Safety Analysis of the TCDQ

11.02.2009

Roberto Filippini

Risk and Human Reliability Group

Department of Energy, Paul Scherrer Institut

Objective of the meeting and Topics

Topics

- Tasks overview
- TCDQ system description
- The modelling framework
- Quantification and results
- Conclusions and Outlook

Overview of tasks

1. Familiarization with TCDQ functioning principles
2. Consequences and scenario frequency
3. Scoping the problem for safety study
4. Systems analysis (mechanisms of failure)
   - Dependency analysis
   - Data base development for calculation
5. Overall **quantification** and result review
6. Final report documentation

Scoping the problem

Scope

- Probability of failure of the TCDQ systems (two TCDQ) to be configured to protect the LHC elements at the occurrence of an asynchronous beam dump over 1 year of LHC operation, 400 fills

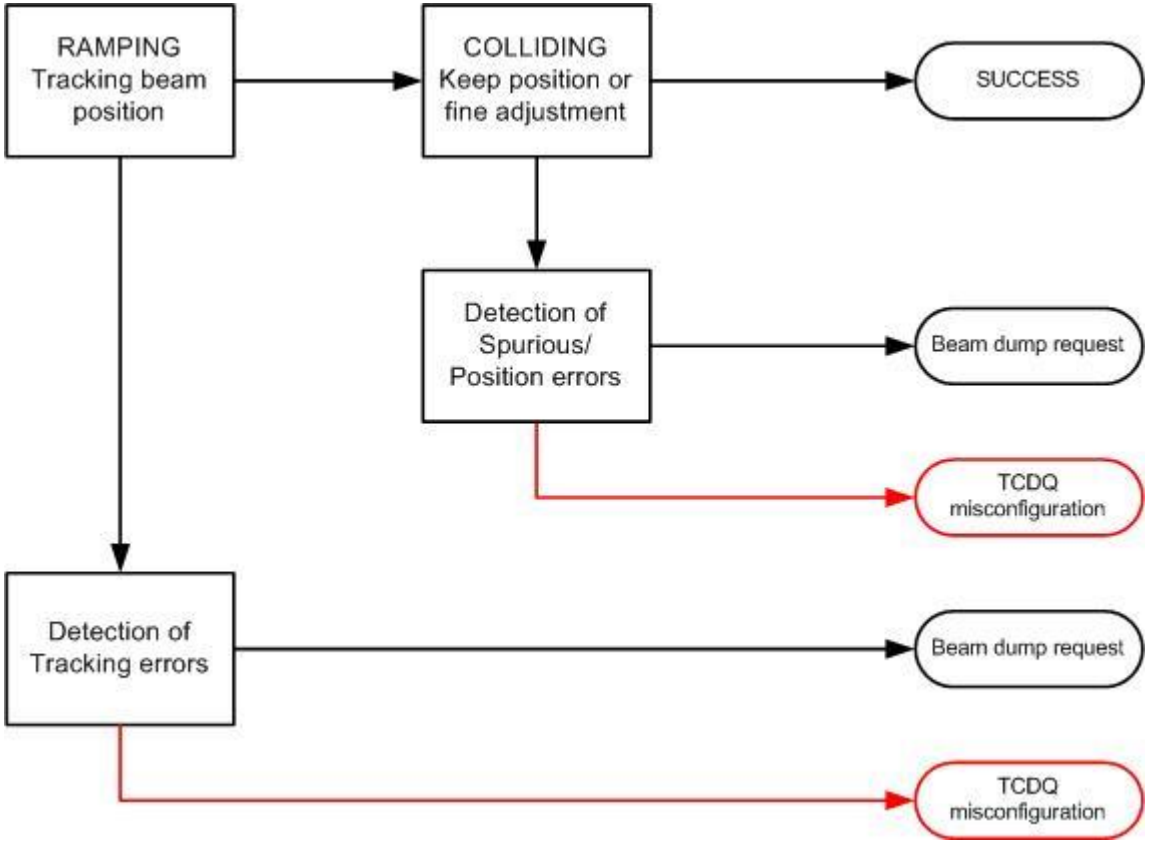
Within the scope

- TCDQ configuration at LHC injection, ramping and colliding (top energy)
- Servo and remote (manual adjustment) controls
- PLC for control and interlocking functions, input-outputs boards, motors and motor drive power converters, position measurements, communications

Outside the scope

- MCS, the timing system, the local BIC, the operator in the control room
- Calculation of frequency and consequences of an asynchronous beam dump (estimate from LBDS reliability studies, R. Filippini 2006)

LHC phases and TCDQ



TCDQ system description: multi-view

- **TCDQ operation modes and LHC phases**

  Understanding TCDQ operations

- **TCDQ functional-logic description**

  Understanding of functions and the way they interact in a logic way (geographical location does not matter)

- **TCDQ layout at high-level**

  Mapping of functions into components and identification of signal paths (geographical location does matter)

