Reliability Considerations for the LHC MKB Re-Trigger Upgrade During LS2

ausgeführt am
Atominstitut
der Technischen Universität Wien

TU Wien

unter der Anleitung von
Privatdoz. Dr.techn Michael Benedikt (CERN, TU Wien)
Dr.techn. Wolfgang Bartmann (CERN)
durch
Elisabeth Renner
Matrikelnr.: 01026129

Datum
Unterschrift

22.07.2018
Abstract

An upgrade of the LHC dilution kicker system (MKB) during LS2 foresees the new implementation of an MKB re-trigger mechanism. In case of a pre-firing module, this upgrade enables immediate re-triggering of the remaining MKBs through the currently existing re-trigger line. A decoupling system in the re-trigger line is proposed to inhibit asynchronous extraction kicker triggering in case of such self-triggering MKBs. In this report, different design proposals for this decoupling mechanism are evaluated and reliability assessments for the newly introduced system are conducted.
Contents

1 Introduction 1

2 The LHC Beam Dump System 2
  2.1 System Layout 2
  2.2 Trigger and Re-Trigger System 4

3 Upgrade of the MKB Re-Trigger System, Failure Scenarios and Proposed Solutions 6
  3.1 Identified Fault of the Current System 6
  3.2 Proposed Upgrade in LS2 and Implications for Reliability 8
  3.3 Proposals for the Decoupling Mechanism 8
  3.4 Specifications for Additional Failure Cases Due to the Decoupling System 11

4 Reliability Model and Simulation Strategy 12
  4.1 Simulation Strategy 12
  4.2 General Assumptions 12
  4.3 Mathematical Model 12
  4.4 Identified Component Failure Modes 15
  4.5 Failure Rate Prediction 17
  4.6 Applied Model Parameters and Correction Factors 18

5 Identified Top Level Failure Scenarios 19

6 Results of the Quantitative Fault Tree Analysis 20
  6.1 General Results 20
  6.2 Sensitivity to Parameter Changes 20
  6.3 Comparison to Current System 22

7 Discussion and Comparison of Proposals 24

8 Conclusion and Outlook 26

Bibliography 27
Chapter 1

Introduction

A new failure mode of the dilution kicker system (MKB) was observed during test runs of the LHC Beam Dump System (LBDS) in 2016. A spontaneously self-firing MKB generator could trigger adjacent modules due to parasitic electromagnetic coupling and thus lead to a multi-erratic [1, 2]. Respecting the current system layout, this failure can lead in certain cases to damage of the beam dump (TDE) due to loss of dilution. Immediate measures for mitigation of this coupling have been carried out and a system upgrade to avoid a damaging impact in such a case was proposed.

In this report a first reliability assessment of this proposed system upgrade is conducted in order to evaluate its feasibility. In addition different system implementations are compared, as well as the requirement for component redundancies evaluated.

The LBDS and its trigger and re-trigger mechanisms are outlined in Chp. 2. In Chp. 3 the recently occurring issue of electromagnetic coupling between the MKB generators, its implications and potential solutions are discussed. Chapter 4 focuses on the chosen simulation methodology and Chp. 5 outlines the identified failure modes of the upgraded system. The results are presented in Chp. 6 and discussed in Chp. 7.
Chapter 2

The LHC Beam Dump System

2.1 System Layout

The LHC extraction system comprises two special dipole families, which fulfil the purpose of deflecting the beam from the reference orbit into the dump line: septa and kicker magnets. The 15 extraction kicker magnets (MKD) are fast pulsed dipoles with a rise-time of 2.8 µs. When the beam is to be extracted, the MKDs are triggered during a 3 µs beam free gap in the beam pattern (abort gap), in order to horizontally kick the extracted beam off the reference orbit by 0.275 mrad. This deflection is further increased by the downstream defocusing quadrupole Q4, resulting in a total deflection of 0.33 mrad and hence an offset at the entrance of the extraction septa magnets.

The extraction septa magnets (MSD) are dipoles, with a thin separation (septum blade) between the high field region and the zero field region. The circulating beam passes through the zero field region and is thus shielded from the deflecting impact of the MSD field. However, upon a dump request the MKDs are triggered and the beam is kicked into the high field aperture of the magnet. The MSD then strongly deflects the beam into the 700 m long dumpline, at the end of which the beam dump (TDE) is located. This ~7 m graphite absorber block is designed to absorb the full beam energy.

Dumping the 7 TeV/c beam with a total beam energy of 350 MJ at nominal intensity poses a severe challenge to the absorber material of the TDE. The beam impacts within 89 µs, resulting in a total power of $3.9 \times 10^{12}$ W. This instantaneous high power density exposes the TDE to high mechanical and thermal stresses. It is required to dilute the power density at the beam dump. Besides increasing the beam size, further dilution is obtained by sweeping the beam across the dump and thus transversely separating the impact position of the single bunches.

This sweep pattern is created by the dilution kicker magnets (MKB), 10 fast pulsed magnets which are installed at the beginning of the dump line. Two sets of MKBs - 4 horizontal (MKBH) and 6 vertical (MKBV) - deflect the extracted beam with a sinusoidal, damped field. Due to the $\pi/2$ phase shift between MKBH and MKBV an e-shaped Lissajous-figure is created as dilution pattern.

