IEC61508 at ISIS

Bob Mannix (Controls Group)

Alan Stevens (Accelerator Operations Group)

Science & Technology Facilities Council
ISIS

Harwell Oxford Campus

The IEC61508 standard

Functional Safety of Electrical/Electronic/Programmable Electronic Safety-related Systems

- A basic standard for Functional Safety that generates others but that can be used alone
- It may need interpretation for particular applications
- 7 volumes, a lot of paperwork and a dose of (apparently) slightly arbitrary calculation

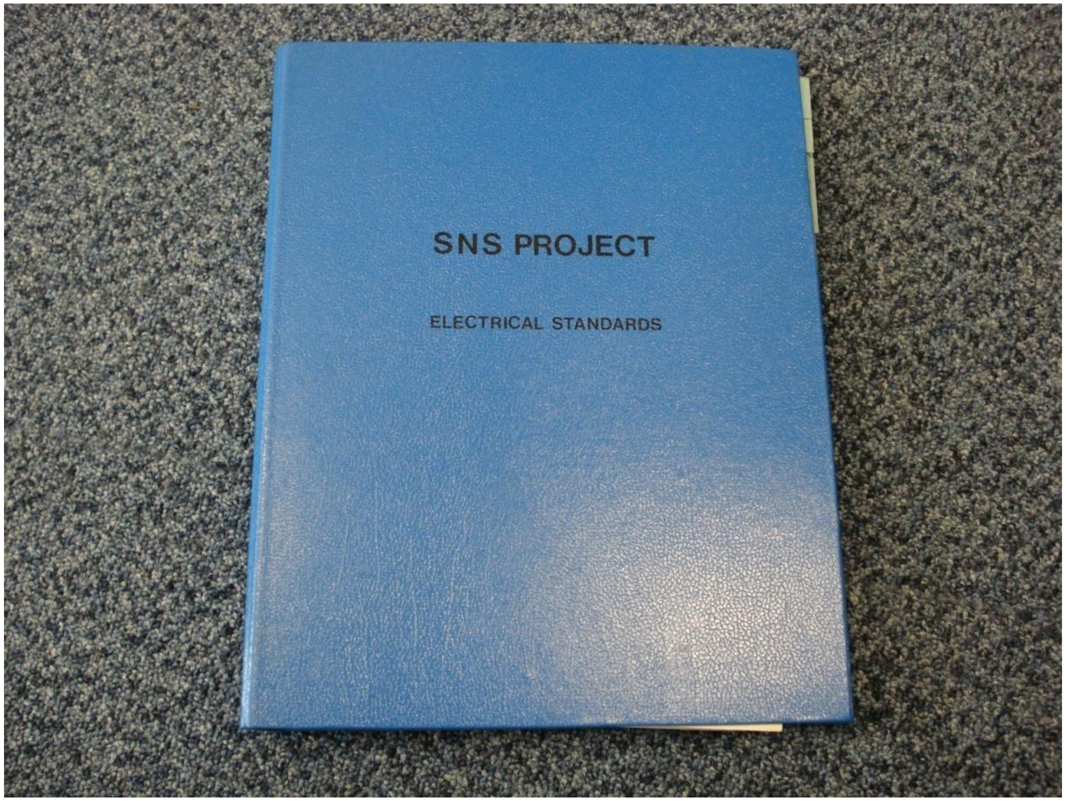
Why would anyone use 61508?!

- The UK Health and Safety Executive have the power to close us down on a single visit
- "In the context of functional safety, HSE recognises …61508 and relevant sector standards (E.g. …61511) as reference standards for determining whether a reasonably practicable level of safety has been achieved.“
- NOT a legal requirement in the UK but regarded as best practice/something to match
- Maybe coming down your hallway soon!

Historical context

- ISIS was constructed from 1978 to 1984, first neutrons being delivered in Dec 1984
- Parts of the machine and the infrastructure date back to the 1960’s
- By 2000 we had a 48V relay based interlock “system” which no-one understood. Changes were ad-hoc and there was little testing but no incidents caused by its failure
- Upgrading to two-target operation meant a large extension of the interlock system
- Decision to use 61508/Functional Safety Analysis to build a new personnel and beam protection system (PPS/BPS). Target Station 2 instruments followed a similar path – “Best practice”

Lets return to the 1980's and look up our standards for interlocks...