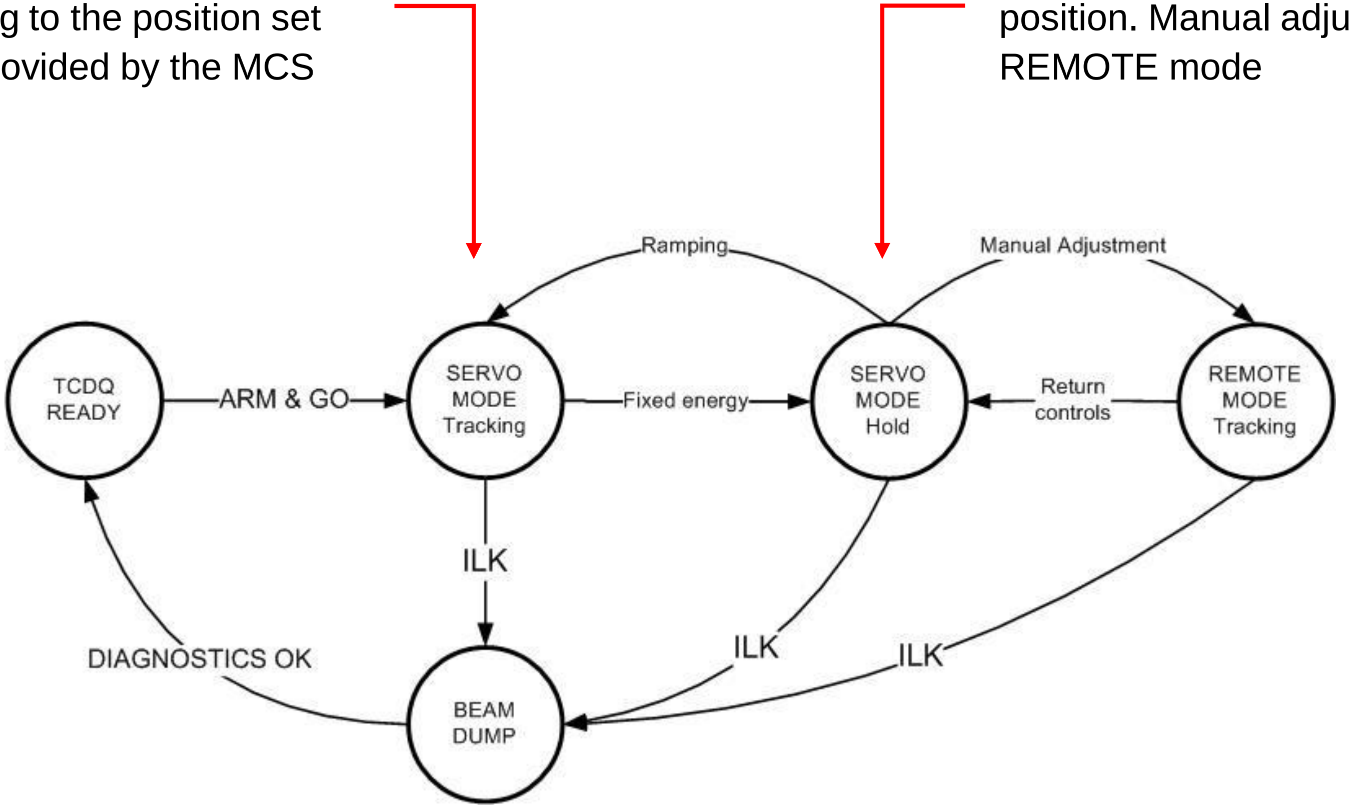
TCDQ operation modes

Injection-Ramping

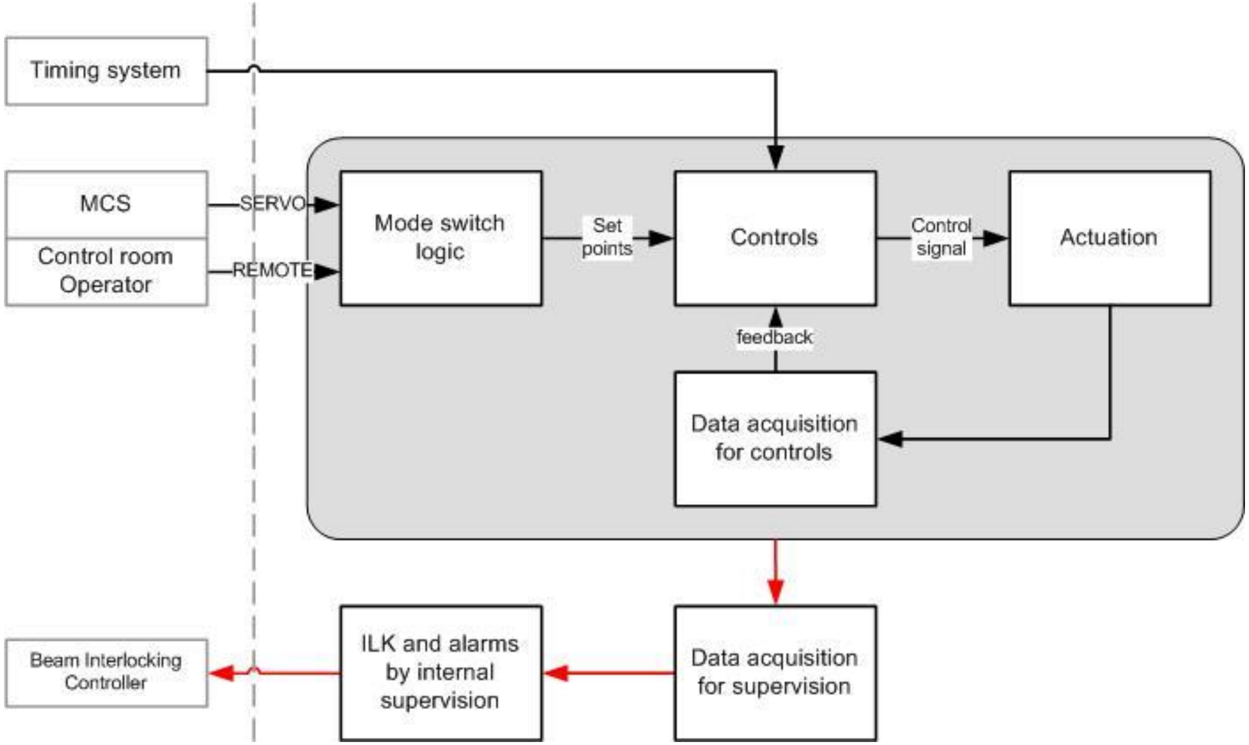
TCDQ tracks beam position according to the position set points provided by the MCS

Colliding

TCDQ keeps the required position. Manual adjustments in REMOTE mode



TCDQ functional description


Timing system
MCS
Control room Operator
SERVO
REMOTE
Mode switch logic
Set points
Controls
Control signal
Actuation
feedback
Data acquisition for controls
Beam Interlocking Controller
ILK and alarms by internal supervision
Data acquisition for supervision

Blocks are functions

TCDQ control loop

Mode switch logic

Controls in servo/remote

Data acquisition for controls (position, settings)

