM	Date of installation
LHC	34	01/01/2008
LHC INJ	4	01/01/2008
SPS Ring	6	01/01/2006
SPS EXT	10	01/01/2006
SPS INJ	3	01/01/2019
LINAC4	3	01/01/2012
PSB EXT	6	01/01/2012
TOTAL	66	
Total Runtime in h	9558024	
Failure rate in FITs	240.9	

2. Objectives –
Integrating field & test data for improved reliability predictions

We need *to better predict the reliability, by*

- Defining and including mission profiles that reflect the actual operational, environmental and other conditions.
- Identifying prediction standards and data sources (monitoring data, data from manufacturers etc.) that reflect the failure rate of our components the best.

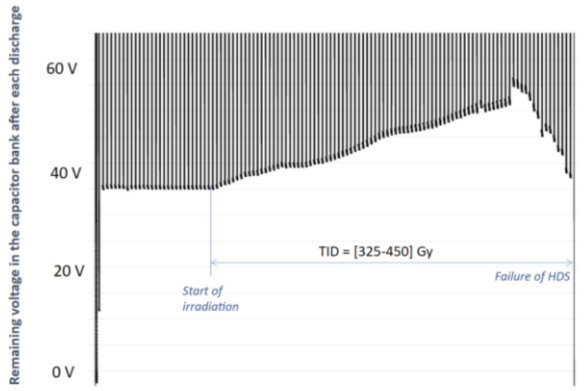
We need to *check and update the reliability prediction during operation,* by

- identifying Key Performance Indicators (KPIs) in the design stage that can be measured and provide information about the reliability/lifetime of the system.
- monitoring and analysing the KPIs and updating the prediction for early end-of-life detection/prediction.

Project: BIS - Analysis of failure data

Machine	CIBM	Date of installation
LHC	34	01/01/2008
LHC INJ	4	01/01/2008
SPS Ring	6	01/01/2006
SPS EXT	10	01/01/2006
SPS INJ	3	01/01/2019
LINAC4	3	01/01/2012
PSB EXT	6	01/01/2012
TOTAL	66	
Runtime in h total	9558024	
Failure rate (FITs)	240.9	

Project: DQHDS - Monitoring of KPIs



Remaining voltage in the cap bank after ~30 min of the discharge

2. Objectives –
Integrating field & test data for improved reliability predictions

We need *to better predict the reliability, by*

- Defining and including mission profiles that reflect the actual operational, environmental and other conditions.
- Identifying prediction standards and data sources (monitoring data, data from manufacturers etc.) that reflect the failure rate of our components the best.

We need to *check and update the reliability prediction during operation,* by

- identifying Key Performance Indicators (KPIs) in the design stage that can be measured and provide information about the reliability/lifetime of the system.
- monitoring and analysing the KPIs and updating the prediction for early end-of-life detection/prediction.

Projects: BIS and DQHDS

Paper for 2026

Topic
Empirical models for predicting the reliability in the design phase und updating the analysis during operation with new data

Aim
- Create mission profiles
- Creation of empirical models that allow the reliability prediction based on mission profiles
- Definition of adequate KPIs and creation of a monitoring framework

Needed Results
- Mission profiles
- Analysis of failure data (from BIS)
- Database with reliability data
- **Empirical models, based on a comparison of the failure data with different prediction standards**
- **Condition based KPIs (e.g. transistor failure in a radiation environment)**
- Monitoring framework

2. Objectives –
Integrating Software assurance processes

In our current process, we do only study hardware failures.

2. Objectives –
Integrating Software assurance processes

In our current process, we do only study hardware failures.

Problems

- Critical functions are increasingly being moved into programmable devices, but we do not consider failures caused by Software.
- We do not yet have a process to fully interface and integrate software aspects.

2. Objectives –
Integrating Software assurance processes

In our current process, we do only study hardware failures.

Problems

- Critical functions are increasingly being moved into programmable devices, but we do not consider failures caused by Software.
- We do not yet have a process to fully interface and integrate software aspects.

We need

- A process to interface and integrate software assurance aspects into a reliability assurance process.
- Focus on PLCs (PIC) and Microelectronics (e.g. UQDS, PDSU etc.).

Project: Software Assurance of the PIC PLC code		
State/ Function	**SW/HW**	**Failure mode**
Fast Power Abort	both	Missed beam dump request upon A & B circuit quench (or discharge request for MB/MQ)
	HW	Blinding of quench loop on 600A circuits with EE

2. Objectives –
Integrating Software assurance processes

In our current process, we do only study hardware failures.

Problems

- Critical functions are increasingly being moved into programmable devices, but we do not consider failures caused by Software.
- We do not yet have a process to fully interface and integrate software aspects.

We need

- A process to interface and integrate software assurance aspects into a reliability assurance process.
- Focus on PLCs (PIC) and Microelectronics (e.g. UQDS, PDSU etc.).

Project: Software Assurance of the PIC PLC code

Paper for 2027

Topic
Interface and integration of software aspects into the reliability assurance process

Aim
- Framework for interfacing and integrating Software aspects into the reliability assurance process
- Guidance in executing formal verification/ reaching a certain SIL level

Needed Results
- Defined Hardware Assurance process
- Analysis of how to interface and integrate software aspects
- **Defined Software Assurance Methods**
- **Formal Verification results of the PIC code**
- Comparison with Standard (which SIL level can be reached)
- Adapted assurance process

3. Summary

3. Summary

Assignment of End Effects in the Component FMECA (Paper ICSRS 2025) → Contactor Controls Board

- Evaluating impact of multi-component failure scenarios and component degradation

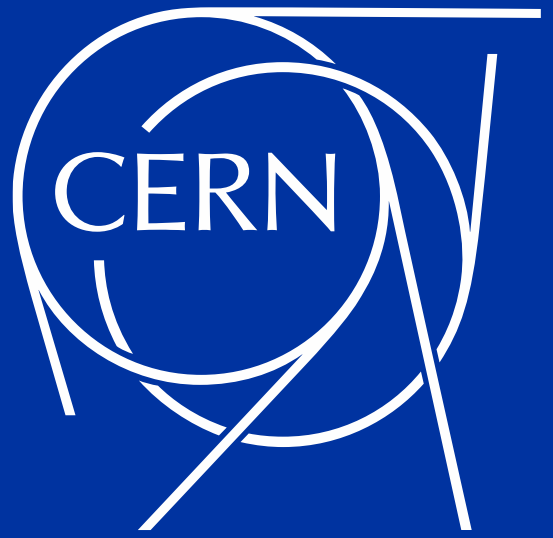
Reliability Prediction (Paper 2026) → BIS and DQHDS

- Improve the prediction of failure rates by using mission profiles and empirical models (BIS)
- Improve end-of-life assessment through defining & monitoring adequate KPIs (DQHDS)

Software Assurance (Paper 2027) → PIC

- Find ways to interface and integrate software aspects into the reliability analysis
- Focus on PLCs (and Microelectronics)

Improve individual steps and extend the reliability assurance process for safety-critical systems to include hardware and software failures.


CERN