Oh cr*p....

Functional Safety Analysis/61508- things you have to get to grips with

- Acceptable death/injury rate, where safety systems are challenged, due to the risk of failure of those systems
- Frequently challenged systems (failure rate) and rarely challenged systems (probability of single failure)
- Safety Integrity Level required of a system to meet the acceptable death/injury rates
- Full lifecycle analysis – no “fit and forget”

How many can your process kill?

- Not really different to previous standards in the Nuclear industry
- For the public 10^{-5} per year from the protected risk
- For employees 10^{-4} per year from the protected risk
- The likelihood of death (or serious injury) if the safety system fails, the frequency of challenge to the system, and the above figures, allow a maximum failure on demand of the system to be calculated and, from this the Safety Integrity Level required for the system

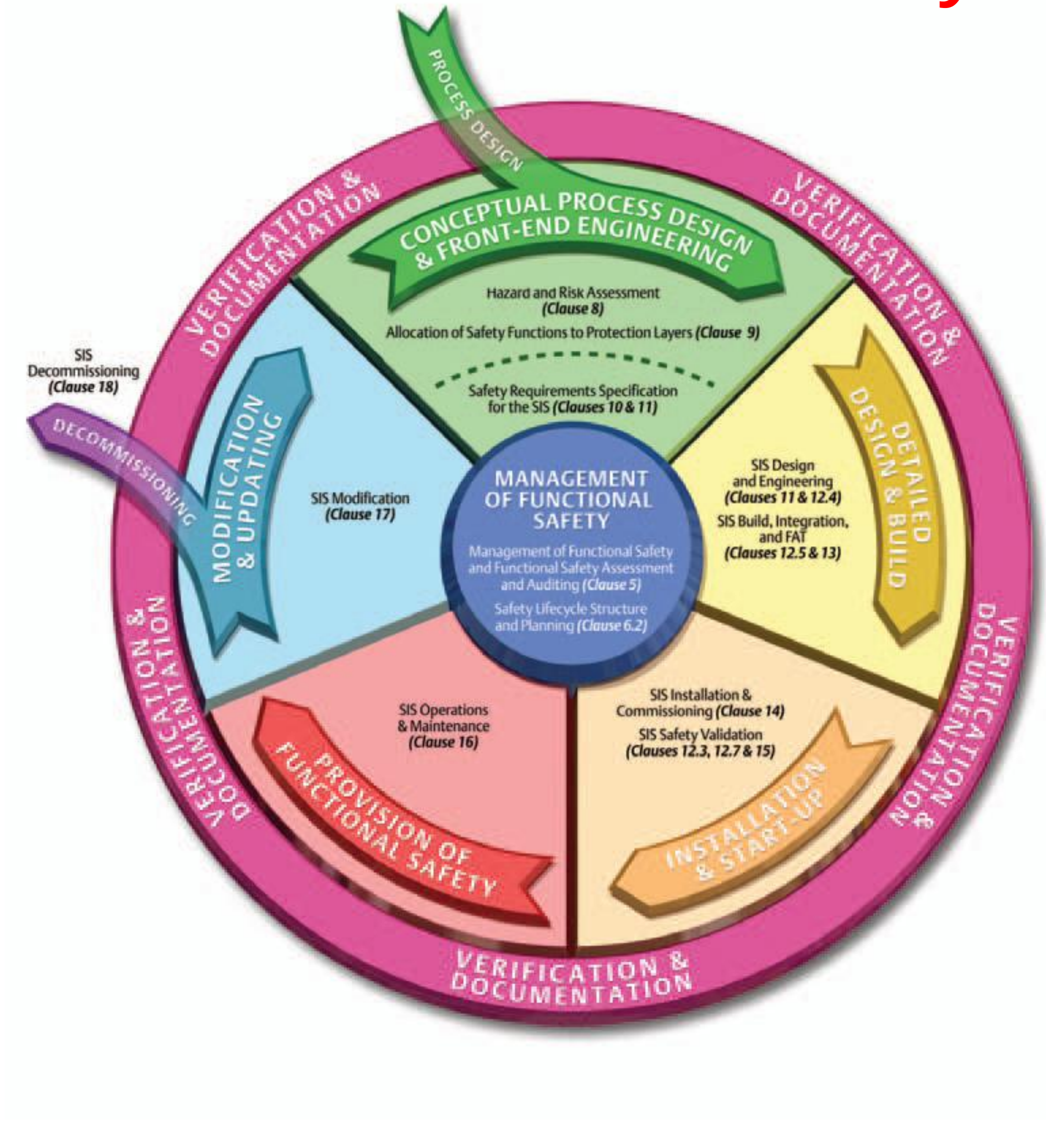
How often do users try it?