For every incoming dump request, the so-called Trigger Synchronization Unit (TSU) synchronizes the MKD trigger with the RF system and hence guarantees a clean extraction with
an MKD field rise during the beam free abort gap. A beam abort which is not synchronized to this abort gap is referred to as asynchronous beam dump.

In case of an asynchronous dump, approximately 120 bunches are mis-kicked with a wrong deflection angle and hence swept over the machine aperture between circulating and extracted orbit (Fig. 2.3). Dedicated absorber blocks protect the downstream equipment from damaging impact: The septum protection (TCDS) is a diluter located upstream of the MSD and protects the septum blade. Another diluter, the quadrupole protection (TCDQ), protects the superconducting quadrupole directly downstream of the MSD. Hadronic showers can lead to magnet quenches in case of an asynchronous beam dump.

**Figure 2.1:** Schematic Layout of the LHC Beam Dump System (courtesy of M. Gyr). Red shadow: MSD, blue: MKD, green: MKB.

**Figure 2.2:** Illustration of timing of the abort gap (AG) in case of a nominal (left) and asynchronous dump (right) (courtesy of D. Barna, with modifications).
2.2 Trigger and Re-Trigger System

A nominal beam dump is introduced by a dump request via the Beam Interlock System (BIS), the heart of the LHC interlock systems. During normal operation the beam permit signal, which is called safe beam flag, is constantly transmitted via two redundant optical loops (BIS loops) in clockwise and in counter clockwise direction. Numerous systems along the collider function as input for the BIS. In case of any non-nominal parameter, such as increased losses in one of the Beam Loss Monitors (BLM), the signal in the BIS loop is interrupted. This interruption of the BIS signal can be interpreted as loss of the beam permit, propagates via the BIS to the LBDS and is there detected by the Trigger Synchronization Unit (TSU) as a dump request. As mentioned before, the TSU synchronises this dump request with the abort gap and creates a synchronised MKD and MKB trigger. This trigger signal is propagated through the Trigger Fan Out (TFO) to the MKB and MKD generators, which are then simultaneously fired.

In case of a pre-firing MKD module, machine damage due to the mis-kicked beam needs to be avoided. Thus, the remaining MKDs and MKBs are re-triggered to extract the beam as fast as possible, resulting in an asynchronous beam dump. To enable such a re-trigger mechanism, all generators are inductively coupled to the Re-Trigger Line (RTL). Any current through the magnet induces a corresponding voltage pulse in the RTL, which is subsequently inductively picked up by the Re-Trigger Receivers (RTR) of the other generators.

However, in contrast to erratic MKDs, an erroneous MKB field due to e.g. a self trigger does not immediately impact the beam. Thus, asynchronously re-triggering the MKDs in case of an erratic MKB is to be avoided. The MKB generators only receive the re-trigger pulse from the RTL and do not inject energy into the RTL in case of an erratic MKB. Instead the decaying capacitor voltage in the MKB generator is detected by the Beam Energy Tracking System (BETS), which is the constant surveillance of the agreement between the loaded ca-
Figure 2.4: Schematic layout of the trigger and re-trigger system of the LBDS.

Figure 2.5: Illustration of the redundancy of the LBDS system exemplified by the nominal trigger path (BIS to MKD generator). This figure is simplified and not exhaustive. Additional safety links, such as the direct link from the BIS to the RTL, are not included.

Capacitor voltage and the beam energy. A non-nominal generator voltage is then an indicator to interrupt the BIS loop and request a synchronous dump via BIS and the LBDS trigger system.

The strict safety requirements on the BIS and LBDS have a major impact on the system design. A safe beam dump has to be always guaranteed and the probabilities of failure cases leading to severe machine damage need to be minimized (failures beyond design). An inherent redundancy dominates the system design in order to meet these safety requirements. Figure 2.5 illustrates the redundant trigger paths A and B. For simplification, in Fig. 2.4 as well as in all schematics below, only one path is illustrated. However, unless stated explicitly otherwise, all systems are redundant.

Apart from the nominal trigger path as explained above (TSU to TFO to generators), two additional paths are indicated in Fig. 2.4. Firstly, a direct connection from the BIS to the RTL creates an asynchronous trigger in case of a silent failure of both TSU modules. This signal is injected into the RTL with a delay of 320 µs, in order not to interfere with the nominal synchronous signal. Furthermore, a direct link between the TSU output and the RTL exists, which creates a re-trigger pulse with a delay of 270 µs. The re-trigger delay (RTD) is created by the so-called Trigger Delay Units (TDU).
Chapter 3

Upgrade of the MKB Re-Trigger System, Failure Scenarios and Proposed Solutions

3.1 Identified Fault of the Current System

During a test run in 2016, parasitic electromagnetic coupling between MKB generators was observed. Despite immediately applied mitigation at hardware level, there is a not quantifiable risk of triggering adjacent MKB generators in case of a pre-firing module.

In case of a phase shift of $\pi/2$ between the spontaneously firing generators and the remaining ones, this can result in a reduced dilution in one plane. The resulting loss of dilution is quantified to be up to 90 % (40 %) for 3 (2) pre-firing modules [1].

The time delay between the pre-firing MKB and the subsequent trigger of the remaining MKBs depends on the BETS delay and the synchronisation to the abort gap. Figure 3.1 illustrates the reduced horizontal deflection in case of 1-4 pre-firing MKB as a function of the BETS delay.

