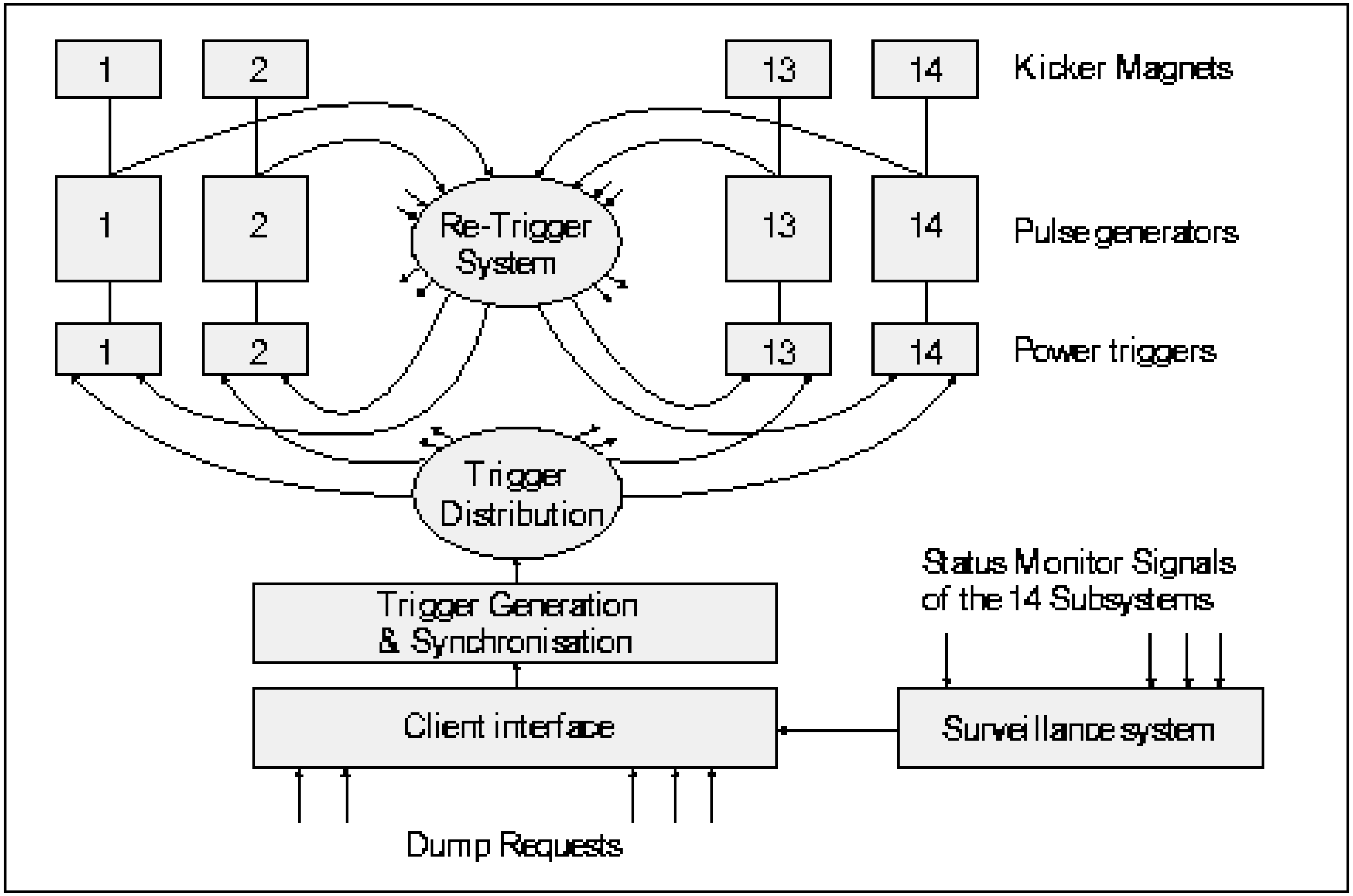
On the Reliability of the LHC Beam Dump Kicker Magnets ‘MKD’

How Reliable does it need to be ?