TCDQ actuation

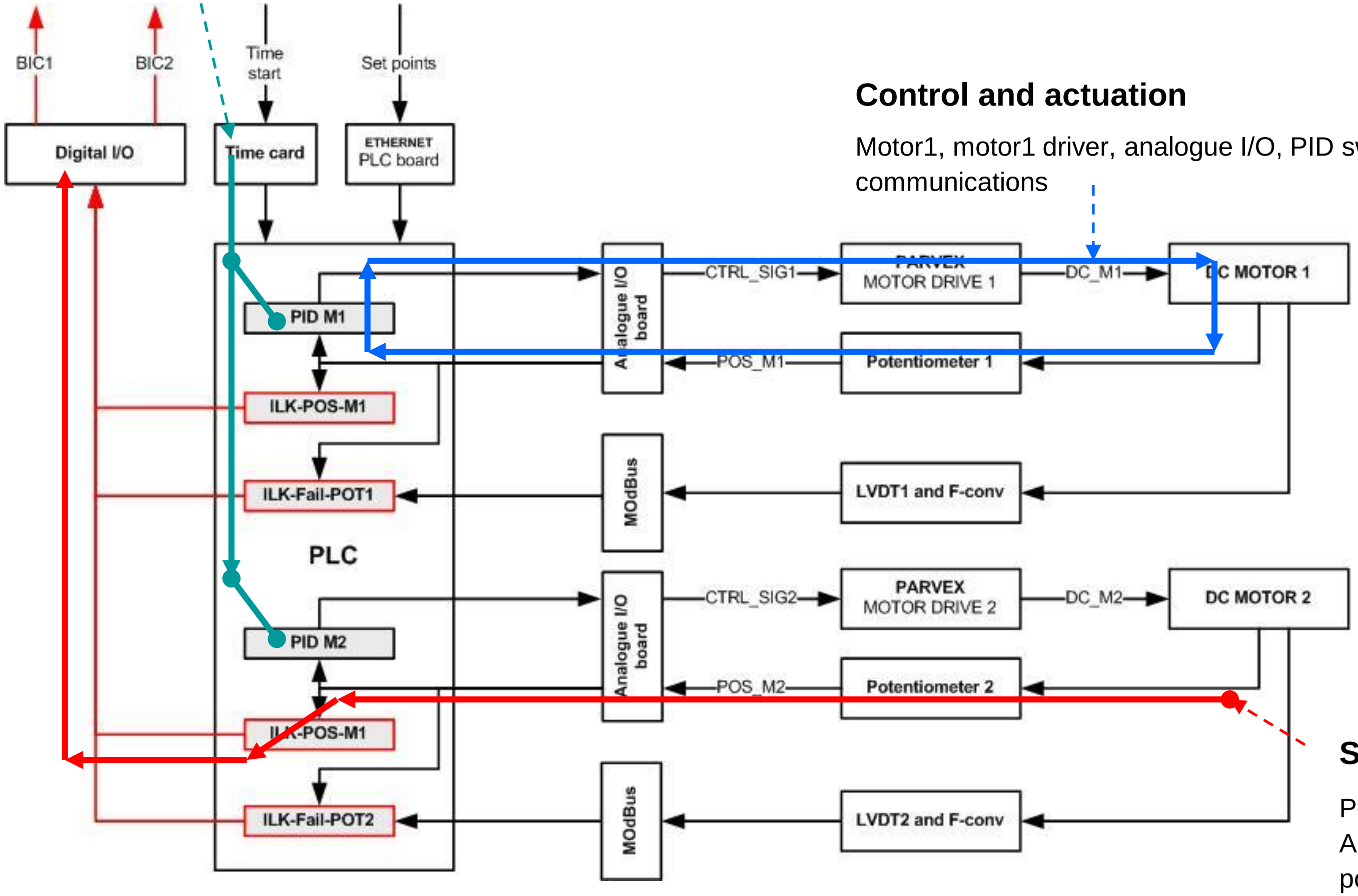
TCDQ supervision

Data acquisition

ILK functions to BIC

TCDQ Layout

Start event: Time card, PLC and communications



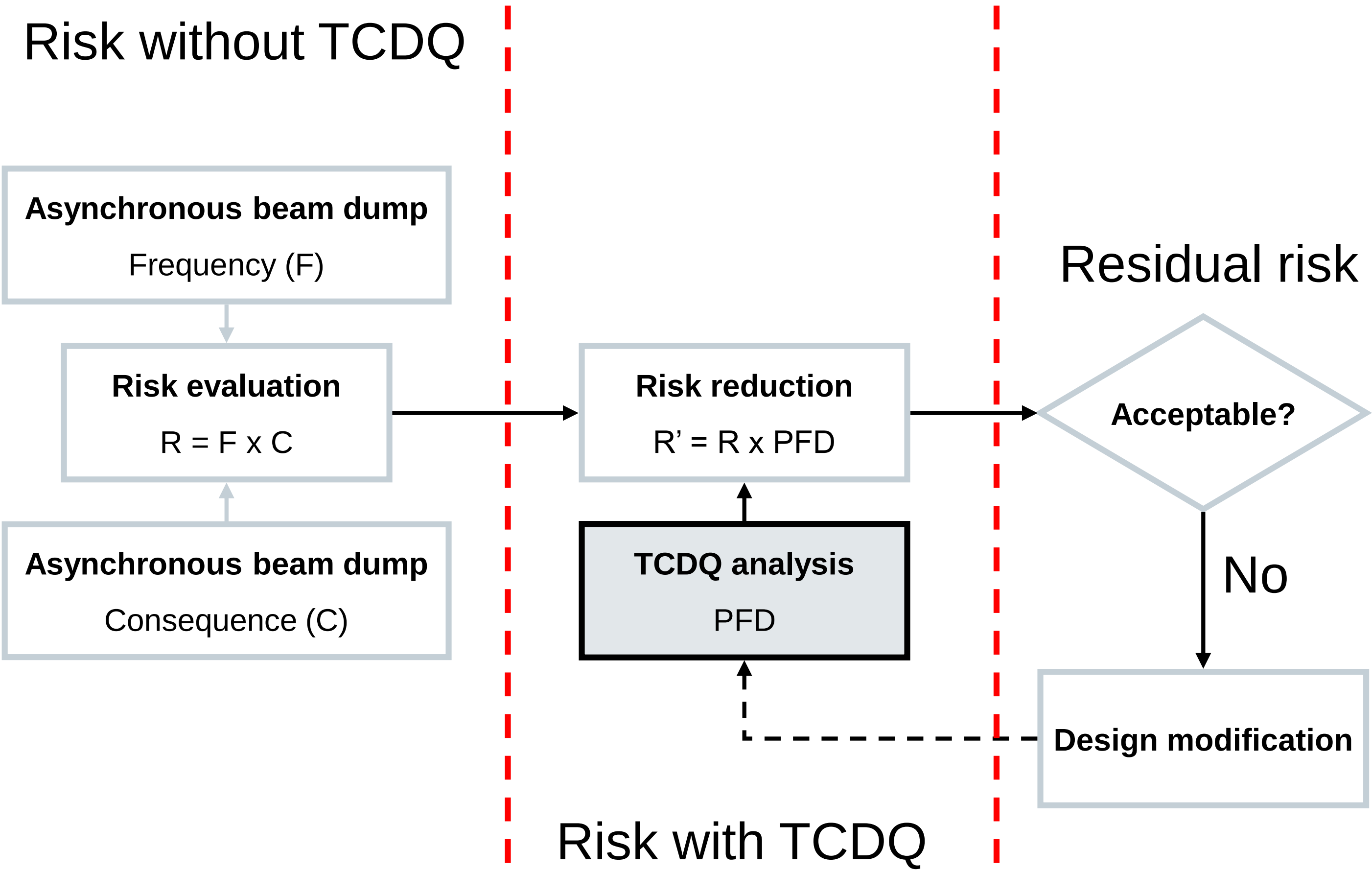
Control and actuation

Motor1, motor1 driver, analogue I/O, PID sw, potentiometer, communications

Supervision of position

Potentiometer, Digital I/O board, Analogue I/O board, PLC position threshold ILK

Risk assessment: general framework



Risk without TCDQ

Asynchronous beam dump

Frequency (F)

Risk evaluation

R = F x C

Asynchronous beam dump

Consequence (C)

Risk reduction

R’ = R x PFD

TCDQ analysis

PFD

Risk with TCDQ

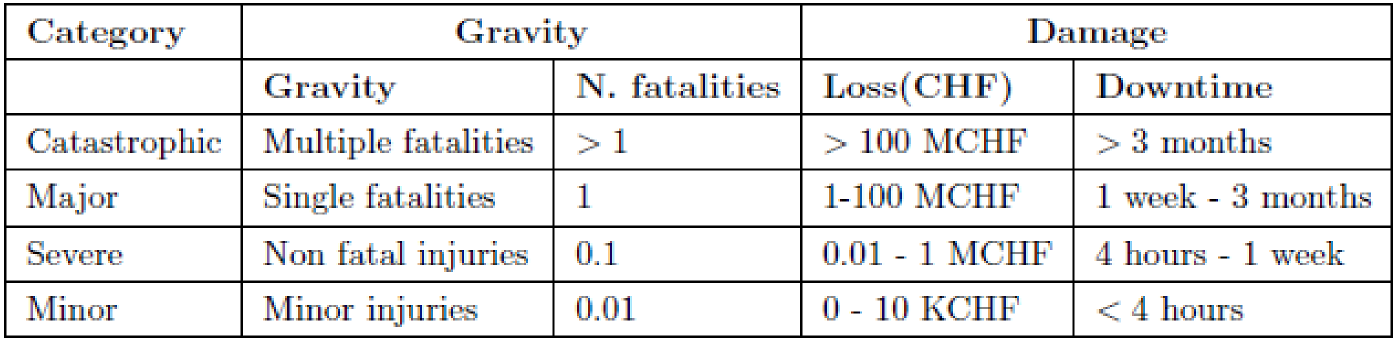
Residual risk

Acceptable?

No

Design modification

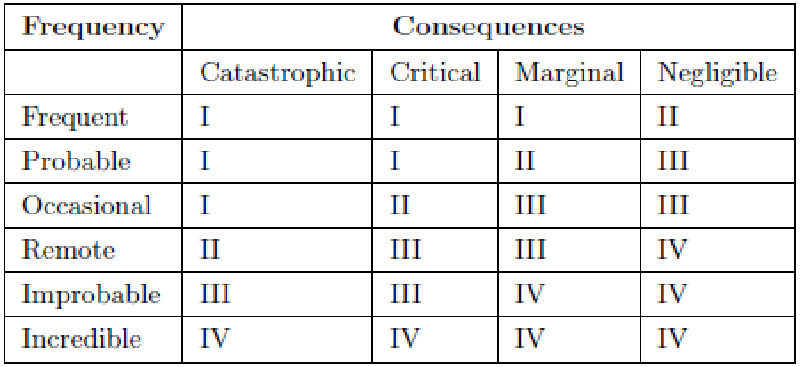
Risk assessment based on IEC 61508 std



Category	Gravity		Damage	
	Gravity	N. fatalities	Loss(CHF)	Downtime
Catastrophic	Multiple fatalities	> 1	$>$ 100 MCHF	$>$ 3 months
Major	Single fatalities	1	1-100 MCHF	1 week - 3 months
Severe	Non fatal injuries	0.1	0.01 - 1 MCHF	4 hours - 1 week
Minor	Minor injuries	0.01	0 - 10 KCHF	$<$ 4 hours

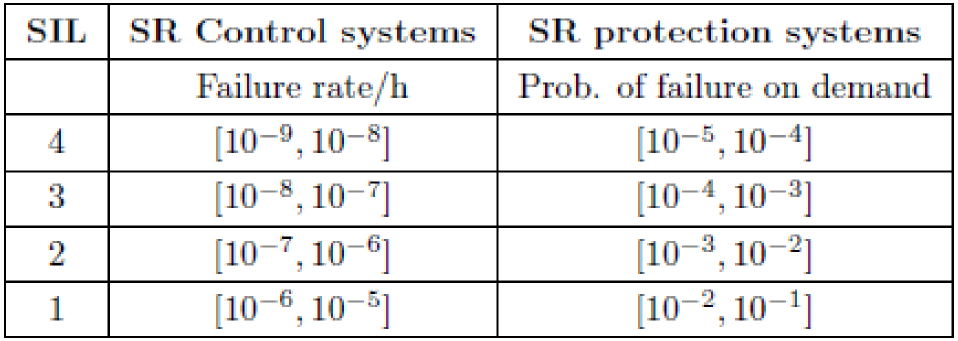
Consequences are catastrophic

Risk = F x C



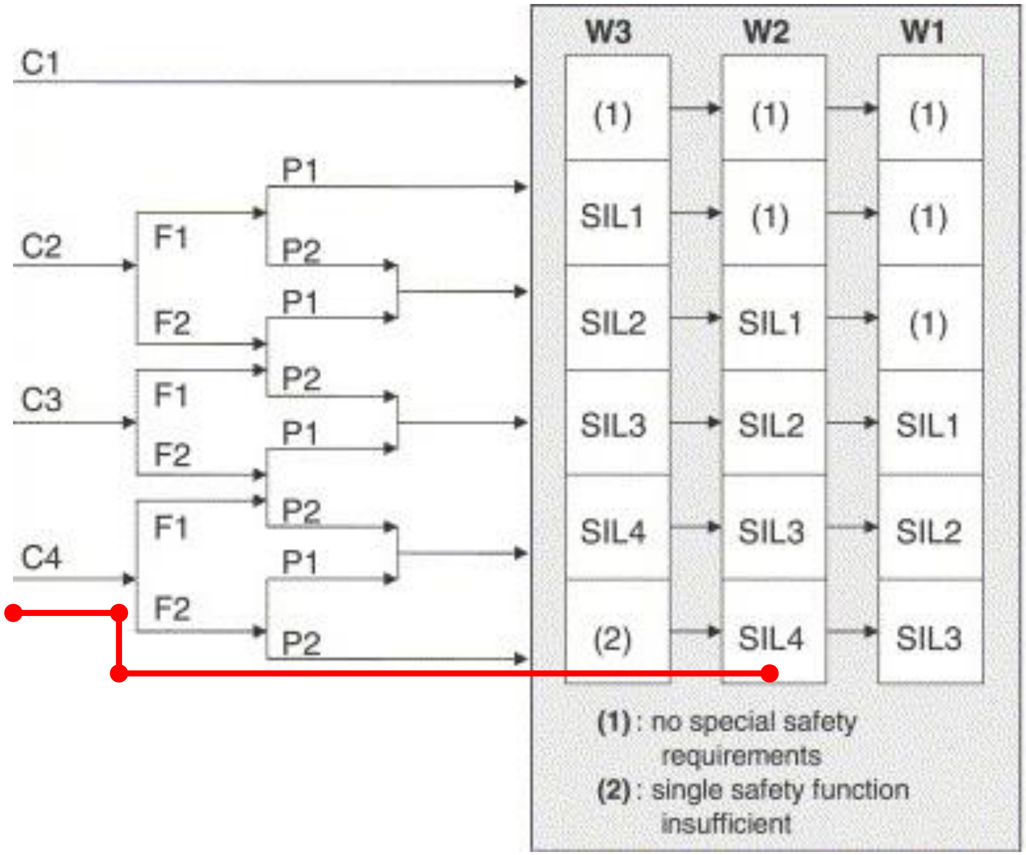
Frequency	Consequences			
	Catastrophic	Critical	Marginal	Negligible
Frequent	I	I	I	II
Probable	I	I	II	III
Occasional	I	II	III	III
Remote	II	III	III	IV
Improbable	III	III	IV	IV
Incredible	IV	IV	IV	IV