It is currently not possible to quantify the probability or exclude this failure case. Different strategies can be pursued as potential long term solutions, which can be summarized by the three cases listed below. It is not possible to fulfil all three conditions that are illustrated in Fig. 3.2 simultaneously. Hence, the different scenarios for the implementations of a re-trigger system in case of an erratic MKB are:

1. **Risk of MKBs in anti-phase (current system, no MKB re-triggering):** Triggering of the remaining MKBs in phase with the MKD generators. Hence, the sweep path (which depends on the timing between MKD and MKB trigger) is not changed and there is no risk for additional asynchronous dumps. The remaining MKBs might be triggered in anti-phase.

2. **Risk of additional asynchronous dumps:** Instantaneous re-triggering of all MKDs and MKBs (nominal sweep path), resulting in an asynchronous dump.

3. **Risk of changed sweep path:** Immediate re-triggering of the MKBs with the pre-firing module and subsequent synchronous triggering of the MKDs with the abort gap. The sweep path changes due to the not nominal delay between MKB and MKD triggering ([2]).
Chapter 3 Upgrade of the MKB Re-Trigger System, Failure Scenarios and Proposed Solutions

Figure 3.1: Reduced deflection by the MKB system in case of multiple pre-firing MKBs and subsequent trigger of the remaining MKBs with a phase shift depending on the BETS delay (courtesy of C. Wiesner).

Figure 3.2: Schematic illustration of different strategies related to MKD and MKB re-triggering (courtesy of C. Wiesner, [2]).
As a result of multiple studies it was decided to proceed with the third option ([1, 2]). The required upgrade should enable an MKB re-triggering with a subsequent synchronous triggering of the MKDs.

### 3.2 Proposed Upgrade in LS2 and Implications for Reliability

The RTRs which connect the MKB generators to the RTL will be exchanged with Re-Trigger Boxes (RTB) similar to the ones of the MKD generators. A decoupling mechanism in the RTL is required to avoid an asynchronous dump in case of an erratic MKB, which is indicated by the red diode symbol in Fig. 3.3 and referred to as *Decoupling Box* (DB). A voltage pulse originating at the MKB side of the DB should not re-trigger an asynchronous beam dump but be picked up by a RTR, propagated to the TSU and trigger a synchronous dump. The key points are summarized again below.

In case of an MKB erratic the upgraded system is supposed to

- re-trigger the remaining MKBs via the RTL so that all MKBs oscillate in phase,
- avoid asynchronous triggering of the MKDs and
- provide a link from the RTL to the TSU to enable a fast synchronous beam abort. The MKDs should be triggered within at most ~120 µs, to guarantee an acceptable alteration of the sweep path.

At the same time, in case of an erratic MKD

- re-triggering the remaining MKDs and MKBs through the RTL needs to be guaranteed.

### 3.3 Proposals for the Decoupling Mechanism

Within the process of this reliability study various system layouts have been proposed, analysed and discussed. In this report only some of the main different options are outlined and
compared. For more details on different design variations it is referred to [2–4]

Option 1: Single Diode Box (DB) per RTL (Fig. 3.4): The option with the fewest system interventions consists of one DB at each RTL. In case of an erratic MKB a RTR picks up the signal from the RTL and propagates it to the TSU. An additional TDU at the MKB side of the DB is required for surveillance of the correct system status. After every dump this signal is injected with a certain delay into the RTL to verify the status of the DB. The timing of this pulse has to be chosen in such a way that it can be uniquely identified by the Internal Post Operational Check Software (IPOC). The status of the DB is registered as ‘OK’ if the pulse is measured on the MKB side but not on the MKD side of the RTL. This is crucial for the assumption, that after every dump (and hence IPOC check) the system can be seen as ‘as good as new’. These checks enable the use of reliability models, that are based on periodic inspection and significantly increase the predicted reliability.

Option 2: Two DBs per RTL (Fig. 3.5): To avoid asynchronous dumps in case of simultaneous short failure of a DB with an erratic MKB a second DB is to be installed in series at the RTL. In this case two additional TDUs are required to observe the system status after every dump. Furthermore, a bypass of the DBs, as described for Option 3, is implemented.

Option 3: Single Diode Box (DB) per RTL with additional bypass of the DB (Fig. 3.6): A single DB is installed in the RTL. An erratic MKD and a simultaneous malfunction of the link from the RTL to the triggering of the MKD generators would result in a delayed beam abort, triggered by e.g. the BETS. However, as mentioned before, this delayed trigger would result in insufficient dilution. To avoid this case a bypass of the DB is proposed: The erratic MKB signal is picked up from the RTL with a RTR and injected at the MKD side of the RTL with a delay of \( \sim 110 \, \mu s \), resulting in an asynchronous beam dump. This delay guarantees, that the asynchronous signal arrives after the synchronous dump and only triggers the MKD in case of the missing synchronous dump.