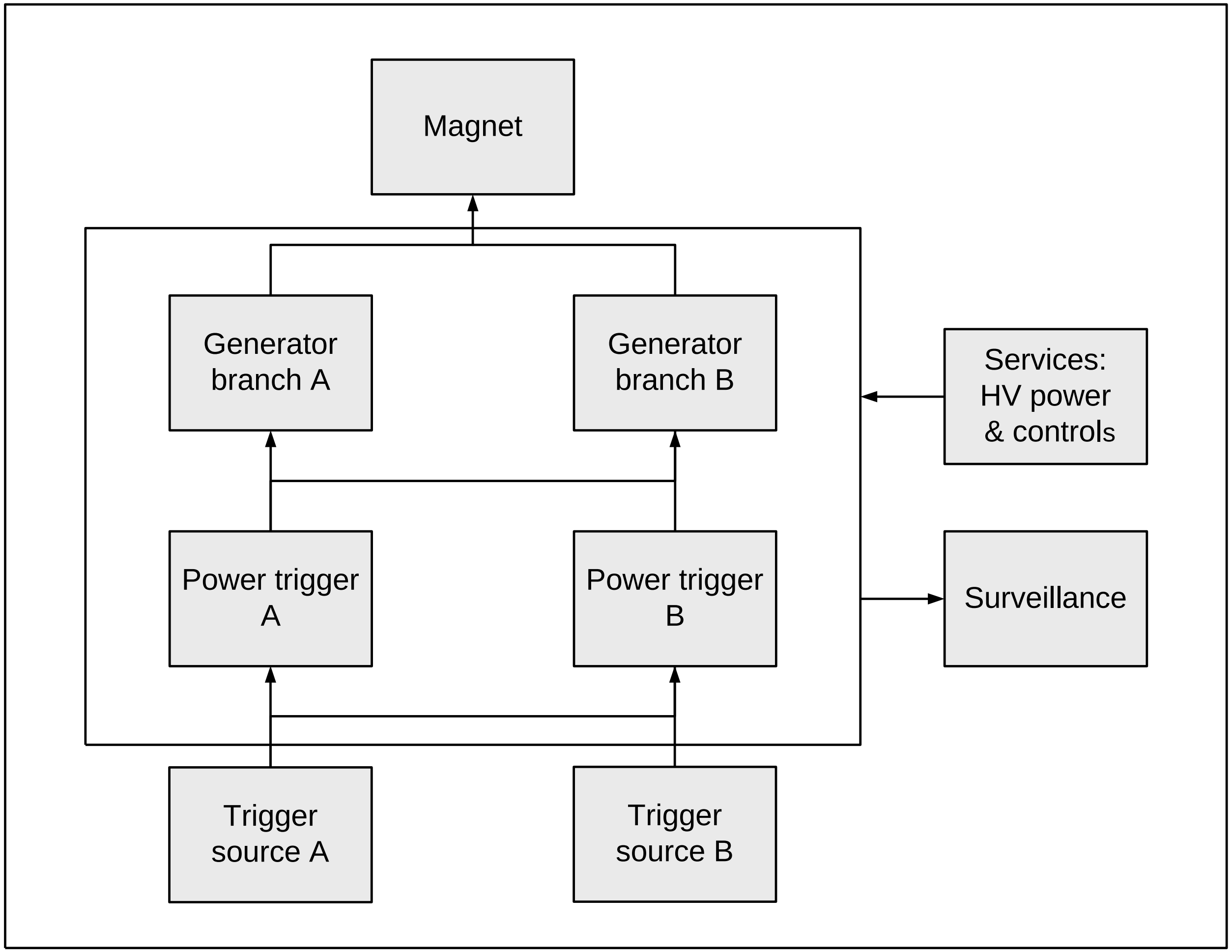
Johan Dieperink

12 April 2002

MKD System Layout



One Single Kicker System



Allocation of Safety Integrity Levels

- References used:
  - ‘Risk tables’ approved in AIWG of 8.11.2001:
    - Consequence Categories
    - Frequency Categories
    - SIL Matrix
  - Standard IEC 61508

Definition of a Hazardous Event

Dump request **issued by the LHC Access and**

Machine Protection Systems

AND / OR

Circulating beam in LHC

AND

Failure in the:

