Project Status

A Failure Catalogue for the LHC

Sigrid Wagner, TE-MPE-PE
MPP, 24 February 2012

Thanks to:
Markus Zerlauth, Rudiger Schmidt, Benjamin Todd, Jan Uythoven, Ivan Romera Ramirez

Motivation

- The MPS was designed considering a large number of possible failures of LHC equipment

- The knowledge of these failures and of the machine protection functions implemented to cover these failures is distributed over the different teams involved in the design and operation of the LHC

→ Project aims at bringing together this knowledge in a common failure catalogue.

Motivation

Goal

A failure catalogue for the LHC

- what can go wrong?
- (how) are we protected against it?

Problem

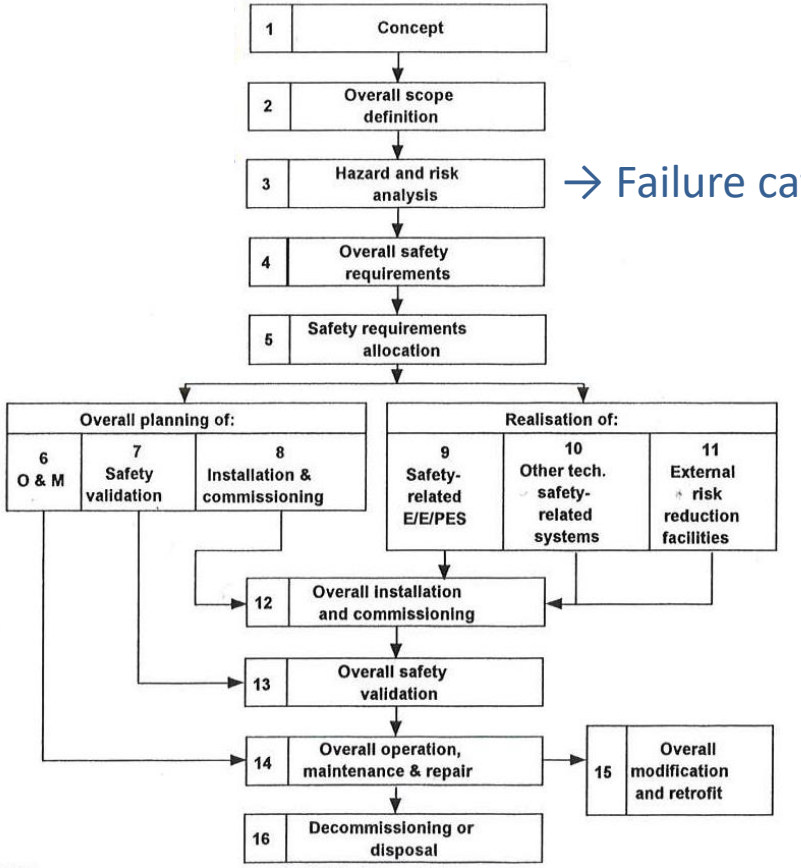
- Multitude of possible failures
- Stand-alone failure catalogue does not mean much, lots of extra information required
  - Description of systems (machine and MPS) and operation
  - Argument on approach
  - References on evidence
  - …

→ How to handle the data? How to bring together the information in a structured way, and in which format?

IEC 61508 Safety Lifecycle

Safety lifecycle

'A model for **structuring** safety management **activities** throughout the life cycle of safety- related systems' [1]



→ Failure catalogue

Safety Case

Safety Case
Documentation ‘ to go to court with’ [1]

containing

- claim
- argument
- evidence

Claim ‘The LHC is safe for operation under given conditions’ or ‘LHC operation is safe’

Argument: what the claim is based on

Evidence based on
- Testing
- Simulation
- Calculation
- Statistics
- Reviews
- …