It has to be noted, that the link from the RTL to the MKD generators in all layouts depends on a correctly working trigger path from TSU to MKD. The additional direct safety link from the BIS to the TDU creates an asynchronous trigger after 320 \( \mu s \), which is too late for an MKD re-triggering in case of an erratic MKB. This is indicated in Fig. 3.4, Fig. 3.5 and Fig. 3.6. by the cross through paths.
3.3 Proposals for the Decoupling Mechanism

**Figure 3.4:** Implementation of the decoupling mechanism: Proposal 1.

**Figure 3.5:** Implementation of the decoupling mechanism: Proposal 2.

**Figure 3.6:** Implementation of the decoupling mechanism: Proposal 3.
3.4 Specifications for Additional Failure Cases Due to the Decoupling System

The main aim of the analysis is to check the feasibility of the upgrade, estimate the necessity of redundancies, compare different implementations and compare the resulting reliability numbers to the current system. No specific hardware design has existed at the time of this analysis. It is not the scope of this study to conduct a detailed reliability assessment of a fully designed system at component level. Such an analysis is recommended once the system upgrade has been planned in detail.

Hence, this study focused on

1. identifying and simplifying system blocks,
2. identifying failure modes and assigning failure rates,
3. quantifying failure rates using a quantitative Fault Tree Analysis (FTA).

Before conducting this study required reliability specifications have been identified [5]. The additional failure rates due to the upgraded system should not exceed:

- 1 additional synchronous dump per year and beam
- 1 additional asynchronous dump per year and beam
- 1 case of missing dilution in 10^5 years (> SIL 4), which is therefore a failure beyond design.

Regarding the Unavailability of the LHC (missing beam permit) due to the upgraded system no specifications have been made. The results will still be presented in Chp. 6.

---

1 SIL: Safety Integrity Level, a standard to assess the safety of a system. SIL4 corresponds to failure probabilities of $< 10^9/h$ or $< 10^9/yr$. However, the methodology of SIL standards is currently assessed as not optimized for particle accelerators and it is recommended to state the required Mean Time To Failure (MTTF) or failure rates instead. [6]
Chapter 4

Reliability Model and Simulation Strategy

4.1 Simulation Strategy

Top level failure scenarios are identified based on component failure modes, as described in Chp. 5. Failure rates of the resulting top level failure scenarios are subsequently computed using the mathematical approach described in Sec. 4.3. Based on the created model, a sensitivity analysis is conducted to estimate the impact of parameter variations.

In general conservative assumptions are used throughout the analysis, as the aim is to assess the feasibility of the system and not exactly predict its Unavailability.

4.2 General Assumptions

- Constant component failure rates are assumed for the quantitative assessment of the failure scenarios.
- The IPOC check after every dump verifies the system status, which can therefore considered to be ‘as good as new’ at the beginning of every new mission (Sec. 4.3.1).
- No common cause failures are considered in this analysis.
- It is further assumed, that failure of one component does not influence the failure rate of other components.

For improved flexibility of the model, the reliability estimates of the failure scenarios are numerically computed using a developed Python [7] script, based on the mathematical model described below. The results are validated using the Fault Tree Module of the reliability workbench Isograph [8].

4.3 Mathematical Model

The assumption of the constant component failure rate implicates an exponential decreasing survival rate with time. The model is briefly outlined below, for further information it is referenced to a variety of textbooks on reliability engineering (e.g. [9]).
Chapter 4 Reliability Model and Simulation Strategy

\( \lambda = \text{const.} \) \hspace{1cm} (4.1)

The failure density \( f(t) \), the survival probability or reliability \( R(t) \) and failure probability \( F(t) \) are therefore given by the following expressions:

\[
f(t) = \lambda \cdot e^{-\lambda t} \hspace{1cm} (4.2)
\]

\[
R(t) = \int_t^\infty f(t) dt = e^{-\lambda t} \hspace{1cm} (4.3)
\]

\[
F(t) = \int_0^t f(t) dt = 1 - e^{-\lambda t} \hspace{1cm} (4.4)
\]

\[
\lambda(t) = \frac{f(t)}{R(t)} = \frac{dF(t)/dt}{R(t)} \hspace{1cm} (4.5)
\]

For two components in series (parallel failure structure; system fails if one of the components fails), the failure modes are connected via a logical OR structure (\( \lor \)). The system reliability can be written as

\[
R(t) = R_1(t) \cdot R_2(t) = (1 - F_1(t)) \cdot (1 - F_2(t)) = e^{-\lambda_{tot} t} \hspace{1cm} (4.6)
\]

In this case the system failure rate can be obtained by adding the component failure rates. As the component failure rates are constant with respect to time, the system failure rate is constant as well.

\[
\lambda_{tot} = \lambda_1 + \lambda_2 = \text{const.} \hspace{1cm} (4.7)
\]

For two components in parallel (serial failure structure; system fails if both components fail), the failure modes are connected via a logical AND structure (\( \land \)). In this case the failure probability can be written as

\[
F(t) = F_1(t) \cdot F_2(t) = (1 - R_1(t)) \cdot (1 - R_2(t)) \hspace{1cm} (4.8)
\]

Thus, for a series failure structure the system failure rate cannot be obtained by the sum of the component failure rates, but must be computed using Eq. (4.5) which introduces a time dependence.