Beam Dump Kicker System

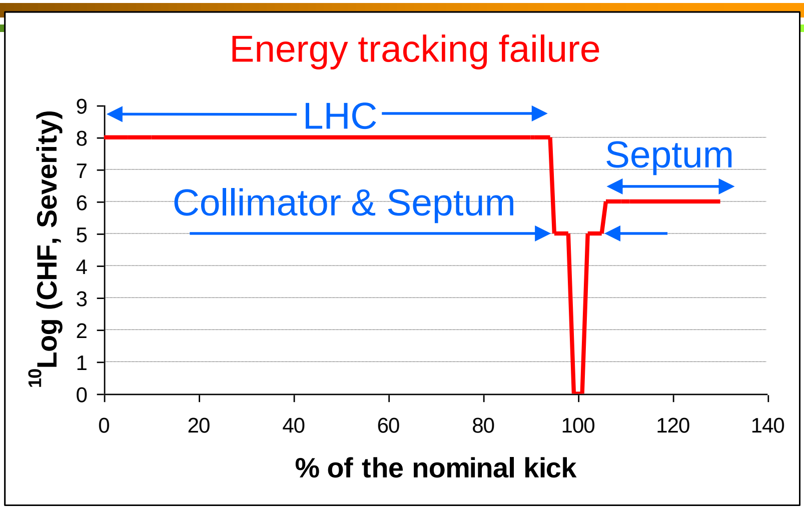
OR

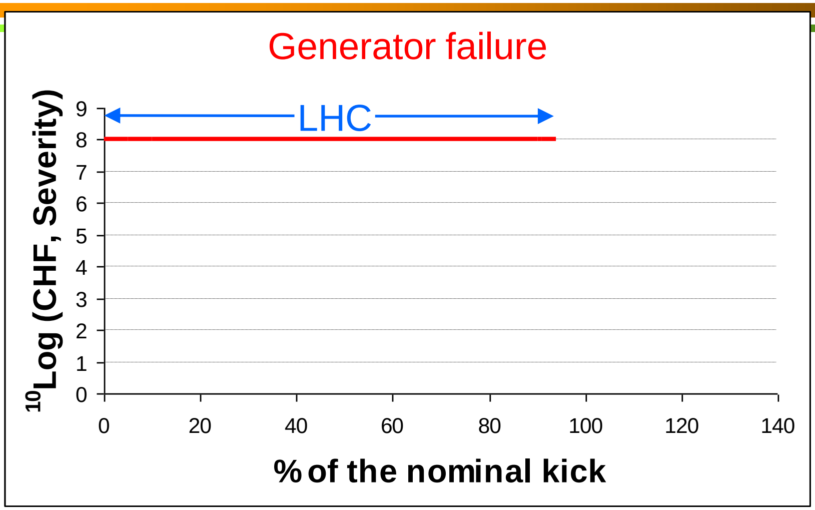
Information coming from BEM or RF

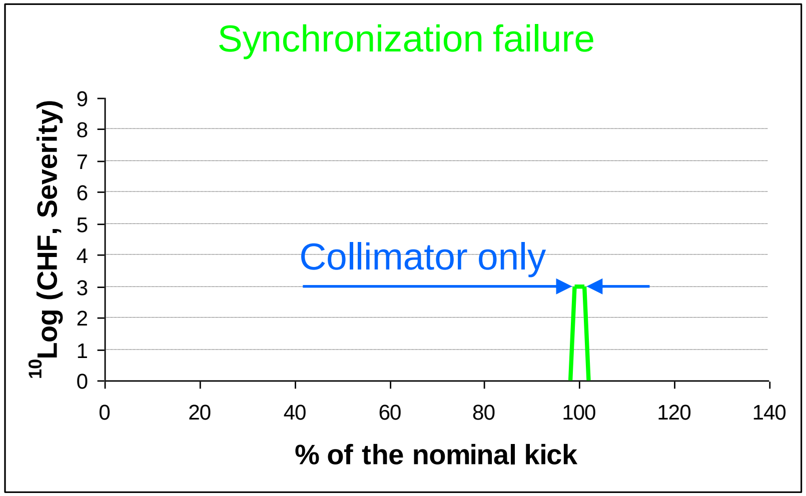
Possible Failures and Origin

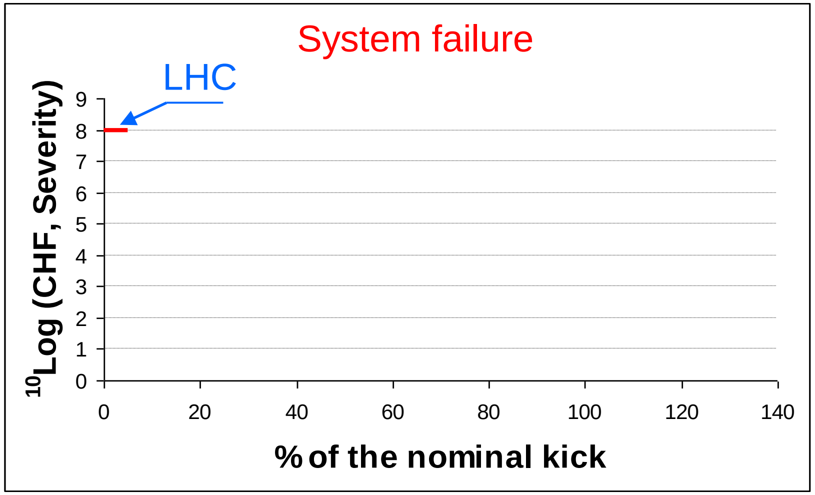
- **Energy tracking failure**
  - Energy tracking outside tolerance window **BEM, MKD**
    - Kick is too large
    - Kick is too small
- **Generator Failure**
  - Less than 14 pulse kickers respond **MKD**
- **System failure**
  - No response to a dump request **MKD**
- **Synchronization failure**
  - A spontaneously triggering of a kicker **MKD**
  - A drift or shift of the synchronization pulse train **RF, MKD**

Estimated damage caused by these failures


Energy tracking failure


Generator failure


Synchronization failure


System failure

System, Generator & Tracking Failures

Consequence

Category	**Injury to personnel**		**Damage to equipment**	
	Criteria	**N. fatalities (indicative)**	**CHF Loss**	**Downtime**
Catastrophic **Most likely**	Events capable of resulting in multiple fatalities	≥1	**> 5*10^{7}**	**> 6 months**
Major **Less likely**	Events capable of resulting in a fatality	0.1 (or 1 over 10 accidents)	**10^{6} – 5*10^{7}**	**20 days to 6 months**