The safety level (low demand mode of operation)



SIL	SR Control systems	SR protection systems
	Failure rate/h	Prob. of failure on demand
4	$[10^{-9}, 10^{-8}]$	$[10^{-5}, 10^{-4}]$
3	$[10^{-8}, 10^{-7}]$	$[10^{-4}, 10^{-3}]$
2	$[10^{-7}, 10^{-6}]$	$[10^{-3}, 10^{-2}]$
1	$[10^{-6}, 10^{-5}]$	$[10^{-2}, 10^{-1}]$

Determining SIL: risk graph method



	W3	W2	W1
C1	(1)	(1)	(1)
	SIL1	(1)	(1)
	SIL2	SIL1	(1)
	SIL3	SIL2	SIL1
	SIL4	SIL3	SIL2
	(2)	SIL4	SIL3

(1): no special safety requirements

(2): single safety function insufficient

Consequence severity

C1 → minor injury

C2 → serious injury or single death

C3 → multiple deaths

C4 → a very high number of deaths

Exposure time

F1 → rare to frequent

F2 → frequent to continuous

Possibility of avoidance

P1 → possible

P2 → not likely

Probability of undesirable occurrences

W1→ very slight probability

W2→ low probability

W3 → high probability

TCDQ safety analysis: modeling steps

Initiating event

- The asynchronous beam dump

System failure model

- Fault tree of the TCDQ to position itself in the correct place

Data collection

- Failure events (independent and CCF),
- Failure rates, probabilities on demand
- Supervision, tests and periodical checks

Analysis and quantification

- Operation scenario of 400 fills (10 hours each), 4000 hours/ year
- 1 fill = about 2 hours tracking position and 8 hours hold position
- 1 remote mode every 10 fills

Data collection

Failure events

- 80 independent failure events, several dependencies and common causes of failure (CCF)

Failure data

- Failure rates and probability of failure on demand are at assembly level.
- Some deduced from previous reliability analysis (LBDS studies)

Periodical checks

- Rearming of between two LHC fills demand almost all components of TCDQ
- Yearly calibration and test

REMARK: spurious ILK, power supply (fail safe), and break-short false contacts results in false beam dumps are not included.

Data Collection: Failure Events

The following features have been modeled

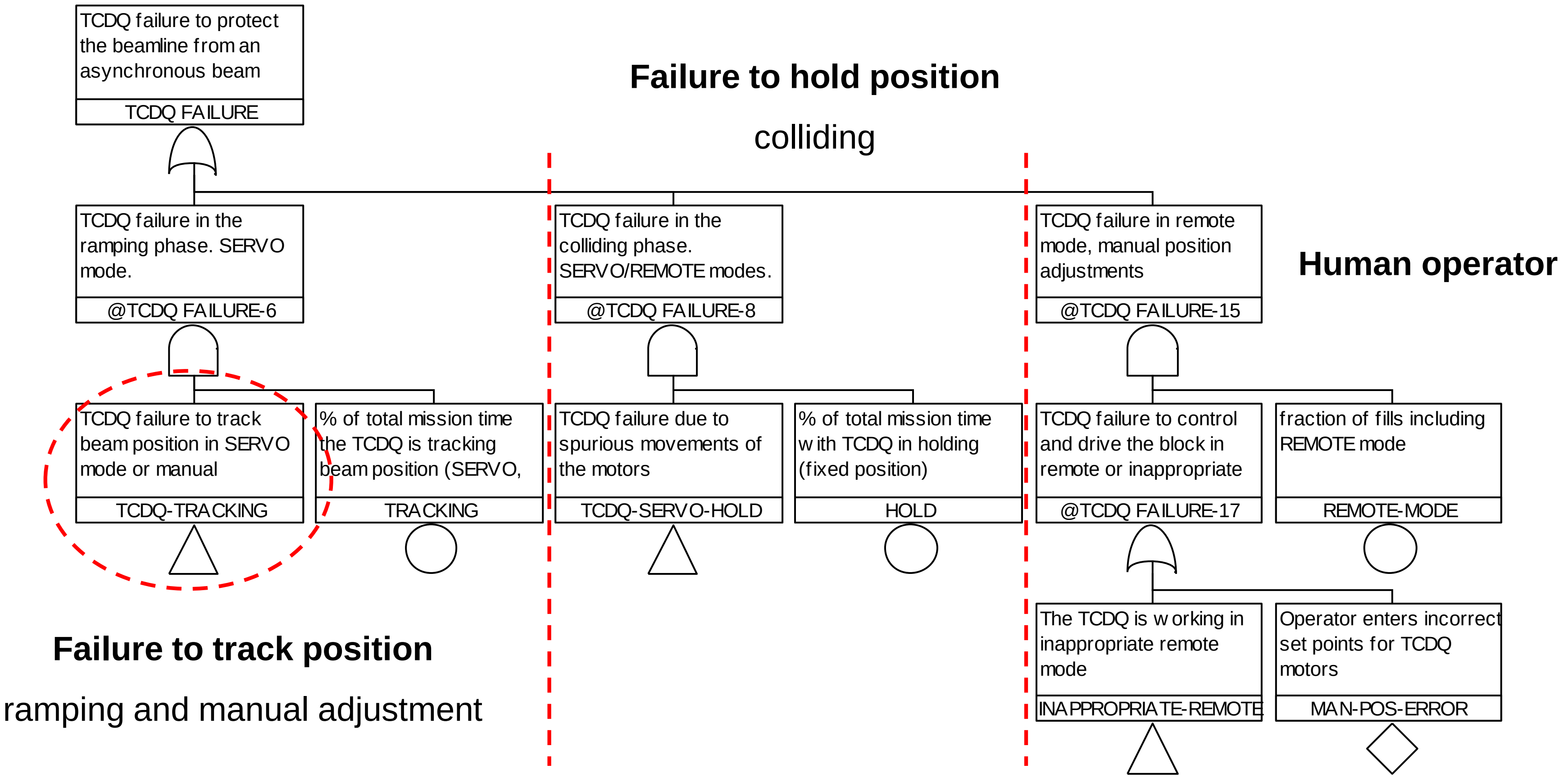
- failure modes of the single system components
- availability of power (electrical, mechanical etc) and other support systems
- presence and correctness of actuation and control signals, considering the signal paths from logic to actuation elements
- correct generation and delivery of ILK signals
- integrity of data from MCS and timing system
- impact of errors during maintenance, testing, return to service, and system configuration
- common cause failures of components within the system or in redundant trains of a system or issued by the same device.

The Failure Model

- **Fault tree:** It represents about 80 failure events, dependencies and CCF in a logic structure. Leaves account for basic failure events of TCDQ components (Risk Spectrum®)

- **The fault tree is split into two branches**
- Tracking beam position: TCDQ failures to track beam position in servo control mode or by manual adjustment (whenever position has to be changed).
- Hold position: TCDQ failure to hold the required position at fixed energy