→ Failure catalogue as a means to support the claim

1 Concept: Machine Protection in Context

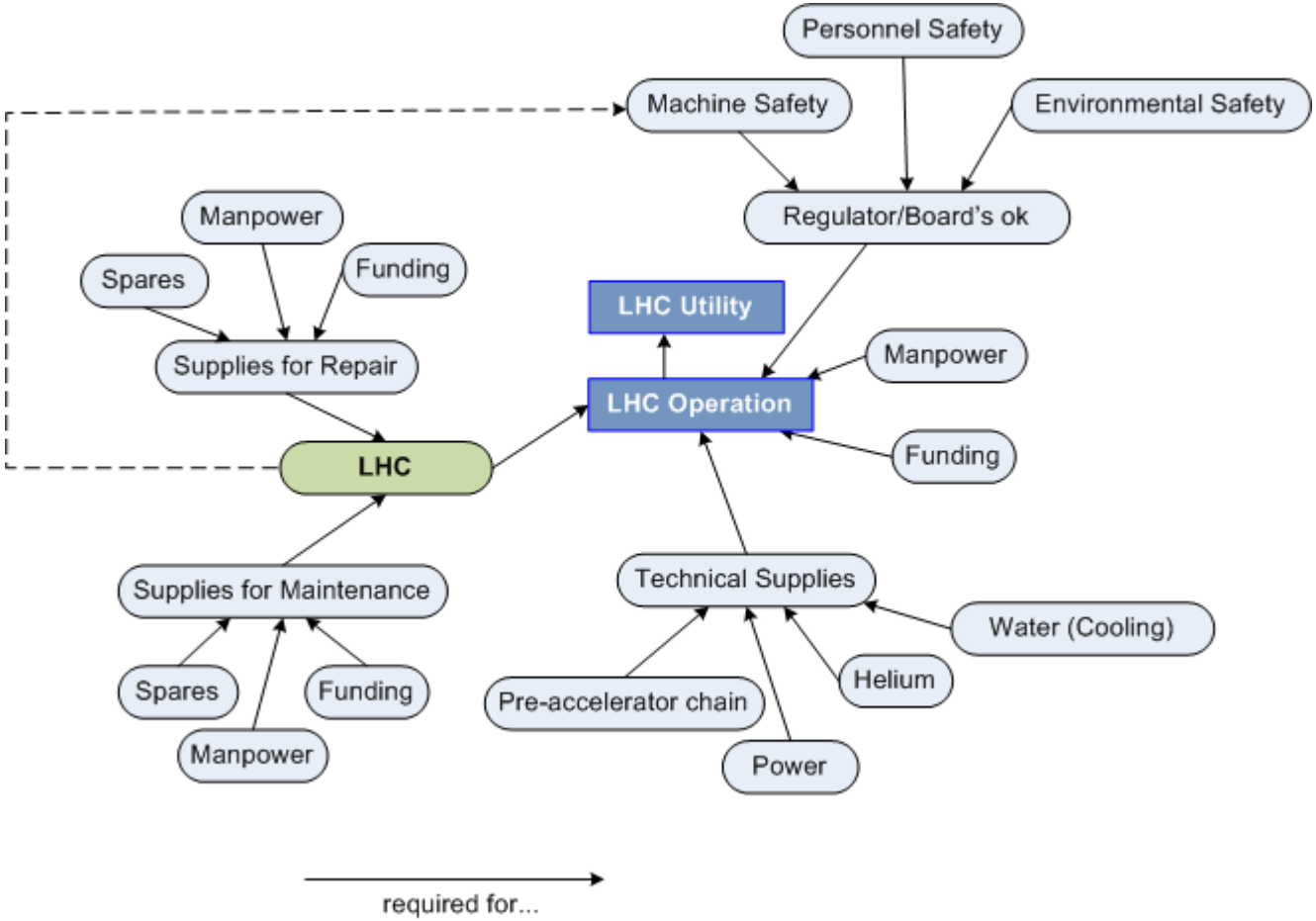


Fig.1 Requirements for LHC Operation (non-exhaustive)

