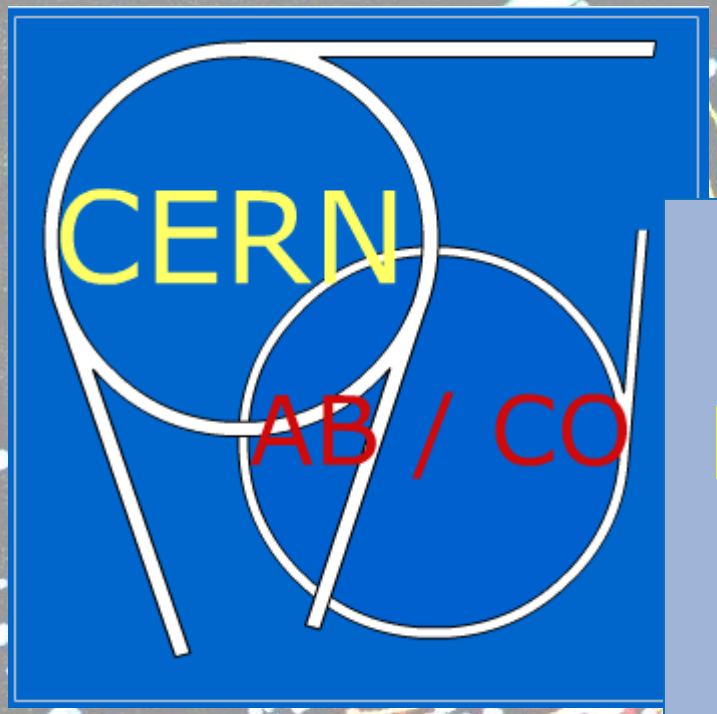
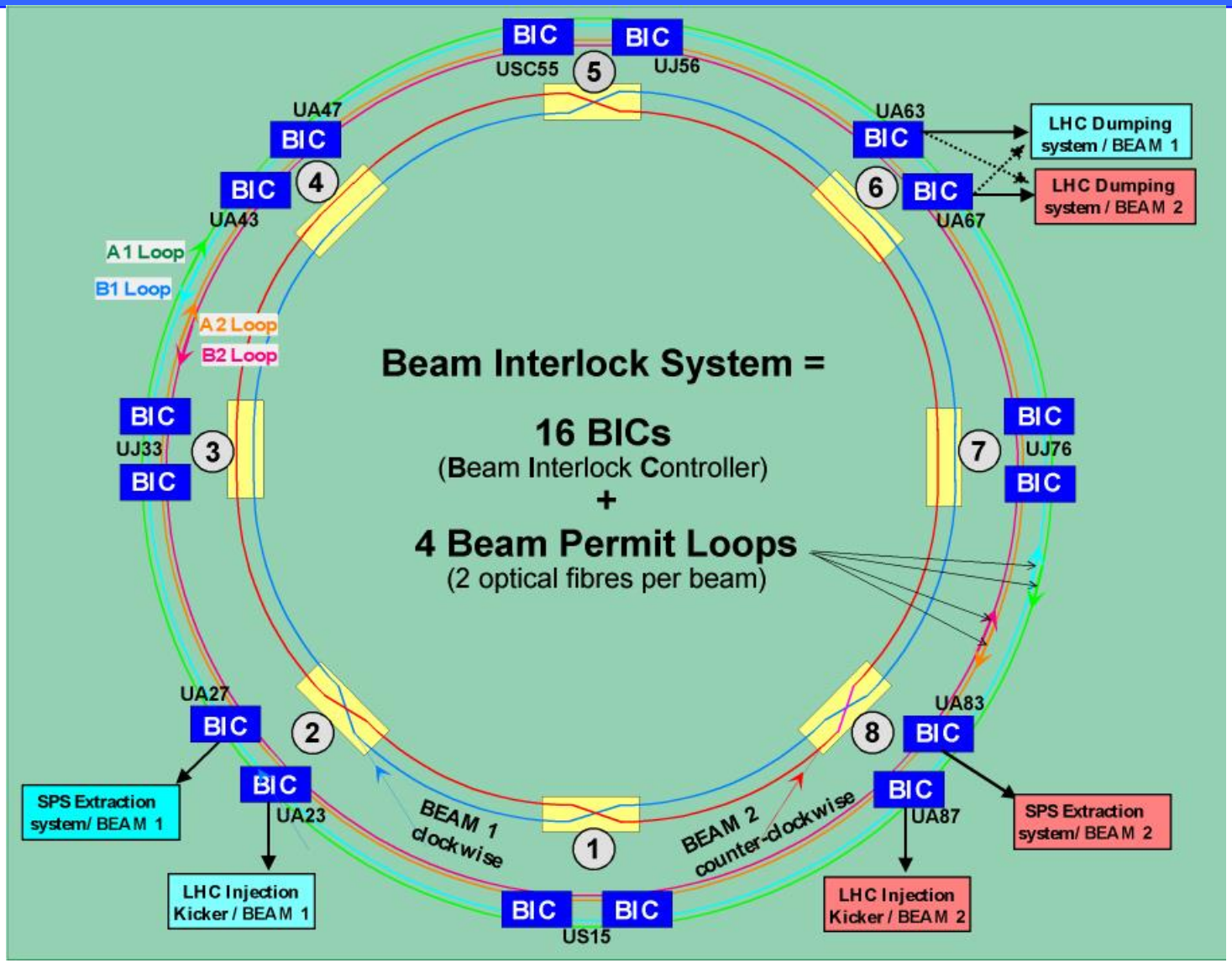