The Fault Tree



Failure to hold position

colliding

Human operator

Failure to track position

ramping and manual adjustment

TCDQ failure to protect the beamline from an asynchronous beam
TCDQ FAILURE

TCDQ failure in the ramping phase. SERVO mode.
@TCDQ FAILURE-6

TCDQ failure in the colliding phase. SERVO/REMOTE modes.
@TCDQ FAILURE-8

TCDQ failure in remote mode, manual position adjustments
@TCDQ FAILURE-15

TCDQ failure to track beam position in SERVO mode or manual
TCDQ-TRACKING

% of total mission time the TCDQ is tracking beam position (SERVO,
TRACKING

TCDQ failure due to spurious movements of the motors
TCDQ-SERVO-HOLD

% of total mission time w ith TCDQ in holding (fixed position)
HOLD

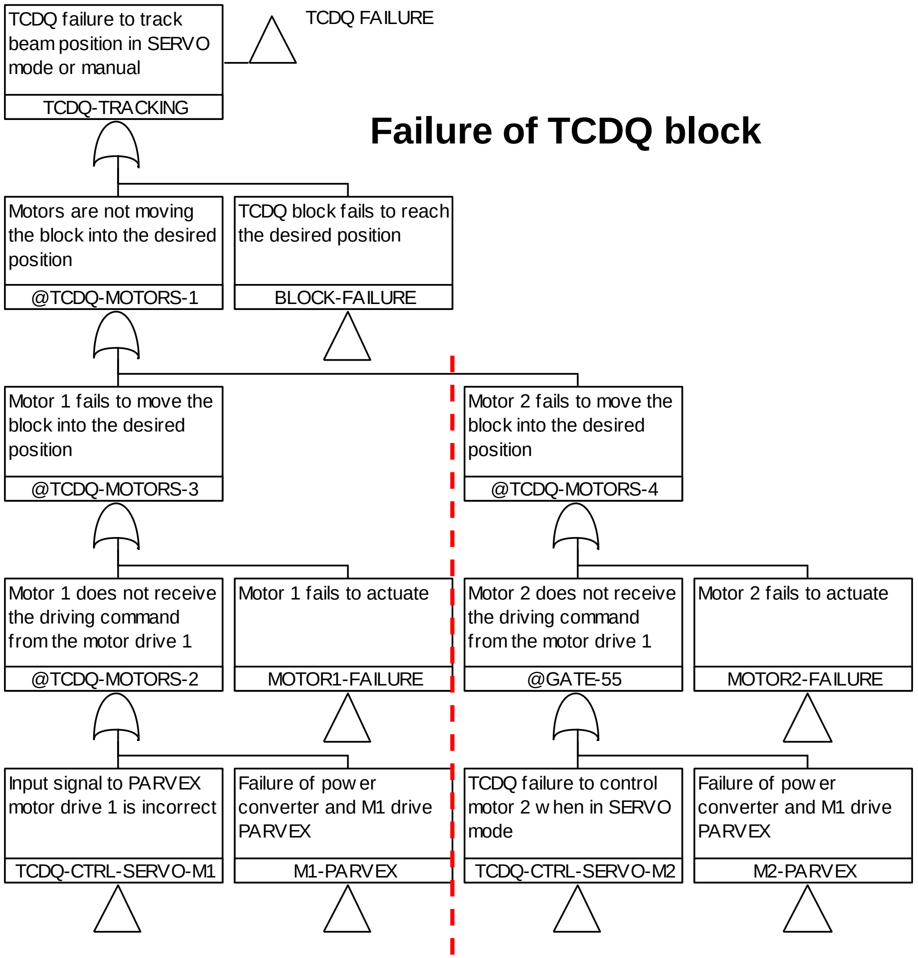
TCDQ failure to control and drive the block in remote or inappropriate
@TCDQ FAILURE-17

fraction of fills including REMOTE mode
REMOTE-MODE

The TCDQ is w orking in inappropriate remote mode
INAPPROPRIATE-REMOTE

Operator enters incorrect set points for TCDQ motors
MAN-POS-ERROR

The Fault tree
Position tracking


TCDQ failure to track beam position in SERVO mode or manual
TCDQ-TRACKING
TCDQ FAILURE
Failure of TCDQ block
Motors are not moving the block into the desired position
@TCDQ-MOTORS-1
TCDQ block fails to reach the desired position
BLOCK-FAILURE
Motor 1 fails to move the block into the desired position
@TCDQ-MOTORS-3
Motor 2 fails to move the block into the desired position
@TCDQ-MOTORS-4
Motor 1 does not receive the driving command from the motor drive 1
@TCDQ-MOTORS-2
Motor 1 fails to actuate
MOTOR1-FAILURE
Motor 2 does not receive the driving command from the motor drive 1
@GATE-55
Motor 2 fails to actuate
MOTOR2-FAILURE
Input signal to PARVEX motor drive 1 is incorrect
TCDQ-CTRL-SERVO-M1
Failure of pow er converter and M1 drive PARVEX
M1-PARVEX
TCDQ failure to control motor 2 w hen in SERVO mode
TCDQ-CTRL-SERVO-M2
Failure of pow er converter and M1 drive PARVEX
M2-PARVEX