Utility New discoveries in the field of particle physics

2 Scope definition: System boundaries

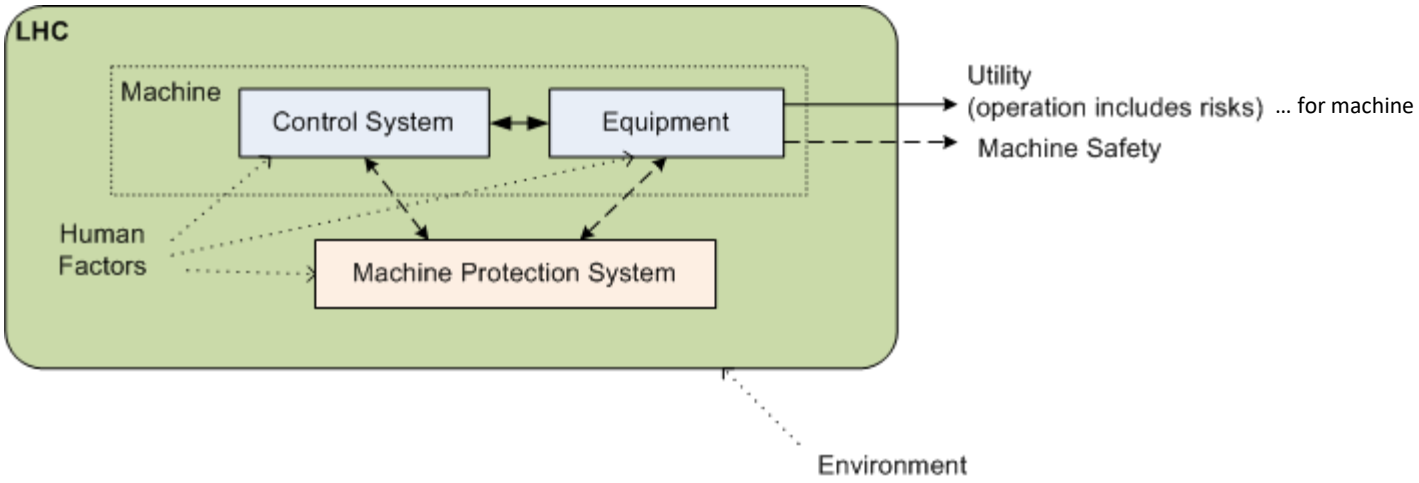


Fig. 2 Interrelation Machine and Machine Protection System (adapted from [1])

Utility New discoveries in the field of particle physics

Machine

Function

- Accelerator: Provide colliding beams in conditions required by experiments
- Experiments: Collect data on particles emerging from collisions

Risk for machine Damage, worst case: beyond repair

Note: equivalent consideration for personnel/environmental safety (Fig.1-2)

3 Hazard and Risk Analysis: Deduce Hazard Chains

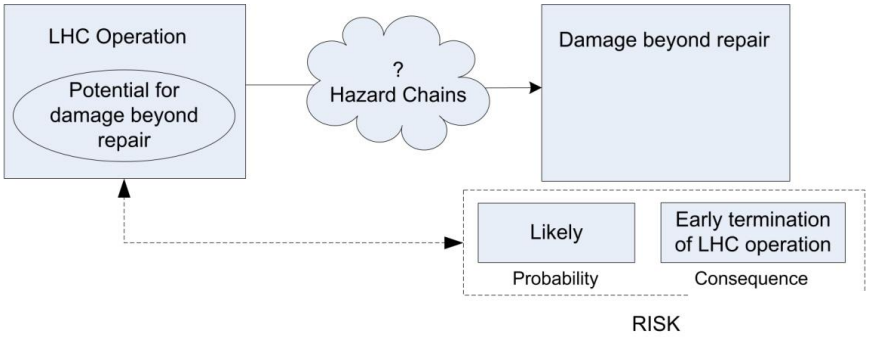
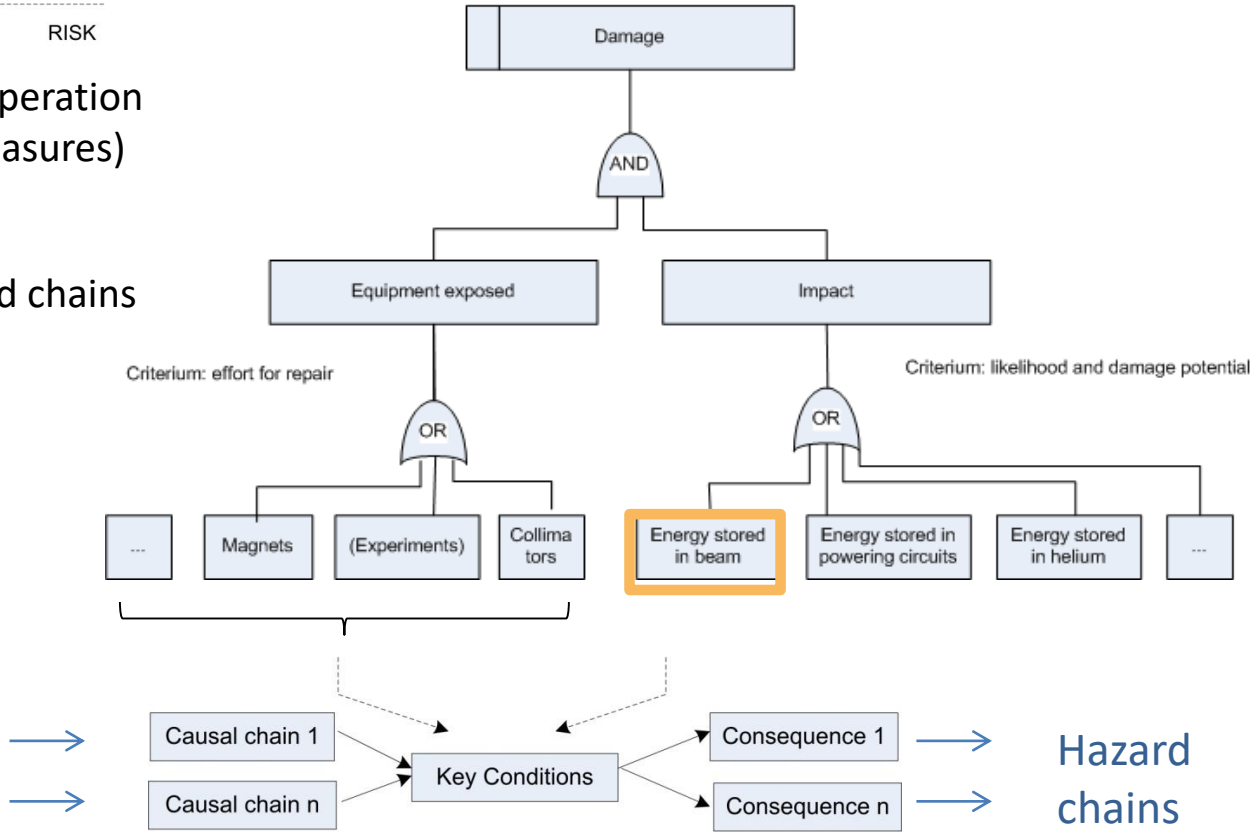