Beam Interlock System Dependability

BT MPWG – 18th March 2005

Reminder


BIC
USC55
5
UJ56
UA47
UA63
LHC Dumping system / BEAM 1
LHC Dumping system / BEAM 2
4
6
UA43
UA67
A1 Loop
B1 Loop
A2 Loop
B2 Loop
Beam Interlock System =
16 BICs
(Beam Interlock Controller)
+
4 Beam Permit Loops
(2 optical fibres per beam)
UJ33
3
7
UJ76
UA27
UA83
2
8
SPS Extraction system/ BEAM 1
UA23
BEAM 1 clockwise
BEAM 2 counter-clockwise
UA87
SPS Extraction system/ BEAM 2
LHC Injection Kicker / BEAM 1
1
LHC Injection Kicker / BEAM 2
US15

On the Agenda…

1. Failure Mode, Effect and Criticality Analysis
   - Background

2. FMECA Results
   - Beam Interlock System User Box Only (CIBU)
   - VME PSU Redundancy effects

3. Conclusions, Concerns and Questions!
   - Conclusions
   - Concerns
   - Questions

FMECA

Failure **M**odes, **E**ffects and **C**riticality **A**nalysis

In what way can something go wrong?…

…when it does go wrong, what happens to the system?…

…and just how much of a problem does this cause?

How is it done?

MIL-STD-1629

FMECA starts at the Component Level of a system

Break a large system into blocks, defining smaller, manageable sub-systems

⇩

get subsystem schematics, component list, and understand what it does

MIL-HDBK-338 ⇩ MIL-HDBK-217

get MTBF of each component on the list, derive P_{FAIL}(mission)

MIL-HDBK-338 ⇩ FMD-97

derive failure modes and failure mode ratios for each component

⇩

explain the effect of each failure mode on both the subsystem and system

⇩

determine the probability of each failure mode happening. Draw conclusions!