Severe	Events which may lead to serious, but not fatal, injury	0.01 (or 1 over 100 accidents)	10^{5} – 10^{6}	3 to 20 days
Minor	Events which may lead to minor injuries	0.001 (or 1 over 1000 accidents)	0 – 10^{5}	< 3 days

Synchronization Failures

Consequence

Category	Injury to personnel		Damage to equipment	
	Criteria	N. fatalities (indicative)	CHF Loss	Downtime
Catastrophic	Events capable of resulting in multiple fatalities	≥1	**> $5*10^7$**	**> 6 months**
Major	Events capable of resulting in a fatality	0.1 (or 1 over 10 accidents)	**10^6 – $5*10^7$**	**20 days to 6 months**
Severe **Less likely**	Events which may lead to serious, but not fatal, injury	0.01 (or 1 over 100 accidents)	10^5 – 10^6	3 to 20 days
Minor **Most likely**	Events which may lead to minor injuries	0.001 (or 1 over 1000 accidents)	0 – 10^5	< 3 days

Frequencies of Initiating Events

- **Dump requests from**
  - Machine Protection **> 1000 / year → Frequent**
    - Emergencies
    - End of coast, MD, …
  - Access System **< 1 / year → Probably**
  - Surveillance of MKD itself **> 1 / year → Frequent**
- **Synchronization failure**
  - An erratic triggering of a kicker **> 1 / year → Frequent**