Failure Motor 1

Tracking errors

Spurious controls

Incorrect set points

Incorrect timing

Failure Motor 2

Tracking errors

Spurious controls

Incorrect set points

Incorrect timing

The Fault tree

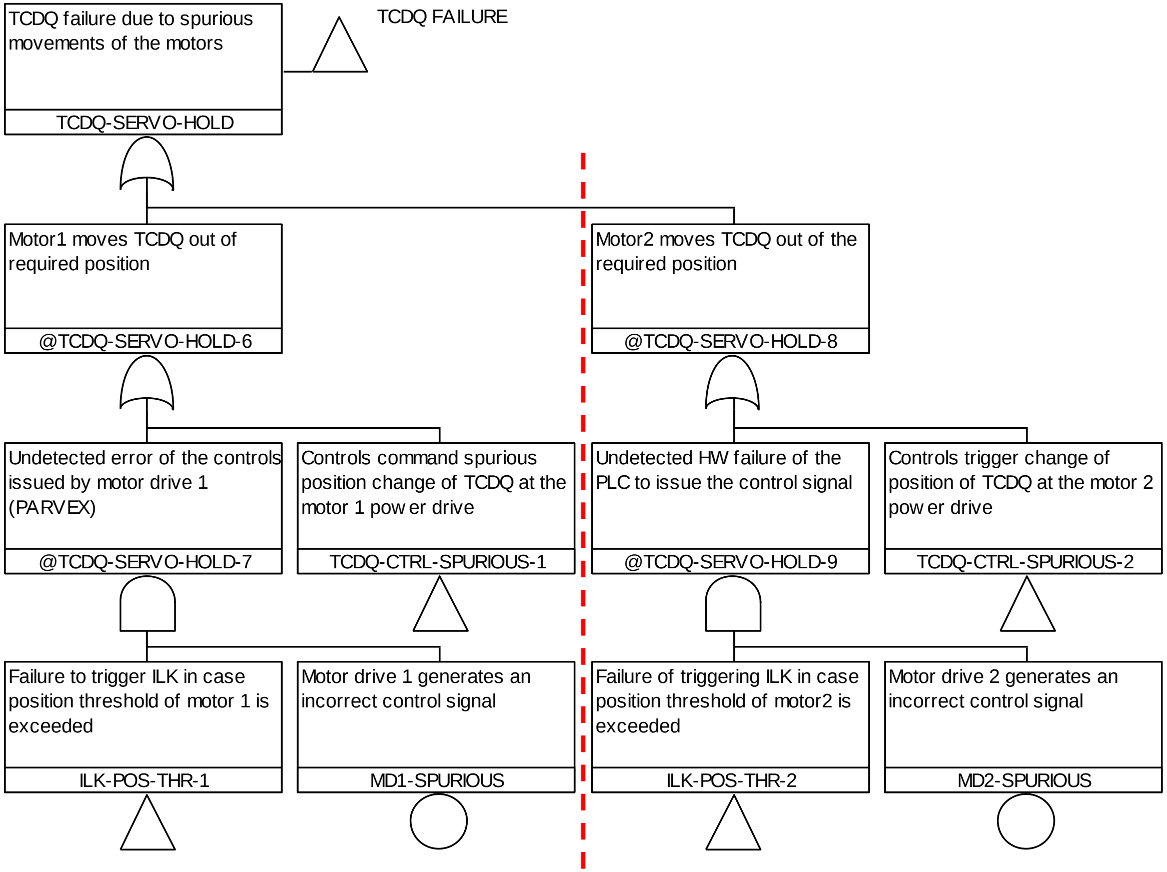
Servo mode, hold position

Failure motor 1

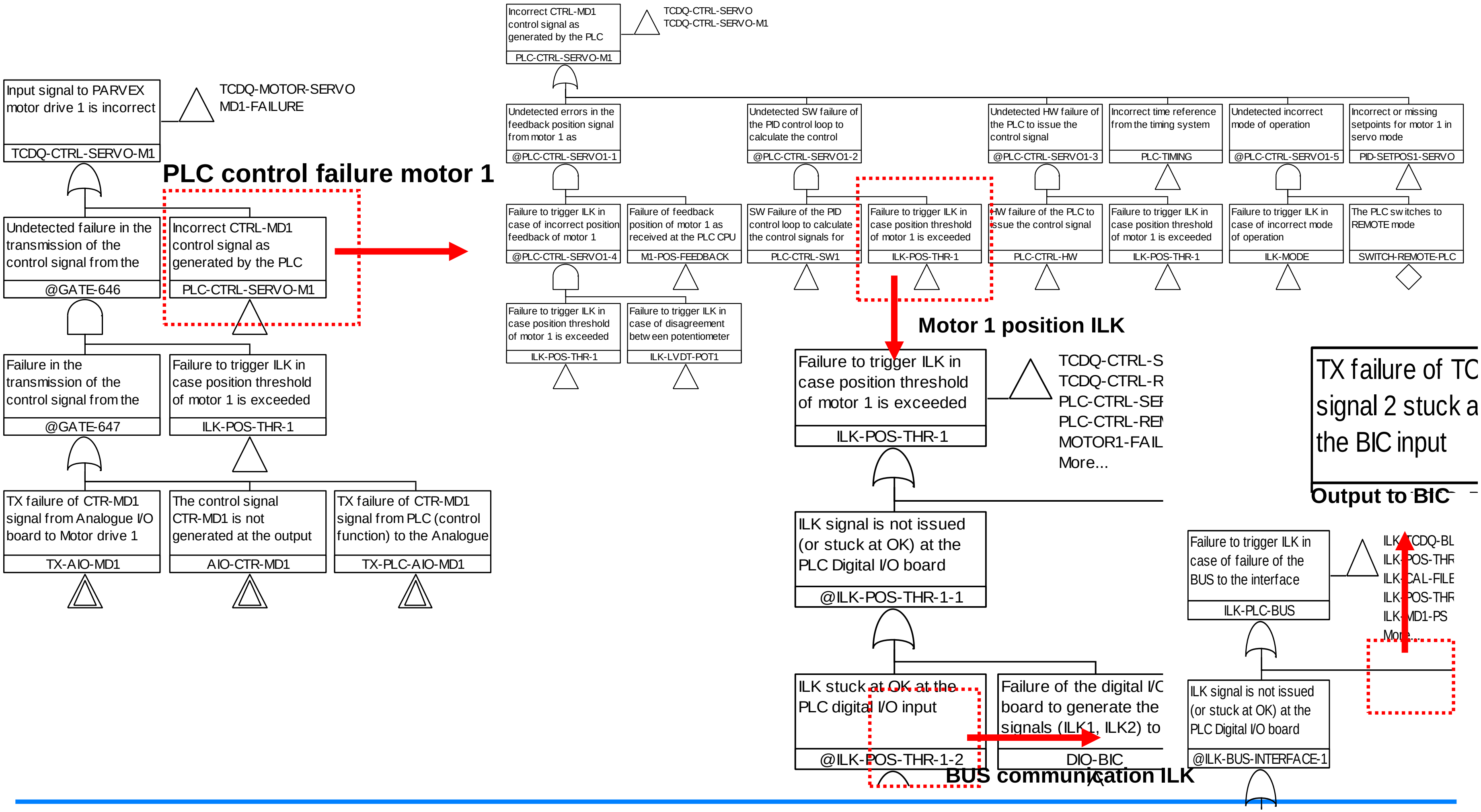
Spurious controls

Failure motor 2

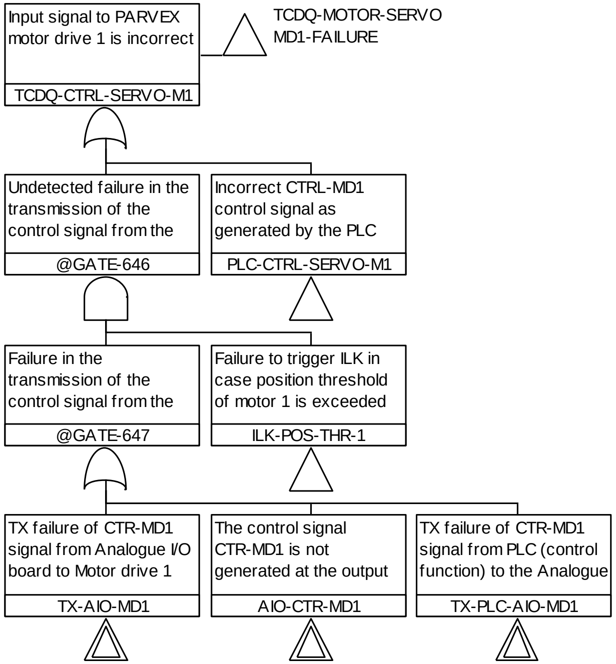
Spurious controls


TCDQ failure due to spurious movements of the motors
TCDQ-SERVO-HOLD
TCDQ FAILURE
Motor1 moves TCDQ out of required position
@TCDQ-SERVO-HOLD-6
Motor2 moves TCDQ out of the required position
@TCDQ-SERVO-HOLD-8
Undetected error of the controls issued by motor drive 1 (PARVEX)
@TCDQ-SERVO-HOLD-7
Controls command spurious position change of TCDQ at the motor 1 power drive
TCDQ-CTRL-SPURIOUS-1
Undetected HW failure of the PLC to issue the control signal
@TCDQ-SERVO-HOLD-9
Controls trigger change of position of TCDQ at the motor 2 power drive
TCDQ-CTRL-SPURIOUS-2
Failure to trigger ILK in case position threshold of motor 1 is exceeded
ILK-POS-THR-1
Motor drive 1 generates an incorrect control signal
MD1-SPURIOUS
Failure of triggering ILK in case position threshold of motor2 is exceeded
ILK-POS-THR-2
Motor drive 2 generates an incorrect control signal
MD2-SPURIOUS

…navigation in the fault tree structure


Input signal to PARVEX motor drive 1 is incorrect
TCDQ-CTRL-SERVO-M1
TCDQ-MOTOR-SERVO
MD1-FAILURE
PLC control failure motor 1
Undetected failure in the transmission of the control signal from the
@GATE-646
Incorrect CTRL-MD1 control signal as generated by the PLC
PLC-CTRL-SERVO-M1
Failure in the transmission of the control signal from the
@GATE-647
Failure to trigger ILK in case position threshold of motor 1 is exceeded
ILK-POS-THR-1
TX failure of CTR-MD1 signal from Analogue I/O board to Motor drive 1
TX-AIO-MD1
The control signal CTR-MD1 is not generated at the output
AIO-CTR-MD1
TX failure of CTR-MD1 signal from PLC (control function) to the Analogue
TX-PLC-AIO-MD1
Incorrect CTRL-MD1 control signal as generated by the PLC
PLC-CTRL-SERVO-M1
TCDQ-CTRL-SERVO
TCDQ-CTRL-SERVO-M1
Undetected errors in the feedback position signal from motor 1 as
@PLC-CTRL-SERVO1-1
Undetected SW failure of the PID control loop to calculate the control
@PLC-CTRL-SERVO1-2
Undetected HW failure of the PLC to issue the control signal
@PLC-CTRL-SERVO1-3
Incorrect time reference from the timing system
PLC-TIMING
Undetected incorrect mode of operation
@PLC-CTRL-SERVO1-5
Incorrect or missing setpoints for motor 1 in servo mode
PID-SETPOS1-SERVO
Failure to trigger ILK in case of incorrect position feedback of motor 1
@PLC-CTRL-SERVO1-4
Failure of feedback position of motor 1 as received at the PLC CPU
M1-POS-FEEDBACK
SW Failure of the PID control loop to calculate the control signals for
PLC-CTRL-SW1
Failure to trigger ILK in case position threshold of motor 1 is exceeded
ILK-POS-THR-1
HW failure of the PLC to issue the control signal
PLC-CTRL-HW
Failure to trigger ILK in case position threshold of motor 1 is exceeded
ILK-POS-THR-1
Failure to trigger ILK in case of incorrect mode of operation
ILK-MODE
The PLC switches to REMOTE mode
SWITCH-REMOTE-PLC
Failure to trigger ILK in case position threshold of motor 1 is exceeded
ILK-POS-THR-1
Failure to trigger ILK in case of disagreement between potentiometer
ILK-LVDT-POT1
Motor 1 position ILK
Failure to trigger ILK in case position threshold of motor 1 is exceeded
ILK-POS-THR-1
TCDQ-CTRL-S
TCDQ-CTRL-R
PLC-CTRL-SEF
PLC-CTRL-REI
MOTOR1-FAIL
More...
ILK signal is not issued (or stuck at OK) at the PLC Digital I/O board
@ILK-POS-THR-1-1
ILK stuck at OK at the PLC digital I/O input
@ILK-POS-THR-1-2
Failure of the digital I/C board to generate the signals (ILK1, ILK2) to
DIO-BIC
BUS communication ILK
TX failure of TC signal 2 stuck a the BIC input
Output to BIC
Failure to trigger ILK in case of failure of the BUS to the interface
ILK-PLC-BUS
ILK-TCDQ-BL
ILK-POS-THR
ILK-CAL-FILE
ILK-POS-THR
ILK-MD1-PS
More...
ILK signal is not issued (or stuck at OK) at the PLC Digital I/O board
@ILK-BUS-INTERFACE-1