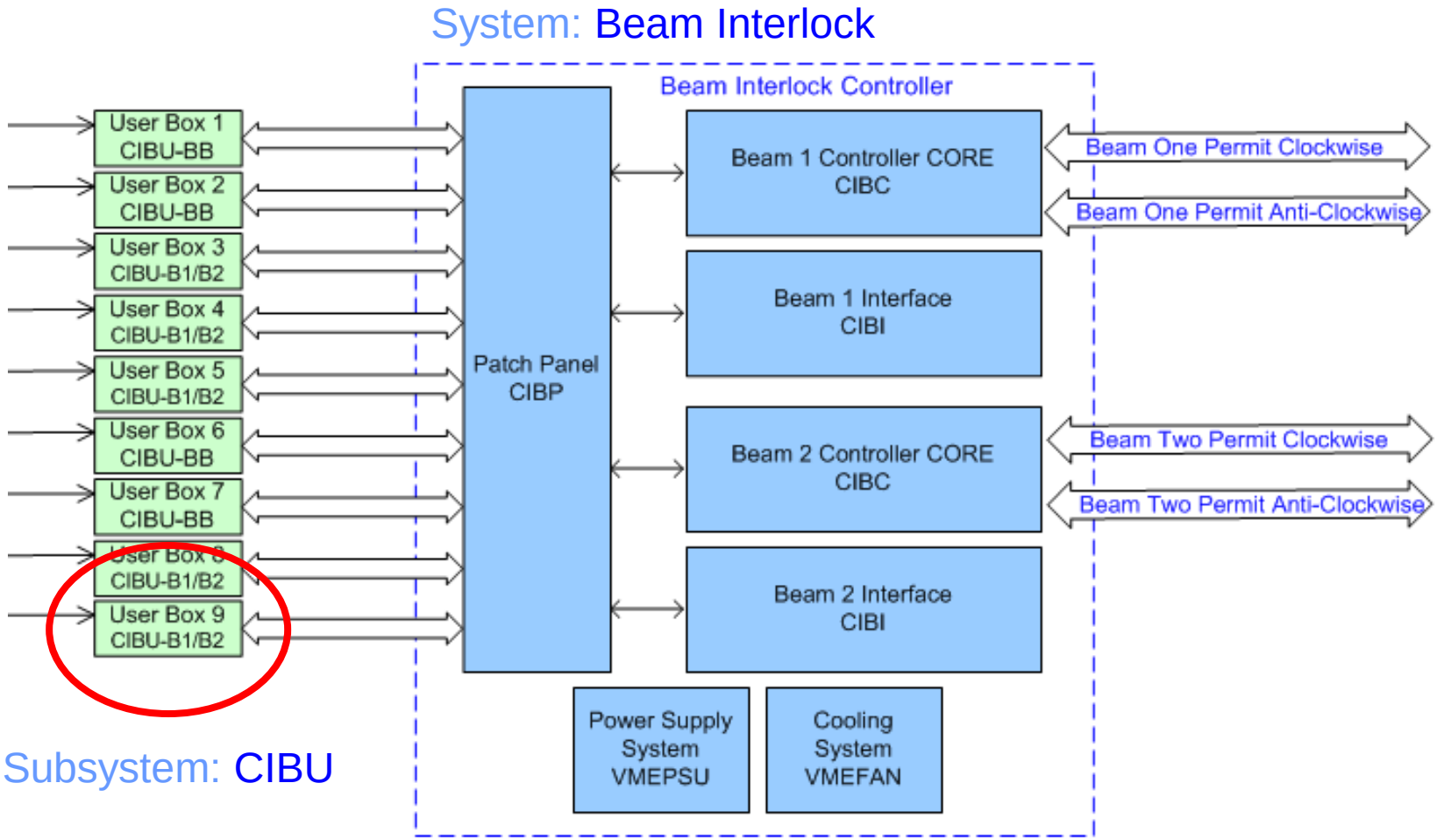
Applying the Method to the CIBU

1. Failure Mode, Effect and Criticality Analysis
   - Background

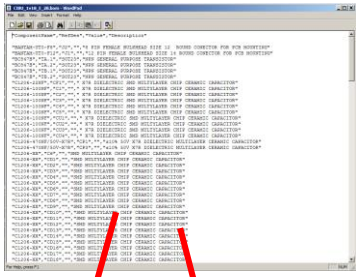
2. FMECA Results
   - Beam Interlock System User Box Only (CIBU)
   - VME PSU Redundancy effects