The Mean Time To Failure \( MTTF \) is generally evaluated by
4.3 Mathematical Model

\[ MTTF = \langle t \rangle = \int_0^\infty t \cdot f(t) dt = \int_0^\infty R(t) dt \quad (4.9) \]

For constant failure rates (no parallel failure structure, i.e. \( \lambda = \Sigma \lambda_i \)) it simplifies to

\[ MTTF = \frac{1}{\lambda} \quad (4.10) \]

### 4.3.1 Model with Periodic Inspection

As the system state is checked after every dump, a model with periodic inspection can be applied. For every run, the system is seen ‘as good as new’. This is represented in the model as followed (mission time \( \tau \) and number of missions \( M \)):

\[ R(t + M \cdot \tau) = 1 - R(t) \cdot R(\tau)^M \quad (4.11) \]

\[ MTTF = \langle t \rangle = \frac{\int_0^\tau R(t) dt}{1 - R(\tau)} \quad (4.12) \]

The occurring number of faults in \( M \) missions is distributed binomially.

\[ p(n \text{ faults}) = \binom{M}{n} p^n (1 - p)^{M-n} \quad (4.13) \]

The expected number of faults and the standard deviation can thus be written as

\[ \langle p \rangle = p \cdot M \quad (4.14) \]

\[ \langle \sigma \rangle = \sqrt{M(1 - p)p} \quad (4.15) \]

### 4.3.2 Beta-Factor Model for Common Cause Failures:

Quantifying the risk of ‘No Dilution’ in the existing (not upgraded) system requires to introduce common cause failures in the failure model.

For a common cause failure, the failure rate can be split into an independent \( \lambda_I \) and a dependant part \( \lambda_{CC} \). The ratio is expressed by the factor \( \beta \):

\[ \lambda = \lambda_I + \lambda_{CC} = (1 - \beta) \cdot \lambda + \beta \cdot \lambda \quad (4.16) \]
4.4 Identified Component Failure Modes

The system is broken down into blocks of subsystems, to which failure modes and rates are assigned:

4.4.1 Newly Implemented Components:

Diode Box (DB): The simplest proposal for the DB consists of two diodes, which block the corresponding pulse of the differential signal (Fig. 4.1). The diodes can either fail in open or short mode. The following simplifications are assumed for the resulting failure mode of the entire DB:

- \( DB_{\text{open}} \): DB fails open if at least one diode fails open
- \( DB_{\text{short}} \): DB fails short if at least one diode fails short.

These conservative assumptions are overlapping but acceptable for this assessment of feasibility. Simulations based on a specific diode model must be conducted to refine the response of the DB to a single open or short failing diode.

Trigger Delay Unit (TDU): Depending on the chosen layout, one to three additional TDUs need to be installed for redundant paths and IPOC checks. The failure modes of these additional TDUs are adopted from [10], a study on the currently installed TDUs.

- \( TDU_{\text{asynch}} \): A spurious, asynchronous signal is created by the TDU.
- \( TDU_{\text{synch}} \): A synchronous beam dump is requested by the TDU due to an internal warning.\(^2\)
- \( TDU_{\text{unav}} \): The IPOC check detects a non-nominal value of the hardware surveillance of the TDU and inhibits the beam permit for the subsequent injection, which impacts availability.\(^3\)

Path from RTL to synchronous trigger of MKD: The detailed layout design for this link is still pending. The currently foreseen design, of a direct link from the RTL to the TSU

\(^2\) Merging of synchronous TDU and connector failure modes from [10]

\(^3\) Merging of failure modes ‘Unavailable TDU’ and ‘TDU warning’ from [10]
4.4 Identified Component Failure Modes

however only requires passive electronics, resulting in low expected failure rates. General expected failure modes are assigned to this link and failure rates are assigned as design specifications. In case of a link from the RTL to the BIS instead of the TSU, a Pulse Detection Module (PED) with active electronics is required. The reliability of such a PED would need to be studied in detail.

For the link from the RTL to the TSU we distinguish between

- \(\text{LINK}_1\text{open}\): No transmission of the signal from the RTL to the TSU
- \(\text{LINK}_1\text{spurious}\): A spurious signal is transmitted to the RTL, requesting a synchronous dump.

As of the missing system design IPOC warnings due to parameter changes of this link and a resulting contribution to downtime are not included in this study.

For the trigger path from the TSU to the MKD generators, only the open failure mode is considered, as no new components are installed introducing new failure modes.

- \(\text{LINK}_2\text{open}\): No transmission of the signal from the RTL to the TSU

4.4.2 Inputs from Existing System:

The following failure modes of the existing system need to be considered, as they function as input for assessing the correct operation of the system upgrade:

- \(\text{MKD}_{\text{async}}\) (Fig. 4.3): An asynchronous signal on the RTL, which originates at the MKD side of the DB. The main cause for the failure mode is a self-trigger of one of the MKD generators. However, this number also includes e.g. a spurious trigger from TFO outputs and spurious triggers of one of the currently existing TDUs.

- \(\text{MKB}_{\text{async}}\) (Fig. 4.2): An asynchronous signal on the RTL, which originates at the MKB side of the DB. The main cause for the failure mode is a self-trigger of one of the MKB generators. However, this number also includes e.g. a spurious trigger from TFO outputs.
4.5 Failure Rate Prediction

Most subsystems of the proposed re-trigger and decoupling systems are already under operation in a similar context and dedicated reliability studies exist. Hence, failure rates and failure modes of these subsystems are taken from results of those studies [10–13].

Parts, which require a failure rate prediction at component level are evaluated with the prediction module of the commercially available software package Isograph [8]. The prediction is based on the MIL-HDBK-217F standard, which is outdated and predicts higher failure rates than modern standards. However, this report is based on previously conducted studies, which use the MIL-HDBK-217F standard. To guarantee uniformity regarding the contributions of subsystems to the investigated failure scenarios the MIL-HDBK-217F is used for failure rate prediction in this study as well.