Fig.3: Risk associated with LHC operation (without machine protection measures)

Fig.4: Approach to deduce hazard chains



3 Hazard and Risk Analysis > 4 Protection requirements

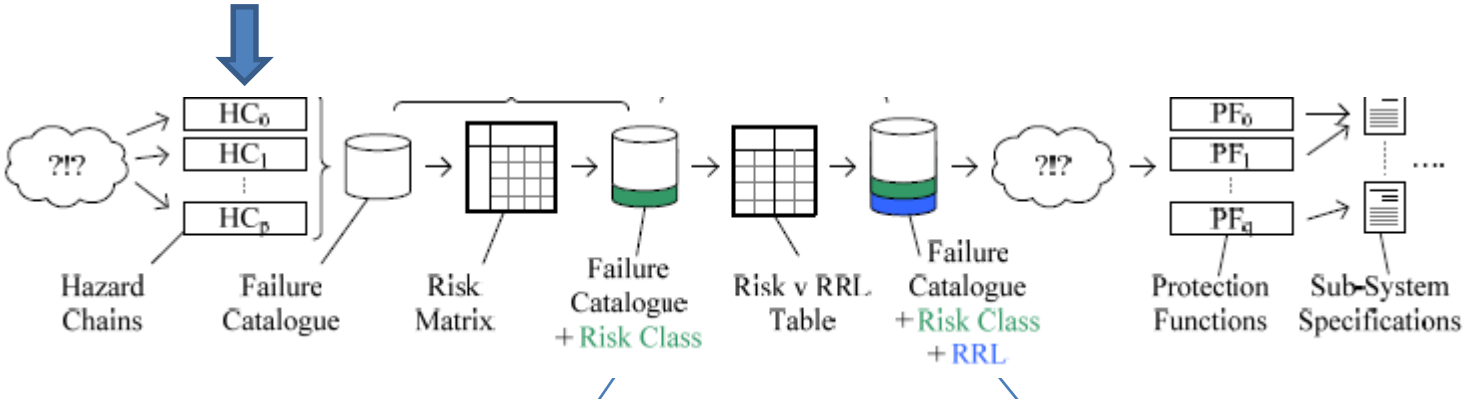
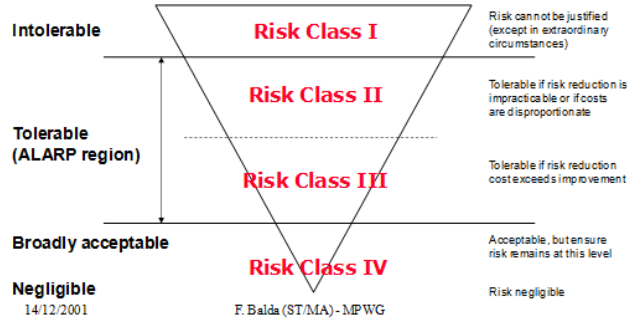


Fig.5: Proceeding in lifecycle from hazard chains to definition of protection functions [2]

Frequency	Consequence			
	Catastrophic	Major	Severe	Minor
Frequent	I	I	I	II
Probable	I	I	II	III
Occasional	I	II	III	III
Remote	II	II	III	IV
Improbable	II	III	IV	IV
Negligible / Not Credible	III	IV	IV	IV



Closer look at Hazard Chain: Example

Equipment: equipment around beam path
Impact: Energy stored in beam
Key condition: Beam energy release in equipment