3. Conclusions, Concerns and Questions!
   - Conclusions
   - Concerns
   - Questions

Block Diagram



Applying the Methodology 1/2



Bill of Materials

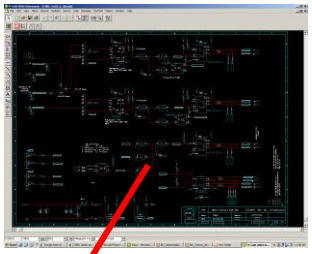
	A	B	C	D	E	F	G
1	**Failure Mode Effect and Criticality Analysis**						
2							
3	**CERN: European Organisation for Nuclear Research**						
4							
5	CRITICALITY WORK SHEET		**System:**	BEAM INTERLOCK SYSTEM			**Sub System:**
6							
7	**Part ID**	**Part Description**	**Base**	**Reference**	**Failure Mode**	**Failure Mode**	**Reference**
8			**Failure Rate**	**BFR**		**Frequency Ratio**	**FMFR**
9	*(schematic RefDes)*		*(/10^9h)*		*(FMD-97)*	*(FMD-97)*	
10							
11	J1	*Burndy F12*	3.9	MIL-HBDK-271F-15-(1-2-3)	*Open BF*	0.000	FMD 97-2-47/NE12 Cable FM
12			*3.9*		*Open BD*	0.060	
13			*3.9*		*Open M*	0.090	
14			*3.9*		*Open NE*	0.241	
15			*3.9*		*Intermittant Operation*	0.552	
16			*3.9*		*Shorted BF*	0.000	
17			*3.9*		*Shorted BD*	0.006	
18			*3.9*		*Shorted M*	0.008	
19			*3.9*		*Shorted NE*	0.043	

MIL-HDBK-217F
or manufacturer

FMD-97

MIL-HDBK-338

Applying the Methodology 2/2



Schematic

H	I	J	K	L	M	N	O
			Criticality of system for: Blind Failures, Beam Dumps, Maintenance and No Effect				
					AB/CO/IN	**Benjamin TODD**	
CIBU			**Version:**	1v0		**Date:**	28.1.05
Failure Mode Effect Analysis *(BF, BD, M, NE)*	**Failure Mode Effect Description**	**Detection Method (BD automatic)**	**P(Fail) During Mission** *(CIBU)*	**P(Blind Fail) Permit A** *(Permit Loop A)*	**P(Blind Fail) Permit B** *(Permit Loop B)*	**P(Fail) Beam Dump** *(CIBU)*	**P(Fail) Maintenance** *(CIBU)*
BF	Permit A/B Fail Blind	Monitoring/Test	0.00E+00	0	0	0	0
BD	Permit A/B break	Monitoring/Test	2.35E-09	0	0	2.346E-09	0
M	Command/Response Fail	Monitoring/Test	3.52E-09	0	0	0	3.519E-09
NE	No Effect	None	9.38E-09	0	0	0	0
BD	Permit A/B break	Monitoring/Test	2.15E-08	0	0	2.1528E-08	0
BF	Permit A/B Fail Blind	Monitoring/Test	0.00E+00	0	0	0	0
BD	Permit A/B break	Monitoring/Test	2.28E-10	0	0	2.28E-10	0
M	Command/Response Fail	Monitoring/Test	3.14E-10	0	0	0	3.135E-10
NE	No Effect	None	1.68E-09	0	0	0	0