- Frequently challenged system:
  - Automobile braking system
  - Assuming this requires a “failure on demand” *rate* of between 10^{-9} to 10^{-8} per hour, it would need a SIL 4 system
- Rarely challenged system:
  - Automobile passenger air-bag
  - Assuming this requires a “failure on demand” *probability* of 10^{-5} to 10^{-4}, it would need a SIL 4 system

How hard do you try and stop them?

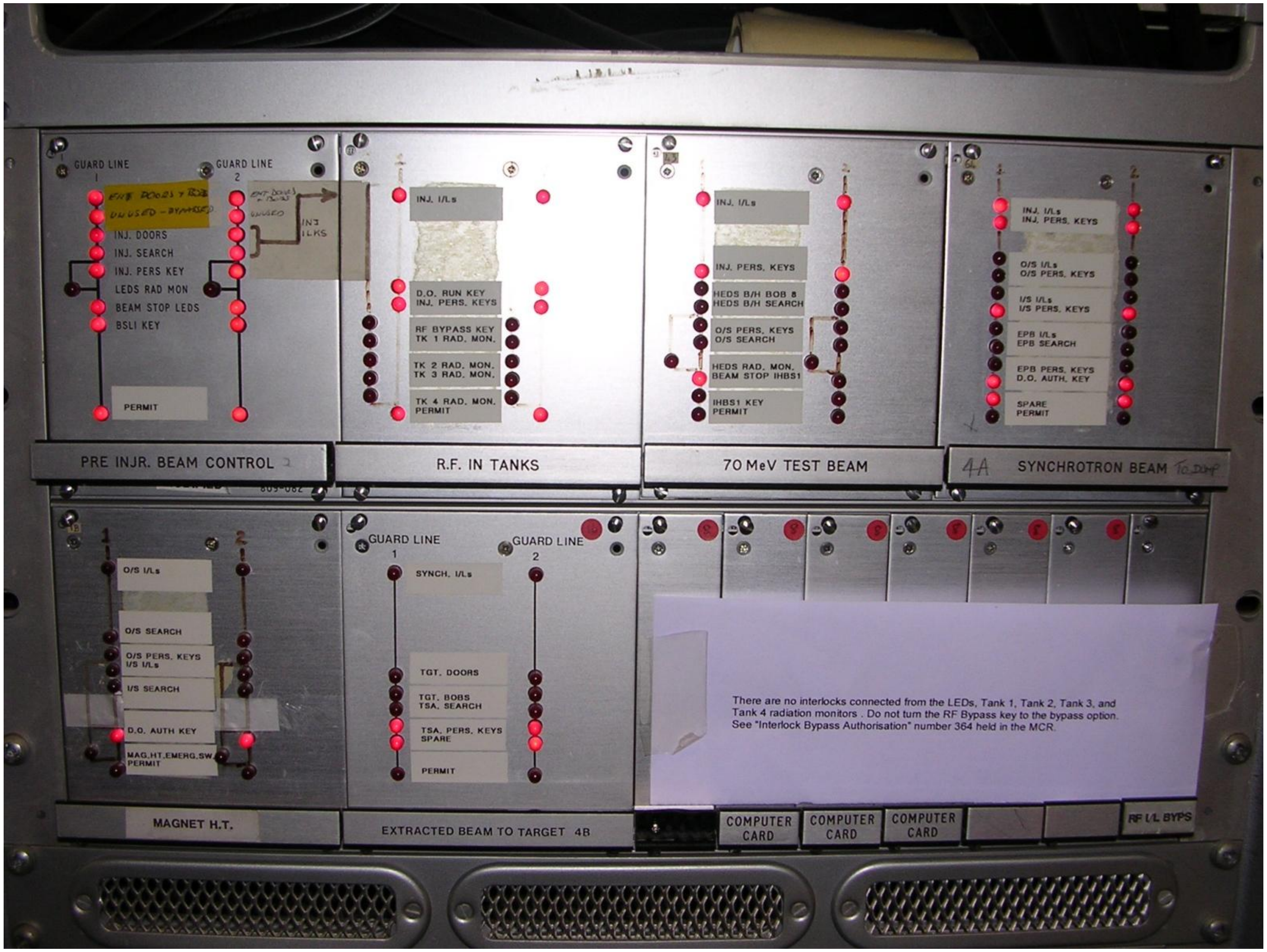
- SIL 4
  - Mad, bad and dangerous to know! (and extremely difficult to achieve in a large system)
- SIL 3
  - Best avoided if possible but may be necessary
- SIL 2
  - Most likely for an interlock/safety system with logic. Design and operating practice very similar to ISO9000/1
- SIL 1
  - Doesn’t really need a interlock/safety system