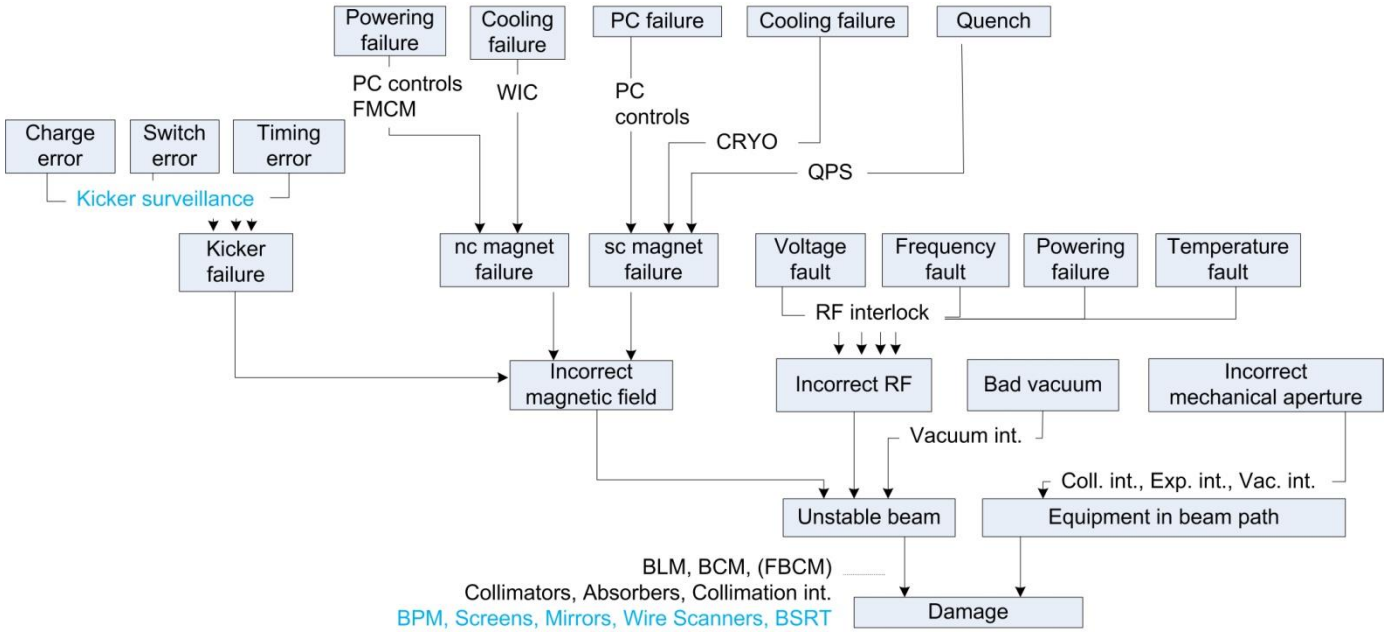


Fig.6: General hazard chain for beam-induced damage (not exhaustive)

Closer look at Failure Catalogue: Status quo

OP	BEAM	EQUIPM.		CONSEQUEN. (Unprot.)						DETAIL	MEASURES			CONSEQU.
		Comp.	Failure	Beam loss		Location		Level			Prevention	Protect. active	Protection passive	
			Angle	opt	pess	opt	pess	opt	pess		Sys/com.	Sys/com	Sys/com	
(1) SPS beam opera-tion	Protons, 450 GeV, nominal	Bumper H(4): common, grouped	Too small (for extr.)	None (will continue circulation in SPS)	All beam lost as not sufficiently kicked for extrraction but lost elsewhere in the SPS	none	MSE/SPS Vacuum chamber	none	2..3 (higher for first magnets in the chain, less for last ones)		Bumper current surveill.	-	SPS coll	
			Too big (for extr.)	Might touch the MSE/vacuum chamber	Lost on MSE	none	MSE/SPS Vacuum chamber	none	2..3 (higher for first magnets in the chain, less for last ones		Bumper current surveill.	-	SPS coll	

Consequences, damage levels:
1: possibly damage beyond repair
2: serious damage, repair expected to take many months(19/9/08)
3: damage, repair expected to take days to weeks