multiply through

Designer Knowledge

MIL-HDBK-338

So…

1. Failure Mode, Effect and Criticality Analysis
   - Background

2. FMECA Results
   - Beam Interlock System User Box Only (CIBU)
   - VME PSU Redundancy effects

3. Conclusions, Concerns and Questions!
   - Conclusions
   - Concerns
   - Questions

Numbers

75 Simultaneous Beam Dump CIBU
39 Independent Beam Dump CIBU
10 Hour LHC mission
400 Missions per year

	CIBU B1&B2 or Half CIBU B1/B2	ALL LHC	One Year ALL LHC
P(Fail) Any Failure	3.82E-05	5.84E-03	2.34
P(Fail) Blind A Failure	4.91E-07	7.51E-05	3.00E-02
P(Fail) Blind B Failure	4.91E-07	7.51E-05	3.00E-02
P(Fail) Blind A&B Failure	2.41E-13	3.68E-11	1.47E-08
P(Fail) Beam Dump	7.82E-06	1.20E-03	0.48
P(Fail) Maintenance	2.01E-05	3.07E-03	1.23

During one year it's probable that for all CIBUs

2-3 will fail in one way or another
0-1 will fail without having any impact on the system
0-1 will fail during a mission causing a Beam Dump, and requesting Maintenance
1-2 will fail only requesting Maintenance at the end of the current mission
3.00E-02 is Probability of a single channel failing blind
1.47E-08 is Probability of a both channels failing blind in the same CIBU

SIL 3

Variations on the Dependability

BIS as it is (75% analysed)

	COMBINED AND AJUSTED TOTALS		
	BIS One Mission	BIS One Year	Safety Integrity Level IEC61508
P(Fail) Any Failure	1.84E-02	7.378	
P(Fail) Blind Failure	3.68E-11	1.473E-08	SIL 3
P(Fail) Beam Dump	3.42E-03	1.368	
P(Fail) Maintenance	1.35E-02	5.419	
Maintance OR Beam Dump	1.70E-02	6.787	

Remove All Redundancy…

	COMBINED AND AJUSTED TOTALS	NO REDUNDANCY	
	BIS One Mission	BIS One Year	Safety Integrity Level IEC61508
P(Fail) Blind Failure	7.51E-05	3.003E-02	< SIL 1

Remove User Input Redundancy…

	COMBINED AND AJUSTED TOTALS	NO USER REDUNDANCY	
	BIS One Mission	BIS One Year	Safety Integrity Level IEC61508
P(Fail) Blind Failure	3.08E-06	1.230E-03	< SIL 1

Add Redundant VME PSU…

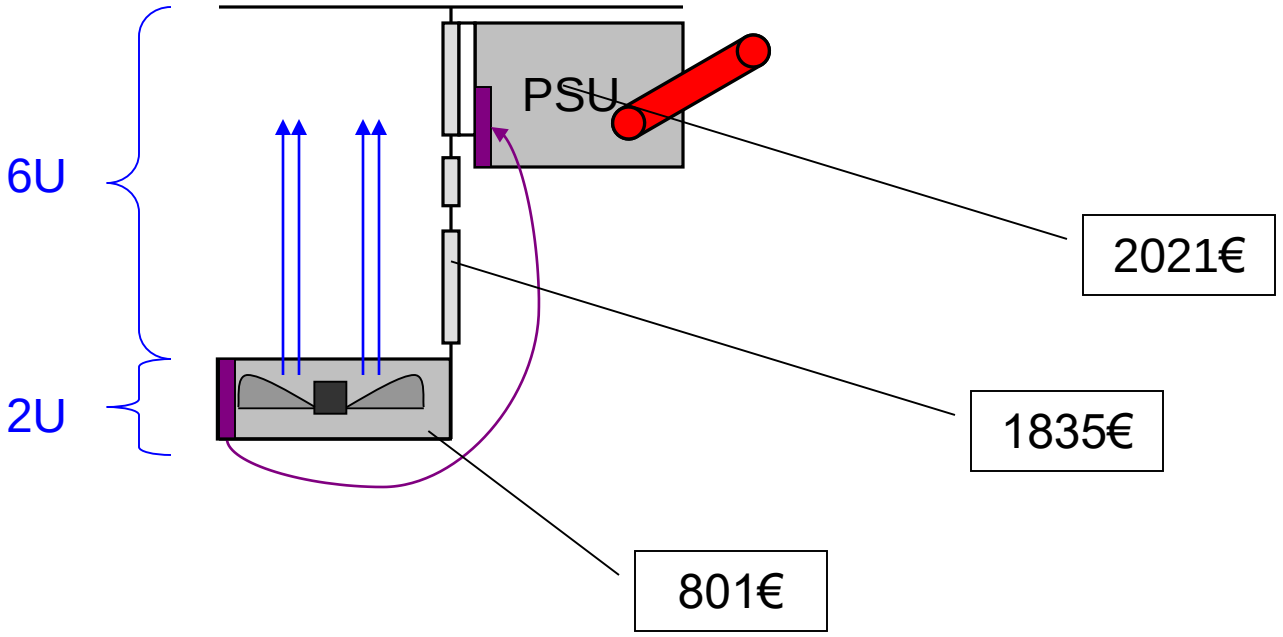
	COMBINED AND AJUSTED TOTALS		
	BIS One Mission	BIS One Year	Safety Integrity Level IEC61508
P(Fail) Any Failure	2.00E-02	8.017	
P(Fail) Blind Failure	3.68E-11	1.473E-08	SIL 3
P(Fail) Beam Dump	1.82E-03	0.729	
P(Fail) Maintenance	1.67E-02	6.698	
Maintance OR Beam Dump	1.86E-02	7.427	