Safety Integrity Levels required

System, Generator and Tracking Failures

Synchronization Failures

Event Likelihood	Consequence			
	Catastrophic	Major	Severe	Minor
Frequent	**SIL 4**	**SIL 3**	**SIL 3**	**SIL 2**
Probable	**SIL 3**	**SIL 3**	**SIL 3**	**SIL 2**
Occasional	**SIL 3**	**SIL 3**	**SIL 2**	**SIL 1**
Remote	**SIL 3**	**SIL 2**	**SIL 2**	**SIL 1**
Improbable	**SIL 3**	**SIL 2**	**SIL 1**	**SIL 1**
Negligible / Not Credible	**SIL 2**	**SIL 1**	**SIL 1**	**SIL 1**

SIL definitions according to IEC 61508

Low demand
mode of operation

SIL	Average probability of failure to perform its design function on demand. (<1/year)
4	$10^{-5} < Pr < 10^{-4}$
3	$10^{-4} < Pr < 10^{-3}$
2	$10^{-3} < Pr < 10^{-2}$
1	$10^{-2} < Pr < 10^{-1}$

High demand /
continuous
mode of operation

SIL	Probability of a dangerous failure per hour
4	$10^{-9} < Pr < 10^{-8}$
3	$10^{-8} < Pr < 10^{-7}$
2	$10^{-7} < Pr < 10^{-6}$
1	$10^{-6} < Pr < 10^{-5}$

System, Generator and Tracking Failure Rate

Synchronization Failure Rate

What can fail in MKD ?

When does it fail ?

Operating phases of MKD

- Two phases
  - **READY-to-DUMP**
    - The phase between injection and dump request
    - Duration can be long → Up to 10 hours or more
  - **PULSING**
    - The phase starting with the dump request
    - Duration is short → 100 µs
- Both phases have their own particular failure behavior

Failures during **READY-to-DUMP**

- Have the consequence that:
  - One or more kickers are lost
    - These failures concern components like:
      - Low and high voltage power-supplies, surveillance system, tracking system, etc.
      - **Note**: The energy needed for pulsing is stored on capacitors in the pulse generator as well as in the power trigger modules.

        Thus, there is still some time to dump the beams !

Failures during **PULSING**

- Have the consequence that:
  - A kicker functions incorrectly.
    - These failures concern components, which become active during **PULSING** only, like:
      - Capacitors and GTO switches in pulse generator and trigger modules. They can be damaged due to high voltage or high current stress.

MKD has 3 clients

- Beam Interlock System
- LHC Access Safety System
- The MKD system itself
  - A failure detected during **READY-to-DUMP** requests immediately a dump. The probability that then all 15 kickers still function is large, but not guaranteed. During the following **PULSING** another kicker can fail.
  - Avoiding such a double failure needs a reliable operation of **14oo14** kicker systems.

Energy tracking failure

- Under study
  - Final solutions needed for:
    - Correction of the non-linearity of the pulse generators
    - Calibration of pulse generators
    - Calibration of magnets
  - Two feed-back loops are needed:
    - During **READY-to-DUMP** on the HV levels
    - After **PULSING** on the magnet currents, using Post-Mortem information
  - Must be very careful
    - Much software involved on different levels !