Closer look at Failure Catalogue: Status quo

OP	BEAM	EQUIPM.		CONSEQ (Unprot.)						DETAIL	MEAS.			C
		Comp.	Failure	Beam loss		Loc.		Level			Prevent.	Prot. active	Prot. passive	
			Angle	opt	pess	opt	pess	opt	pess		Sys/com.	Sys/com	Sys/com	
(4) Extr. to TED.8 (TI8)	Protons, 450 GeV, nominal	Bumper H(4): common, grouped												
		MKE(5): Kicker, grouped	Too Small (T0, deltaT: nom.)	None (still remains in SPS chamber)	Entire beam lost	None	MSE, transfer lines or SPS	none	Vacuum chamber or 1-2 magnets damaged: 2..3 (higher for first magnets in chain, less for last ones)	Kicker flashover	Inject./ Extract. kicker surveill.		SPS coll (e.g. absorber in front of septum), transfer line coll	
			Too Big (T0, deltaT: nom.)	None (still remains in SPS chamber)	Entire beam lost	none	(MKE), MSE, transfer line	none	Vacuum chamber or 1-2 magnets damaged, more likely damage of MSE: 2..3 (higher for first magnets in chain, less for last ones		Inject./ Extract. kicker surveill.		Transfer line coll	
		MSE(6): common, grouped	Too Small	None (still remains in TI8 chamber)	Entire beam lost (see TT40 incident in fall 2004)	None	(MSE), transfer line or SPS	None	Vacuum chamber or 1-2 magnets damaged: 2..3 (higher for first magnets in chain, less for last ones)	Powering failure Comment: no spares for MSE!	PCS, FMCM		SPS and transfer line coll.	
			Too Big	None (still remains in TI8 chamber)	Entire beam lost	none	(MSE), transfer line	none	Vacuum chamber or 1-2 magnets damaged, more likely damage of MSE: 2..3 (higher for first magnets in chain, less for last ones)	Powering failure	PCS, FMCM		Transfer line coll	
		MBSG(8): common, grouped	Too big	None (still remains in TI8 chamber)	Entire beam lost	none	MBSG, TI8, CNGS line, CNGS target?	none	Vacuum chamber or 1-2 magnets damaged: 2..3 (higher for first magnets in chain, less for last ones)	Powering failure Comment: MBSG powered	PCS, FMCM		Transferline coll, CNGS coll	

Conclusion: Hazard chains/Failure catalogue

- Compiling the hazard chains/failure catalogue requires profound expert knowledge and accuracy (only then useful)
- If done in a systematic way, patterns appear allowing to ultimately boil the catalogue down to the essentials
- Takes time and staying power

Status quo

- Under development
- Approach defined, exemplified by general hazard chain and partial failure catalogue INJECTION

As for the format…

- **Report?**
  - Tedious to compile
  - Not maintainable

- **Website!**
  - Allows for piece-by-piece compiling
  - Easy to maintain
  - Interactive
  - Fun to work with

Conclusion: Website

Claim 'The LHC is safe for operation under given conditions' or 'LHC operation is safe'

- To collect the relevant information and evidence or provide links to it
- To put the failure catalogue into context
- To provide an overview on the Machine Protection activities, structured according to IEC 61508 safety lifecycle
- To be understood as a means for a safety case