Redundant VME PSU

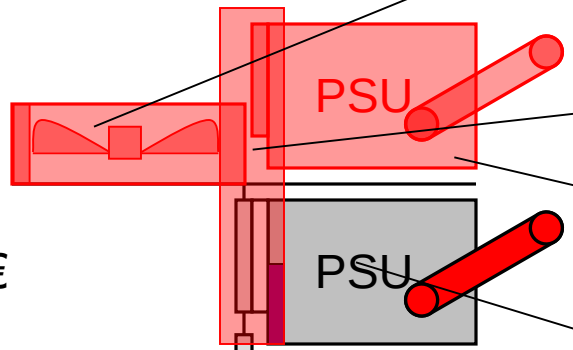
As discussed with Wiener, and Elcotron!

Standard VME Chassis CERN
AB CO 8U

4657€ TOTAL



Redundant VME PSU



New Standard VME Chassis
CERN AB CO 11U

3U

NON-REDUNDANT = 4657€

PREPARED* = 5107€

FULLY-REDUNDANT* = 7929€

801€

450€

2021€

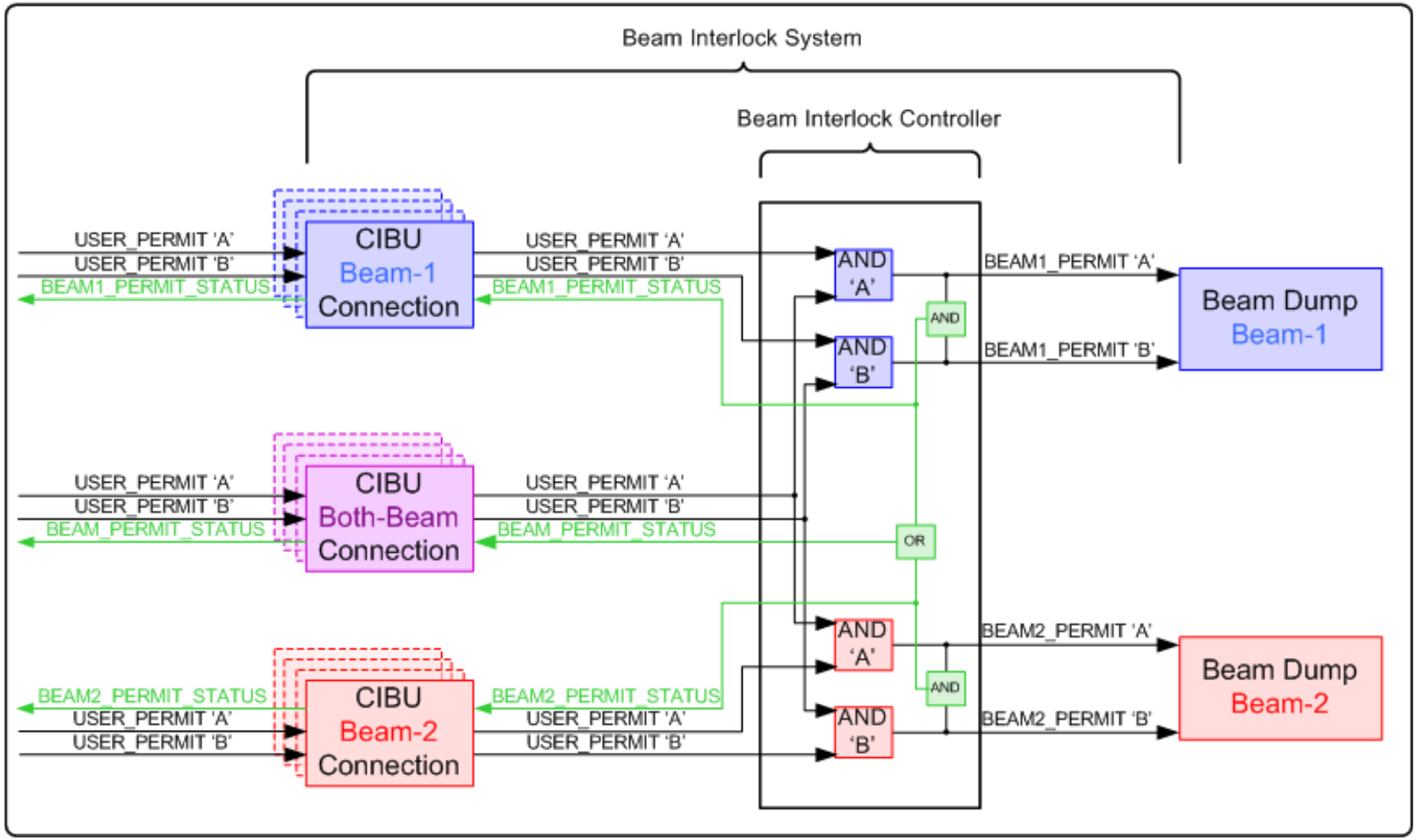
2021€

1835€

801€

*No, I'm not earning commission…

N.B. Beam Permit Status 1/2



N.B. Beam Permit Status 2/2

- BEAM PERMIT STATUS failure rate
  - Around 0.1% chance of failure in a year for only the CIBU
  - This will definitely get worse as the rest of the system is analysed
- Dependability Motivations
  - Described in Engineering Specification as SIL 2..
  - Not very simple to Test
    (Engineering Specification dictates Permit A and Permit B cannot be asserted simultaneously)
  - Making it SIL2 is going to mean an almost complete redesign of the distribution of this signal
  - Redundancy is necessary!
  - ‘As Good As New’ will no longer apply to the system after testing
  - **AAARRRGGH!!**

Conclusions

- SAFETY
  - Results are excellent for Communications from User to BIS
  - Numbers for BIS safety are converging on SIL 3
    (CIBU accounts for most probable common mode failures)
- AVAILABILITY
  - Results for False Beam Dumps are OK
  - Spend a little money now and if VME PSU becomes an issue $$$ will fix it
- MAINTAINABILITY
  - From the FMECA it's relatively simple to derive the Maintainability of the system… Just have to calculate the repair times…
    - On my list of things to do

Concerns and Questions…

- Beam Permit Status:
  - Do I really need to make this SIL 2?
  - What is it being used for?
  - Can we not use the SLP for this signal?
- From the User Systems:
  - To get SIL 3 we need a redundant input.
  - Users shouldn't wire this together.
  - Can Users accommodate this?
- VME PSUs 11U Redundant:
  - Anyone else interested??
  - I'll keep anyone who's interested up to date…

FIN