Pulse Generator failures

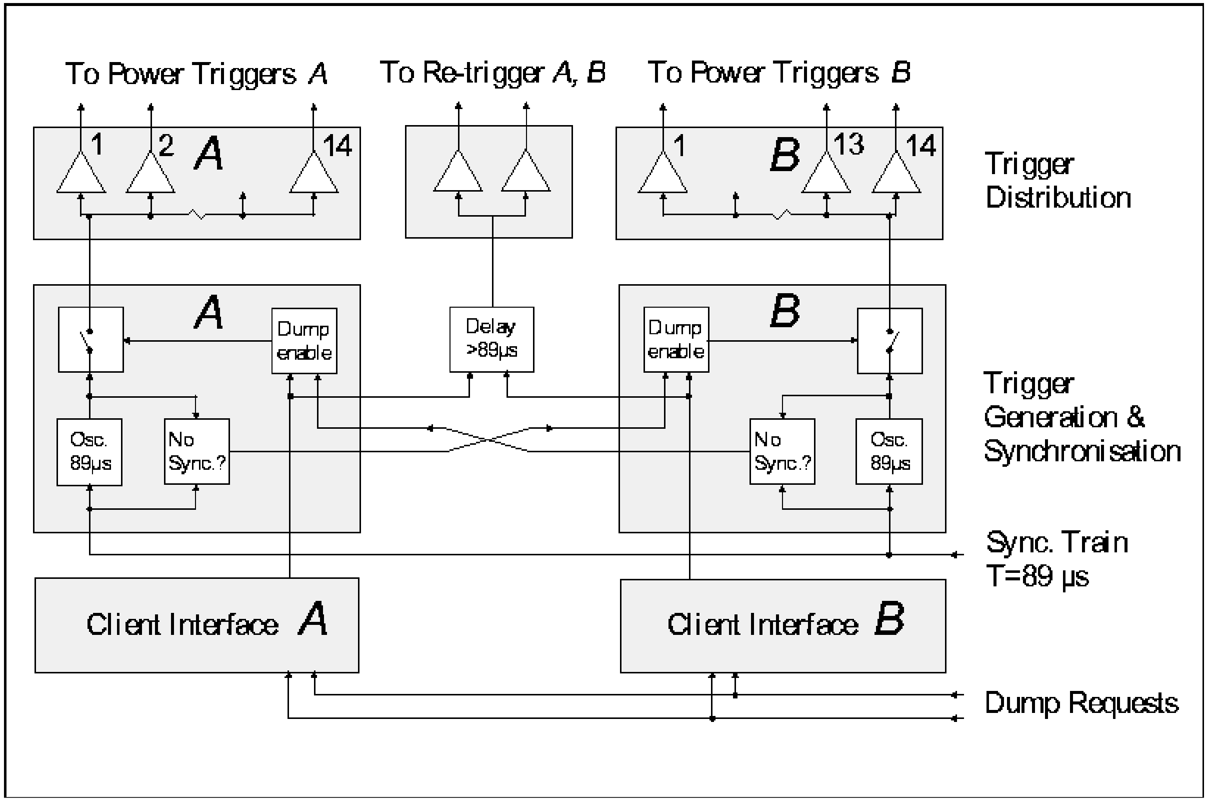
- Assumptions
  - Failure rates:
    - During **READY-to-DUMP**: 10^{-4} / h / kicker branch
    - During **PULSING**: 10^{-5} or 10^{-4} / h / kicker branch
  - External dump requests: ~ 1000 / y
  - Internal dump requests: 28 / y
    - Of which 25%, thus 7 / y, need 14oo14 pulse generators
  - Mission time: 10 h
  - Before each beam injection, thus when the mission begins, maintenance tests are made. The dump system is than “As good as new”.

Pulse Generator failures

Failure rate	Mission time	Unreliability (High demand)	
/ h	h	14oo15 / h	SIL
$1.0\ 10^{-4}$	10	$1.05\ 10^{-11}$	> 4
$3.16\ 10^{-5}$	10	$1.05\ 10^{-13}$	> 4
$1.0\ 10^{-5}$	10	$1.05\ 10^{-15}$	> 4