A pessimistic approach is used for the failure rate prediction. For example, a total failure rate (for open, short and parameter change failure modes) of 20 FIT is applied to describe the diode failure rate, even though a realistic prediction considering the installation environment and electrical load would result in a prediction of 2 FIT. Furthermore, eventual contributions of the predicted failure rate to a parameter change of the component, as foreseen in the MIL-HDBK-217F standard, are assigned to both (short and open) failure modes. This conservative approach results in an increased total failure rate.
4.6 Applied Model Parameters and Correction Factors

The failure metrics are computed for 400 missions per year, each with a runtime of 20 hours. The system upgrade is to be compared to the currently existing system regarding the occurrence of insufficient dilution. A first approach based on the Beta-Factor model is applied to quantify the probability of a multi-erratic of the current system. A multi-erratic is defined as two or more MKBs, which fire within a time-interval of 200 µs, either due to coupling ($\beta \neq 0$) or due to two independently firing MKBs ($\beta = 0$). The resulting probability is then corrected by the following factors:

- 0.2: Only 20% of the random BETS and synchronization delay times result in an anti-phase oscillation of the remaining MKBs.
- 0.33: The critical dilution loss occurs, if out of the remaining 9 generators one of the remaining 3 MKBH is triggered simultaneously with the pre-firing MKBH.

It has to be noted, that a damaging impact of insufficient dilution is only expected for runs at top energy and nominal intensity. A correction factor might be applied to all results to include different operational conditions. However, based on the conservative approach of this study, this correction factor has not been applied to the results.

---

**Table 4.1**: Summary of Applied Failure Rates. FIT: Failure in Time = 1 failure / $10^9$ hours.

<table>
<thead>
<tr>
<th>System</th>
<th>Failure Mode</th>
<th>Failure Rate</th>
<th>Reference</th>
</tr>
</thead>
<tbody>
<tr>
<td>Existing</td>
<td>$MKD_{asynch}$</td>
<td>2 yr-1 ($2.5 \cdot 10^5$ FIT)</td>
<td>operation [14]</td>
</tr>
<tr>
<td>Existing</td>
<td>$MKB_{asynch}$</td>
<td>4 yr-1 ($5 \cdot 10^5$ FIT)</td>
<td>operation [14]</td>
</tr>
<tr>
<td>Diode (in DB)</td>
<td>open</td>
<td>10 FIT</td>
<td>prediction, MIL-HDBK-217F</td>
</tr>
<tr>
<td>Diode (in DB)</td>
<td>short</td>
<td>13 FIT</td>
<td>prediction, MIL-HDBK-217F</td>
</tr>
<tr>
<td>TDU</td>
<td>$TDU_{asynch}$</td>
<td>60 FIT</td>
<td>[10–13]</td>
</tr>
<tr>
<td>TDU</td>
<td>$TDU_{synch}$</td>
<td>180 FIT</td>
<td>[10]</td>
</tr>
<tr>
<td>TDU</td>
<td>$TDU_{unav}$</td>
<td>230 FIT</td>
<td>[10]</td>
</tr>
<tr>
<td>TFO</td>
<td>$TFU_{spur.}$</td>
<td>250 FIT</td>
<td>[12, 13]</td>
</tr>
<tr>
<td>Link: RTL to TSU</td>
<td>missing</td>
<td>10 FIT</td>
<td>specified</td>
</tr>
<tr>
<td>Link: TSU to MKD</td>
<td>missing</td>
<td>10 FIT</td>
<td>based on [11–13]</td>
</tr>
<tr>
<td>Link: RTL to TSU</td>
<td>spurious</td>
<td>200 FIT</td>
<td>estimated, based on [10]</td>
</tr>
</tbody>
</table>

The sensitivity to varying failure rates has been assessed and examples are presented in Sec. 6.2.
Chapter 5

Identified Top Level Failure Scenarios

A bottom-up approach is used to identify the component/subsystem failure modes and relate them as causes to higher level failure modes. Failure rates of the resulting top level failure scenarios are subsequently computed using the mathematical approach described in Sec. 4.3. The identified top level failure scenarios are categorized as follows:

• **(A) No or insufficient dilution:** Any combinations of failure modes, leading to an insufficient dilution. The two contributing paths are:
  
  – Open RTLs in case of an asynchronous MKD trigger.
  
  – Delayed MKD trigger in case of an asynchronous MKB trigger and re-trigger, resulting in a changed sweep path. The maximum acceptable delay is 120 µs.

• **(B) Additional asynchronous dump due to system upgrade:** Any combinations of failure modes leading to additional asynchronous dumps.
  
  – Short RTLs in case of an asynchronous MKB trigger.
  
  – Asynchronous trigger of additional TDUs installed on the MKD side.

• **(C) Additional synchronous dump due to system upgrade:** Any combinations of failure modes leading to additional synchronous dumps. The main contributions are:
  
  – Synchronous trigger due to internal errors of additional TSUs, pulse detection hardware etc.
  
  – Synchronous trigger due to a spurious signal in the link from the RTL to the TSU.

  Synchronous dumps in case of erratic MKBs and a correctly working decoupling system are not included in these numbers, as they occur as well in the current system.