Fault tree: documentation



Input signal to PARVEX motor drive 1 is incorrect

TCDQ-CTRL-SERVO-M1

TCDQ-MOTOR-SERVO MD1-FAILURE

Undetected failure in the transmission of the control signal from the

@GATE-646

Incorrect CTRL-MD1 control signal as generated by the PLC

PLC-CTRL-SERVO-M1

Failure in the transmission of the control signal from the

@GATE-647

Failure to trigger ILK in case position threshold of motor 1 is exceeded

ILK-POS-THR-1

TX failure of CTR-MD1 signal from Analogue I/O board to Motor drive 1

TX-AIO-MD1

The control signal CTR-MD1 is not generated at the output

AIO-CTR-MD1

TX failure of CTR-MD1 signal from PLC (control function) to the Analogue

TX-PLC-AIO-MD1

PLC-CTRL-SERVO-M1	Models the failure of PLC control function to generate the correct command to DC motor 1	PLC CPU Bus communications ETHERNET MCS Set points table Timing card	Calculation of control signal to motor 1
		PLC CPU Bus communications Analogue I/ O Digital I/ O ETHERNET Threshold table Potentiometer 1 LVDT	ILK function for position threshold and feedback comparison for motor 1
ILK-POS-THR-1	Models the failure of the PLC interlock function to trigger the ILK to BIC in case the position threshold of motor 1 is exceeded	PLC CPU Bus communications Digital I/ O board Threshold table	Position threshold ILK of motor 1
TX-AIO-MD1	Models the failure of the transmission from the Analogue IO board to the motor drive (PARVEX) power converter of motor 1	TX from Analogue I/ O output to MD1 input	Control signal motor 1
AIO-CTR-MD1	Models the failure of the analogue IO board to present the control signal of motor 1 at its output	Analogue I/ O board output and analogue I/ O board	Control signal motor 1
TX-PLC-AIO-MD1	Models the TX failure of control signal of motor 1 from the PLC to the analogue I/ O board	PLC Profibus internal communications	Control signal motor 1

Analysis and Quantification
Results overview

Assumptions

- One year of LHC operation consists of 400 fills
- 1 Fill is 10 hours, of which 2 hours injection-ramping, 8 hours colliding
- 1 remote manual adjustment every 10 fills, of 2 hours length
- All failures are discovered at the rearming before next fill
- Demand rate = 0.4 asynchronous beam dump per beam line, per year (LBDS reliability study, R. Filippini)

Safety figures-of-merit (average Probability of Failure on Demand**)**

- TCDQ is 1.82 E-5 per demand (5th% = 2.7 E-06, 95th % = 5.4 E-05)
- Two TCDQ are 3.64 E-05 ⇒ **SIL4**

Quantification and results: contributors

Major contributors (94%)

Secondary contributors (6%)

Combination of the failure event and its missed detection

1	1.100E-05	60.52	TRACKING	PLC-TIMING-CARD	
2	3.900E-06	21.46	HOLD	PLC-CPU-SW	
3	1.100E-06	6.05	TRACKING	PLC-CPU-SW	
4	1.100E-06	6.05	TRACKING	ETHERNET-BOARD	
5	1.100E-07	0.61	TRACKING	BLOCK FAILURE	PLC-ILK-BLOCKER-SW
6	9.900E-08	0.54	TRACKING	NO-CAL-MOTOR	PLC-ILK-CAL-FILE-SW
7	8.910E-08	0.49	TRACKING	DC-MOTOR2-CAL	PLC-ILK-POS-THR2-SW
8	8.910E-08	0.49	TRACKING	DC-MOTOR1-CAL	PLC-ILK-POS-THR1-SW
9	3.900E-08	0.21	HOLD	AIO-CTR-MD2	PLC-ILK-POS-THR2-SW
10	3.900E-08	0.21	HOLD	TX-AIO-MD1	PLC-ILK-POS-THR1-SW
11	3.900E-08	0.21	HOLD	MD1-SPURIOUS	PLC-ILK-POS-THR1-SW
12	3.900E-08	0.21	HOLD	PID-CONTROL-M2	PLC-ILK-POS-THR2-SW

Quantification and Results:
Main contributors

- **Start signal (60.5%)**

  Failure of the PLC time card to transmit start signal to PLC

- **Control and supervision (27.5%)**

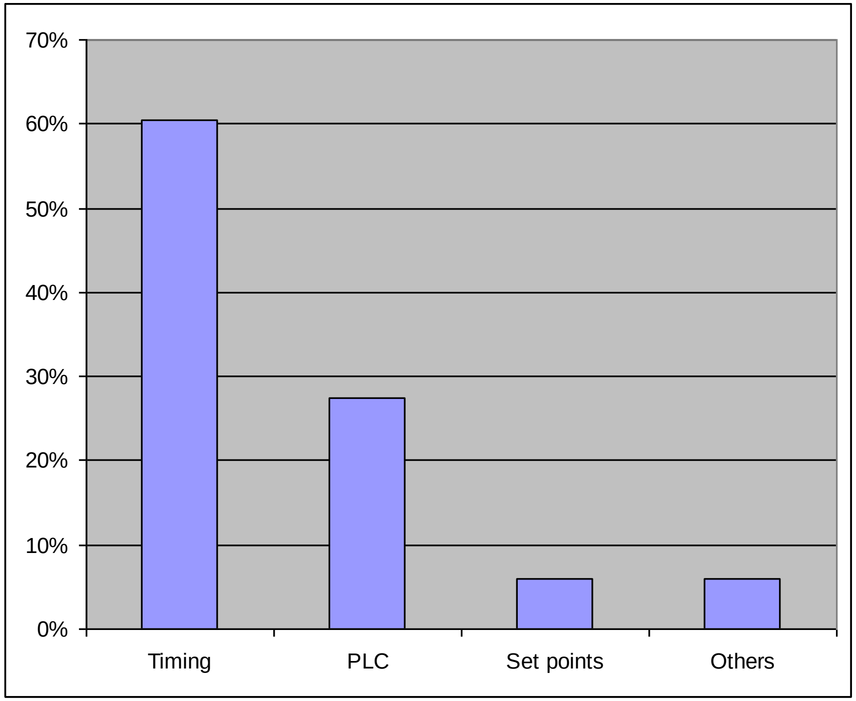
  PLC CPU fails with both control and supervision functions

- **Position settings (6.0%)**

  ETHERNET board fails to transmit position settings to PLC

- **Several others (6.0%)**

  Failure event and missed fault detection (< 0.6% each)



Discussion of results: default case study

Results insights

<u>Conservative assumptions</u>

- Misconfigurations of TCDQ, either small or big, lead always to failure

<u>Optimistic assumptions</u>

- Source of asynchronous beam dump is the LBDS, while other sources exist
- Rearming cover diagnostics of the system components, which is recovered to an as good as new state.

Sensitivity analysis

1. **Sensitivity to operation scenario**

   The TCDQ is always demanded in “tracking configuration”

   - 10 hours of fill, instead of 2 hours

2. **Sensitivity to failure data**

   Failure data increased of a factor 10

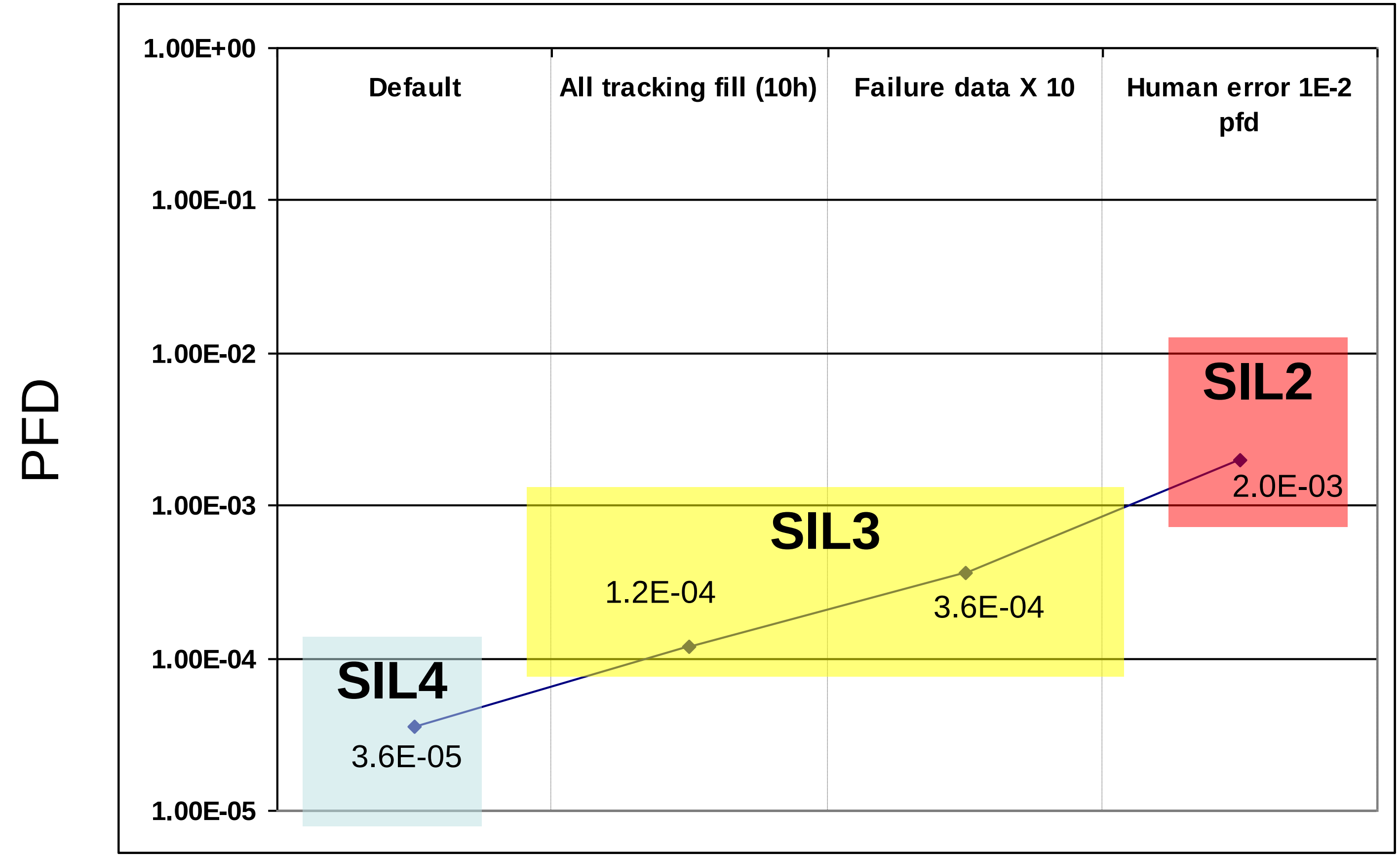
3. **Sensitivity to external factors: human error**

   Human errors when TCDQ is in remote mode.