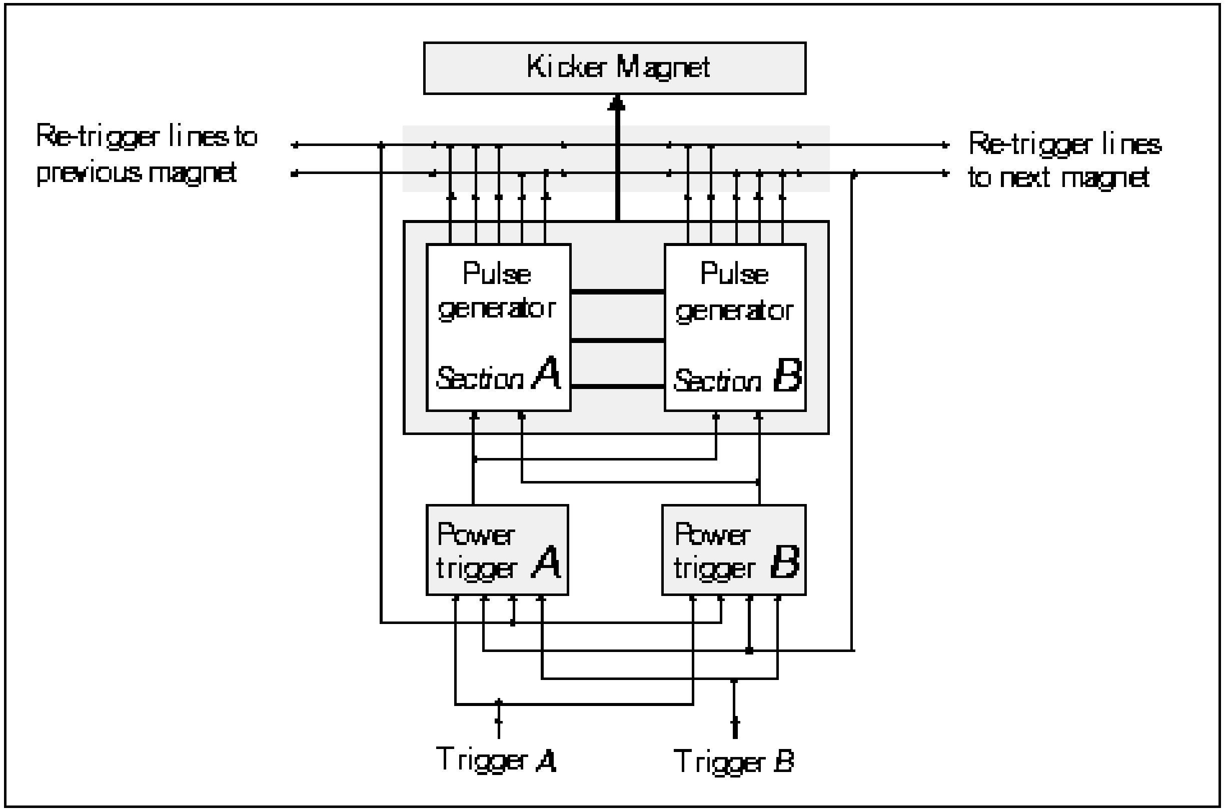
Failure rate	Mission time	Unreliability (High demand)		Unreliability (Low demand)	
/ h	h	14oo14 / h	SIL	14oo14	SIL
$1.0\ 10^{-4}$	10	$1.4\ 10^{-6}$	1	$1.4\ 10^{-5}$	4
$3.16\ 10^{-5}$	10	$1.4\ 10^{-7}$	2	$1.4\ 10^{-6}$	> 4
$1.0\ 10^{-5}$	10	$1.4\ 10^{-8}$	3	$1.4\ 10^{-7}$	> 4

Trigger Synchronization failures



- **1oo4** independent trigger channels can issue the dump trigger.
- **1oo2** ‘Trigger Generation & Synchronization’ systems can sync. the dump trigger.
- Both systems are independent.
- The mission time for tests is 89 µs.
- Expected SIL s 4

Re-trigger System failures


Kicker Magnet
Re-trigger lines to previous magnet
Re-trigger lines to next magnet
Pulse generator Section A
Pulse generator Section B
Power trigger A
Power trigger B
Trigger A
Trigger B

- Each branch has 5 re-trigger sources which feed 2 re-trigger distribution lines. Twice **1oo5.**
- Each source can deliver sufficient energy to trigger all power triggers of all magnets MKD/MKB.
- Continuity of re-trigger lines is continuously checked (pulse train).
- Expected SIL s 4

Conclusions

- Energy tracking failures are orders of magnitude more dangerous than synchronization failures
  - Preferred failure behavior: Kick too large
  - Tracking complicated due to non-linearity and calibrations
  - Still some work to do !
- Estimated Safety Integrity Levels

– External dump requests:	SIL r 4
– Internal dump requests:	SIL c 3 if > 1 / year
	SIL s 4 if < 1 / year
– Trigger and re-trigger systems:	SIL s 4
– Synchronization system:	SIL s 4

Question

- Which failure will be the first one ?

  - ❑ No detection of a dump condition
  - ❑ No response to a dump request
  - ❑ Dump request does not arrive
  - ❑ Kick too large
  - ❑ Kick too small
  - ❑ Simultaneous failure in 2 pulse generators