• **(D) Required maintenance / downtime due to warnings of system upgrade:** Any combination of failure modes, leading to required downtime due to an IPOC error.
  
  – IPOC warnings due to failing IPOC checks of additional TSUs, pulse detection hardware, decoupling boxes etc.

Fault tree representations for the respective failure scenarios and layout options are to be found in the appendix.
Chapter 6

Results of the Quantitative Fault Tree Analysis

The main results of this first reliability analysis are listed and illustrated below. Based on these results a discussion is provided in Chp. 7 and the decision of implementing layout 3 (1 DB, bypass) in the system upgrade is motivated in Chp. 8

6.1 General Results

The Mean Time to Failure (MTTF) is chosen as a metric for the results in this report. Table 6.1 lists the resulting MTTFs for the different design options.

6.2 Sensitivity to Parameter Changes

Sensitivity to diode failure rates: Only the failure scenarios, which are dominated by faults including the DB are sensitive to a variation of the diode failure rate. The sensitive failure cases are 'Asynchronous Dump' for layout 1 (Fig. 6.2) and 'No Dilution' for layout 2 and 3 (Fig. 6.1, Fig. 6.3)

Sensitivity to failure rate of link from RTL to MKD triggering: The sensitivity of layout 1 (no bypass of the DB) is analysed regarding the specified required total failure rate of the link from the RTL to the TSU and the MKD generators. The results are illustrated in Fig. 6.4.

Table 6.1: Predicted Mean Time To Failure (MTTF) for Different Layout Implementations and Failure Modes.

<table>
<thead>
<tr>
<th>Failure Modes</th>
<th>Layout 1, MTTF</th>
<th>Layout 2, MTTF</th>
<th>Layout 3, MTTF</th>
</tr>
</thead>
<tbody>
<tr>
<td>No Dilution</td>
<td>$6.3 \cdot 10^9$ yrs</td>
<td>$7.5 \cdot 10^{11}$ yrs</td>
<td>$3.2 \cdot 10^{12}$ yrs</td>
</tr>
<tr>
<td>Additional asynch. dump</td>
<td>$2.5 \cdot 10^5$ yrs</td>
<td>1012 yrs</td>
<td>1008 yrs</td>
</tr>
<tr>
<td>Additional synch dump</td>
<td>94 yrs</td>
<td>47 yrs</td>
<td>75 yrs</td>
</tr>
<tr>
<td>Downtime / No beam permit</td>
<td>168 yrs</td>
<td>71 yrs</td>
<td>105 yrs</td>
</tr>
</tbody>
</table>
Chapter 6 Results of the Quantitative Fault Tree Analysis

Figure 6.1: Sensitivity of failure modes to variations in the diode failure rate; Layout 1 (1 DB, no bypass).

Figure 6.2: Sensitivity of failure modes to variations in the diode failure rate; Layout 2 (2 DBs and bypass).

Figure 6.3: Sensitivity of failure modes to variation of the diode failure rate; Layout 3 (1 DB and bypass).
6.3 Comparison to Current System

The MTTF for 'No Dilution' in case of layout 3 is illustrated in Fig. 6.5 and compared to the estimated values for 2 pre-firing and in anti-phase oscillating MKBs of the current system. The MTTF of the current system depends on the coupling factor, as listed below. The impact of such a coupling factor on the diode and hence DB failures (i.e. failure due to a high voltage pulse, which puts load on all DBs) is represented in Fig. 6.5 for comparison.

- $\beta = 0$: MTTF = $3.8 \cdot 10^7$ years
- $\beta = 10^{-6}$: MTTF = $2.5 \cdot 10^5$ years
- $\beta = 10^{-4}$: MTTF = $2.5 \cdot 10^3$ years

Sensitivity to runtime: The failure modes, which are dominated by the simultaneous occurrence of two independent failures are sensitive to changes in the runtime. The results for an operational year with 160 missions, each of which lasts 50 hours (instead of 400 Missions with a runtime of 20 hours), are presented in Table 6.2.

Table 6.2: Predicted Mean Time To Failure (MTTF) for Different Layout Implementations and Failure Modes in Case of an Increased Runtime (Runtime: 50 hours, 160 Missions / Year)

<table>
<thead>
<tr>
<th>Failure Modes</th>
<th>Layout 1, MTTF</th>
<th>Layout 2, MTTF</th>
<th>Layout 3, MTTF</th>
</tr>
</thead>
<tbody>
<tr>
<td>No Dilution</td>
<td>$2.5 \cdot 10^6$ yrs</td>
<td>$1.2 \cdot 10^{11}$ yrs</td>
<td>$0.5 \cdot 10^{12}$ yrs</td>
</tr>
<tr>
<td>Additional asynch. dump</td>
<td>$9.8 \cdot 10^4$ yrs</td>
<td>1012 yrs</td>
<td>1002 yrs</td>
</tr>
<tr>
<td>Additional synch dump</td>
<td>94 yrs</td>
<td>47 yrs</td>
<td>75 yrs</td>
</tr>
<tr>
<td>Downtime / No beam permit</td>
<td>168 yrs</td>
<td>71 yrs</td>
<td>105 yrs</td>
</tr>
</tbody>
</table>

Sensitivity of the failure scenario (A) 'No Dilution' to variations of the specified failure rate of the link from the RTL to the TSU and the MKD generators. Layout 1 (1 DB, no bypass).
Figure 6.5: Comparison of the MTTF for ‘No Dilution’ of layout 3 with the current system, depending on the coupling between the MKB generators. A common cause failure of the DBs is introduced ($\beta = 0$ to $\beta = 1$).
Chapter 7

Discussion and Comparison of Proposals

The in Table 6.1 presented results show, that all system layouts fulfil the specified requirements.