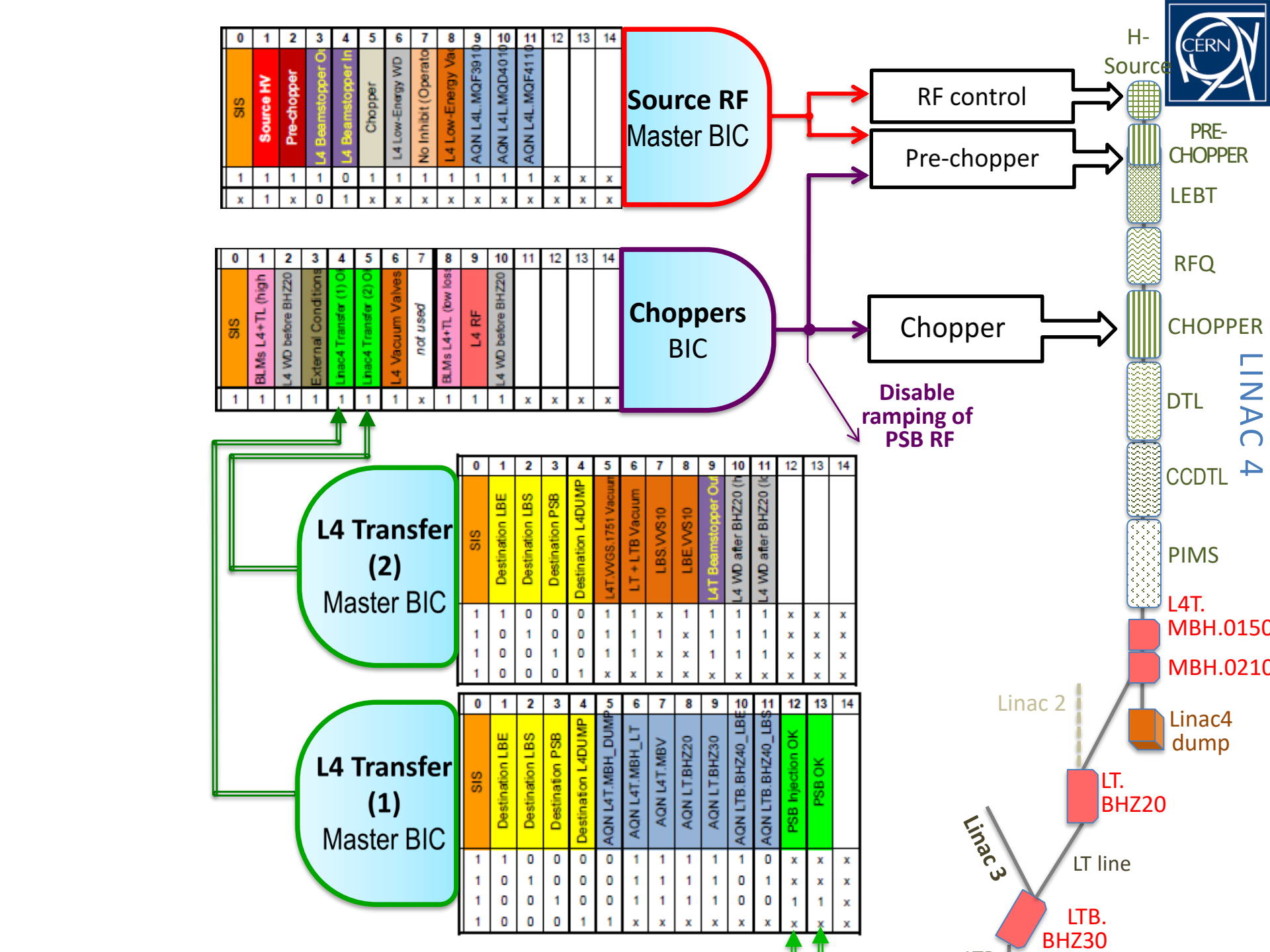
Status quo

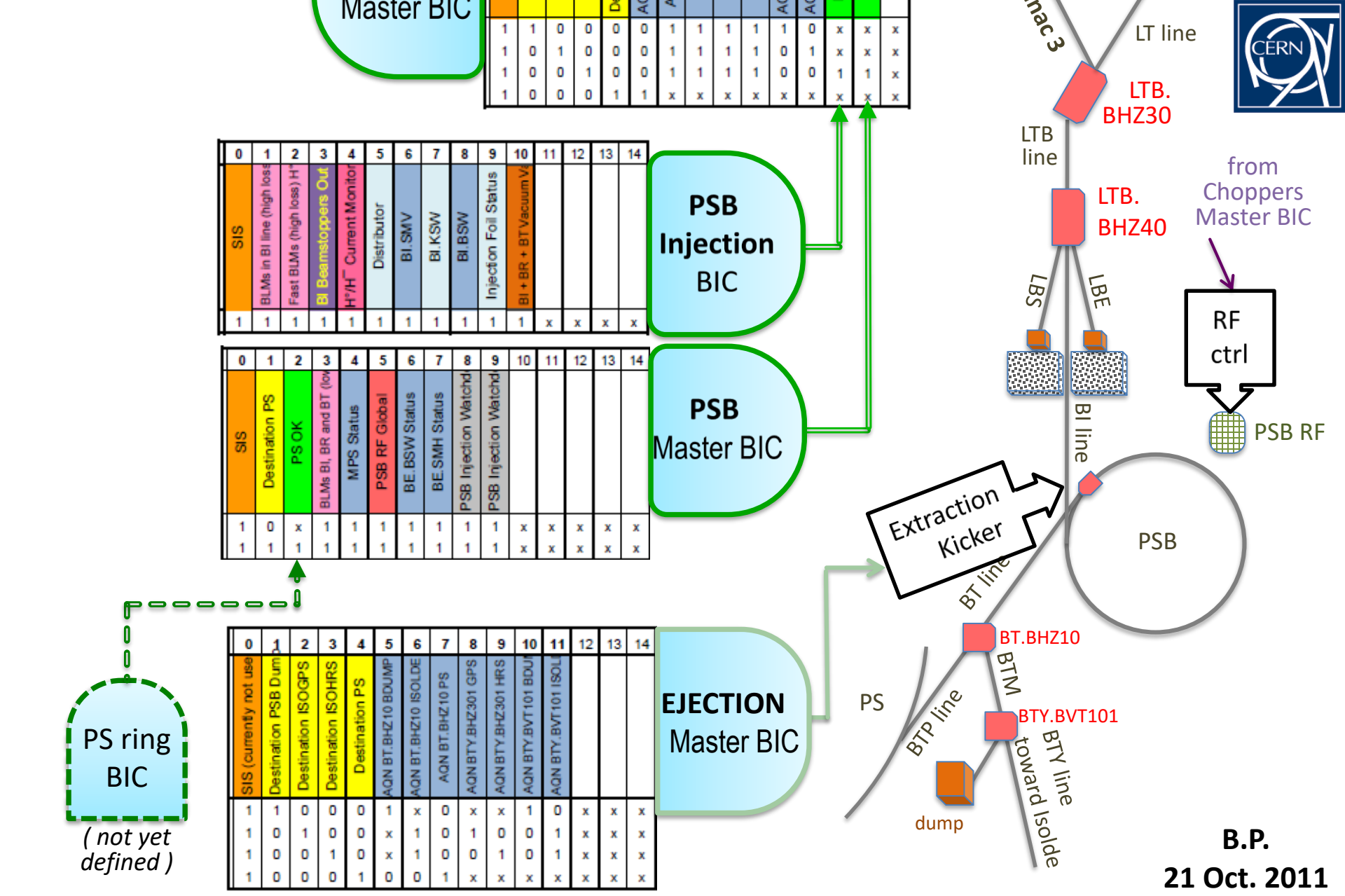
- Under development: https://espace.cern.ch/lhc-and-machine-protection/
- Being tested by means of PIC documentation
- Possibly used as guidance for a risk assessment project on LINAC4