   - Probabilities on demand 1E-3 to 1E-2

REMARK: the model is updated to include the external failure events

Sensitivity analysis: Results



Operator manual adjustments of TCDQ

- A study of the task and performance conditions has not been performed.

Assumptions for manual adjustment of TCDQ position:

- Manual adjustments are performed in 1 of 10 fills, or 40 times a year based on the assumed 400 fills per year.
- A manual misconfiguration of the TCDQ always leaves the TCDQ unavailable to protect the LHC in the event of an asynchronous beam dump.
- Multiple adjustments may be performed in a fill that includes a manual adjustment and adjustments are made to both TCDQ motors. In this sensitivity analysis, all adjustments are viewed as a single operation.

Basis for Human Error Probability = 0.01

Source	Description	Value
THERP	**Initial-screening** model Table 20-2 Failure to perform rule-based action correctly when written procedures are available and used (1) **Errors per critical step without recovery factors**	0.05
	Initial-screening model Table 20-2 (2) **Errors per critical step with recovery factors**	0.025
NARA	Generic Task Type A2 **Start or reconfigure a system from the Main Control Room following procedures, with feedback.**	1E-3
Kirwan (p. 204)	Human Performance Limiting Values **Single operator carrying out task(s), less than optimum ergonomics**	1E-3
ATHEANA	Suggested calibration points for experts, e.g. **The operator(s) is “Unlikely” to fail.** The level of difficulty is quite low and we should not see any failures if all the crews/operators were to experience this scenario.	0.01

“Best” value for HEP ~ 0.01 Without crediting features to be documented in a detailed analysis of task, ergonomics, and performance conditions (V. Dang, PSI)

HEP and SIL

P(misconfiguration / adjustment) (human error probability)	**P (manual misconfigured TCDQ / fill*)** * all fills
0.01	**1E-3**
0.001	***1E-4***
0.0001	***1E-5***

Value to be compared to required SIL

Some factors that could reduce the human error probability

To be examined in a detailed analysis of the task, interface, and other performance conditions:

- **how desired manual settings are determined**
- the **information (input) used** to determine these settings
- **how the desired settings are entered** (e.g. absolute settings, absolute change, percent change, etc.)
- **system feedback**: how the operator may perceive the overall system response to the new settings and whether the new settings have the desired effect
- the **“aids”** (tables, etc.) that would support the operators in determining whether the desired settings are reasonable

- **technical interface / TCDQ features**
  - a) compare manually entered settings to previous values set by the MCS for the given LHC state or energy (i.e. current values before the adjustment),
  - b) automatic “sanity checks” for the entered settings, or
  - c) limit values, one-sided limit values?
- Administrative provisions for **independent checking and/or confirmation** of the settings

Conclusions

1. **"Risk assessment"** (IEC 61508) for ABD and consequences leads to the requirement that TCDQ must meet SIL 4.
2. **This safety analysis** assesses the expected unavailability of TCDQ (prob. of failure on demand). It does not review the SIL-related requirements on design, maintenance, and operation of the system.
3. **The probability of failure** is estimated to be 3.6E-5 for the two TCDQs (one per beam line). Two major assumptions underlying this value are:
   - MCS and timing system inputs to TCDQ are correct
   - The system is operated only in servo (automatic) mode with no manual adjust. of TCDQs.

   With these assumptions, the TCDQs satisfy **SIL 4**.
4. **The dominant contributions** to TCDQ unavailability are:

   1) failure of PLC timing card, 2) failure of PLC CPU control and supervision functions 3) failure of Ethernet to transit set points to PLC

   Note: all 3 dominant contributors appear to be single points of failure, based on the provided documentation.

Conclusions (cont.)

5. **Potential means** to address dominant contributors (tentative)

   a - acknowledge start signal and feedback status of TCDQ before injection

   b - PLC internal checks to prevent complete failure of controls and supervision

   c - ILK software to be checked at regular intervals

   Note: it may be that some of these means are already implemented.

6. **Manual adjustments** of TCDQ

   An analysis of the manual adjustment task, associated ergonomics, and performance conditions has not been performed. At this time, a “best” value for the probability of misconfiguration of the TCDQ is 0.01 per manual adjustment. This corresponds to 1E-3 per “demand” when the fractions of fills that include a manual adjustment phase is 1/10.

   Based on the conservative treatment of manual adjustment failures (all errors result in an unsafe configuration of TCDQ), the TCDQ would only satisfy SIL2.

   An analysis of the manual adjustment task, procedures, and performance conditions would be useful in order to identify the defenses currently in place and possible improvements.

Acknowledgement

Many thanks to **J. Uythoven** for the useful comments, **E. Carlier and C. Boucly** for their support in the system familiarization.

I am also grateful to **V. Dang** for the fruitful discussions during the preparation of this work

The END

SPARE SLIDES

Quantification and results:

Failure event importance analysis

#	FAILURE EVENT	Q	FV
1	TRACKING	2.20E-01	7.62E-01
2	PLC-TIMING-CARD	5.00E-05	6.05E-01
3	PLC-CPU-SW	5.00E-06	2.75E-01
4	HOLD	7.80E-01	2.38E-01
5	ETHERNET-BOARD	5.00E-06	6.06E-02
6	PLC-ILK-POS-THR1-SW	1.00E-03	2.16E-02
7	PLC-ILK-POS-THR2-SW	1.00E-03	2.16E-02
8	BLOCK FAILURE	5.00E-04	6.11E-03
9	PLC-ILK-BLOCKER-SW	1.00E-03	6.05E-03
10	NO-CAL-MOTOR	4.50E-04	5.50E-03
11	PLC-ILK-CAL-FILE-SW	1.00E-03	5.45E-03
12	DC-MOTOR1-CAL	4.05E-04	5.08E-03
13	DC-MOTOR2-CAL	4.05E-04	5.08E-03

Quantification and results:

Parameter Importance analysis

#	PARAMETER	time/q,rate		Sensitivity
1	CHECK CONTROL FUNCTION	Ti	1.00E+01	8.08E+01
2	GENERIC-HW	r	1.00E-05	1.42E+01
3	TRACKING	q	2.20E-01	1.18E+01
4	CPU-SW	r	1.00E-06	4.62E+00
5	ETHERNET	r	1.00E-06	1.64E+00
6	ILK-SW	q	1.00E-03	1.60E+00
7	HOLD POSITION	q	7.80E-01	1.36E+00
8	CAL-FILE	q	4.50E-04	1.17E+00
9	MD-FAILURE	r	1.00E-05	1.07E+00
10	BLOCKER	r	1.00E-04	1.06E+00
11	ANALOGUE-OUT	r	1.00E-05	1.06E+00
12	PID-FAILURE	r	1.00E-05	1.06E+00
13	TX-CPU-ANALOGUE	r	1.00E-05	1.06E+00
14	TX-ANALOGUE-MD	r	1.00E-05	1.06E+00
15	MOTOR-BLOCKER	Ti	1.00E+01	1.05E+00

Conclusions

Result for the default operation scenario

- The TCDQ system globally meets safety requirement,

  PFD is 3.6E-05, for 2 TCDQ systems, which is **SIL4**

Vulnerabilities

- TCDQ HW: failure of the TCDQ timing card and Ethernet communication with the MCS
- TCDQ SW: CPU failure at the application level with control and supervision function

Sensitivity to external contributions

- Missed start signal, correctness of position settings and human errors.
- The safety level of the TCDQ may drop to **SIL2** in case human error is included

Conclusions cont.

In the view of results the following recommendations are given:

1. **Review of failure data set that influence directly results**

   Analyze in detail most important contributors in particular the timing card and see if reliability statistics exist, how often are the cards replaced, etc.

2. **Design review**

   Modifications should go into the direction of covering the identified failure events, for example by removing or detecting them during a LHC run

   a - acknowledge start signal and feedback status of TCDQ before injection

   b - PLC internal checks to prevent complete failure of controls and supervision

   c - ILK software to be checked at regular intervals

3. **Additional investigations**

   Interface of TCDQ PLC to MCS and timing system

   Impact of human errors