It can be further seen, that the redundancy of the DB in layout 2 is not required. The resulting MTTF for the system with 1 DB per RTL is \( O(1000 \text{ yrs}) \), which is three orders of magnitude above the specified requirement of at most 1 additional asynchronous dump per year and beam. Furthermore, the failure case ‘Asynchronous Dump’ is mainly dominated by an asynchronous trigger of the additionally installed TDU 1, with a MTTF of \( O(10^3 \text{ yrs}) \). The contribution of erratic MKBs and a simultaneously short failing DB to the MTTF is \( O(10^6 \text{ yrs}) \) and therefore negligible.

Sensitivity Analysis:

Failure rates for increased system runtimes have been estimated. The resulting values still fulfil the specifications. It should be noted, that all failure scenarios, which are dominated by a path based on AND junctions are sensitive to a variation in the system runtime.

The sensitivity analysis regarding a variation of the diode failure rate shows, that the sensitive failure modes exhibit acceptable failure rates also for significantly increased diode failure rates (i.e. 200 FIT).

The sensitivity analysis regarding the rate of an open failure of the link from the TSU to the RTL underlines, that this link needs to be carefully designed. In case of layout 1 (no bypass) the MTTF of ‘No Dilution’ is dominated by the failure rate of the mentioned link. Values higher than the here assumed 20 FIT for the entire link (RTL to MKD) are not acceptable, if the specified minimum MTTF of \( 10^5 \text{ years} \) should be met. This value seems feasible, as only passive electronics are required for the pulse transmission from the RTL to the TSU. However, the foreseen redundancy (RTR from RTL A transmits to TSU A, RTR from RTL B transmits to TSU B) is therefore obligatory. The bypass of the DB, which is considered in layout 2 and 3, enables asynchronous MKD triggering in case of such a missing synchronous

---

\(^4\) It has to be noted, that the specified minimum MTTF of \( 10^5 \text{ years} \) has also been discussed to be conservative, implying that a MTTF of \( 10^4 \text{ years} \) (SIL3) could be acceptable.
trigger propagation. Hence, the results for layout 2 and 3 do not significantly depend on the failure rate of the RTL-TSU-MKD link.

**Comparison to current system:**

As soon as coupling cannot be excluded, an OR condition is introduced in the fault tree. This means, that without electromagnetic coupling two independent failures have to occur simultaneously. The electromagnetic coupling inhibits this independence (AND junction) and the predicted MTTF rapidly decreases to values in the order of ten years. As an example, the MTTF for a case of ’No Dilution’ in the current system is smaller than 10 years in case of a coupling factor of 0.1, i.e. 1 out of 10 MKB erratics is a mult-erratic. Also for coupling factors as low as $10^{-4}$ (i.e. 1 in $10^4$ MKB erratics is a multi-erratic) the predicted MTTF does not meet the required specification of $10^5$ years. Further, also for $\beta = 0$, the estimated risk of ’No Dilution’ is higher than estimated for the system upgrade. It can therefore be concluded, that as coupling cannot be excluded, installing the proposed upgrade will decrease the risk of ’No Dilution’. The newly introduced failure modes leading to ’No Dilution’ all depend on simultaneous failure of two independent systems (e.g. MKD erratic AND open RTL), which reduces the failure probability in comparison to the current system.
Chapter 8

Conclusion and Outlook

Different proposals for a decoupling mechanism between the MKB and MKD Re-Trigger Boxes at the RTLs have been assessed regarding failure modes and probability. It can be concluded, that all outlined designs fulfil the previously defined specifications.

The link from the RTL on the MKB side to the TSU needs to be carefully evaluated. Special attention has to be given to the fact, that some redundant safety paths of the trigger system (i.e. direct link from BIS to RTL) will be insufficient in case of erratic MKBs due to the large delay time. An additional bypass of the DB for triggering a delayed asynchronous dump in case of an MKB erratic is favoured as a safety measure (Layout 2 and 3). Firstly, this additional link helps to reduce the rate of the failure mode ‘No Dilution’ in case of a fault in the trigger propagation from the RTL at MKB side to the MKD generators. This bypass is furthermore favoured as it minimizes the impact of any failure modes, which have been missed at this point of the system analysis.

Additionally, it can be stated that due to the small failure rates of ‘Asynchronous Dump’ the implementation of two decoupling boxes in series (layout 2) is not necessary. Furthermore, in case of the system implementation with the bypass of the DB, this failure mode is not dominated by failures of the DB but by additional asynchronous triggers of the required TDU at MKD side (TDU 1). Installing two DB in series would not have any impact on the resulting MTTF.

The study further shows, that as electromagnetic coupling between the MKB generators cannot be excluded, the upgrade of the system reduces the probability of the failure case ‘Insufficient / No Dilution’ in comparison to the current system.

The results of this study have been discussed in the CERN Machine Protection Panel, together with energy deposition studies for the dump and the associated vacuum windows [2]. It has been decided to implement option 3 (1 DB, bypass with delayed asynchronous dump).
Bibliography