Outlook: Risk assessment project on LINAC4

To provide a proof of concept of the approach on a smaller scale system

- Function of the equipment
- Failure modes of the equipment
- Consequences of failures
- Assess coverage of failures/consequences through the proposed interlock truth tables


0 1 2 3 4 5 6 7 8 9 10 11 12 13 14
SIS
Source HV
Pre-chopper
L4 Beamstopper Ou
L4 Beamstopper In
Chopper
L4 Low-Energy WD
No Inhibit (Operato
L4 Low-Energy Va
AQN L4L.MQF3910
AQN L4L.MQD4010
AQN L4L.MQF4110
1 1 1 1 0 1 1 1 1 1 1 1 x x x
x 1 x 0 1 x x x x x x x x x x
Source RF
Master BIC
RF control
Pre-chopper
0 1 2 3 4 5 6 7 8 9 10 11 12 13 14
SIS
BLMs L4+TL (high
L4 WD before BHZ20
External Conditions
Linac4 Transfer (1) O
Linac4 Transfer (2) O
L4 Vacuum Valves
not used
BLMs L4+TL (low los
L4 RF
L4 WD before BHZ20
1 1 1 1 1 1 1 x 1 1 1 x x x x
Choppers
BIC
Chopper
Disable
ramping of
PSB RF
0 1 2 3 4 5 6 7 8 9 10 11 12 13 14
SIS
Destination LBE
Destination LBS
Destination PSB
Destination L4DUMP
L4T.VVGS.1751 Vacuum
LT + LTB Vacuum
LBS.VVS10
LBE.VVS10
L4T Beamstopper Ou
L4 WD after BHZ20 (h
L4 WD after BHZ20 (k
1 1 0 0 0 1 1 x 1 1 1 1 x x x
1 0 1 0 0 1 1 1 x 1 1 1 x x x
1 0 0 1 0 1 1 x x 1 1 1 x x x
1 0 0 0 1 x x x x x x x x x x
L4 Transfer
(2)
Master BIC
0 1 2 3 4 5 6 7 8 9 10 11 12 13 14
SIS
Destination LBE
Destination LBS
Destinaton PSB
Destinaton L4DUMP
AQN L4T.MBH_DUMP
AQN L4T.MBH_LT
AQN L4T.MBV
AQN LT.BHZ20
AQN LT.BHZ30
AQN LTB.BHZ40_LBE
AQN LTB.BHZ40_LBS
PSB Injection OK
PSB OK
1 1 0 0 0 0 1 1 1 1 1 0 x x x
1 0 1 0 0 0 1 1 1 1 0 1 x x x
1 0 0 1 0 0 1 1 1 1 0 0 1 1 x
1 0 0 0 1 1 x x x x x x x x x
L4 Transfer
(1)
Master BIC
H-
Source
PRE-
CHOPPER
LEBT
RFQ
CHOPPER
DTL
CCDTL
PIMS
LINAC 4
L4T.
MBH.0150
MBH.0210
Linac4
dump
Linac 2
LT.
BHZ20
LT line
Linac 3
LTB.
BHZ30



Linac4/TL/PSB Beam Interlock System layout

References

[1] Felix Redmill, 2011: Workshop on System Safety Principles, CERN

[2] B. Todd et al. Machine Protection of the Large Hadron Collider, 6th IET International System Safety Conference 2011, Birmingham, UK

[3] S. Wagner et al., A Failure Catalogue for the LHC, Proceedings of IPAC 2011, San Sebastian, Spain

Thank you for your attention!