When can you relax?


PROCESS DESIGN
CONCEPTUAL PROCESS DESIGN & FRONT-END ENGINEERING
Hazard and Risk Assessment (Clause 8)
Allocation of Safety Functions to Protection Layers (Clause 9)
Safety Requirements Specification for the SIS (Clauses 10 & 11)
VERIFICATION & DOCUMENTATION
DETAILED DESIGN & BUILD
SIS Design and Engineering (Clauses 11 & 12.4)
SIS Build, Integration, and FAT (Clauses 12.5 & 13)
MANAGEMENT OF FUNCTIONAL SAFETY
Management of Functional Safety and Functional Safety Assessment and Auditing (Clause 5)
Safety Lifecycle Structure and Planning (Clause 6.2)
SIS Installation & Commissioning (Clause 14)
SIS Safety Validation (Clauses 12.3, 12.7 & 15)
INSTALLATION & START-UP
SIS Operations & Maintenance (Clause 16)
PROVISION OF FUNCTIONAL SAFETY
SIS Modification (Clause 17)
MODIFICATION & UPDATING
SIS Decommissioning (Clause 18)
DECOMMISSIONING

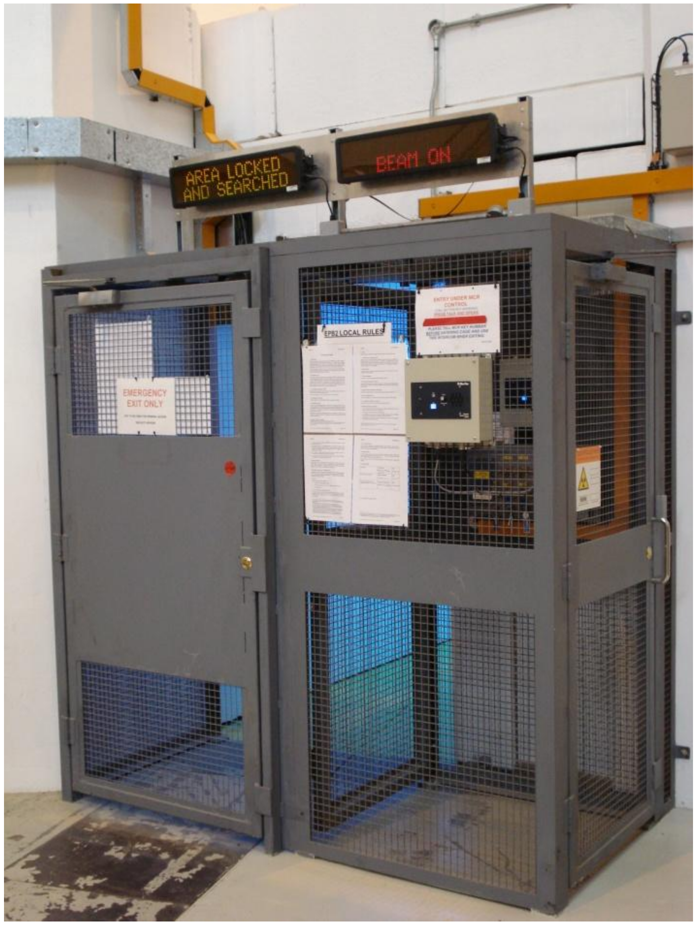
Science & Technology Facilities Council ISIS

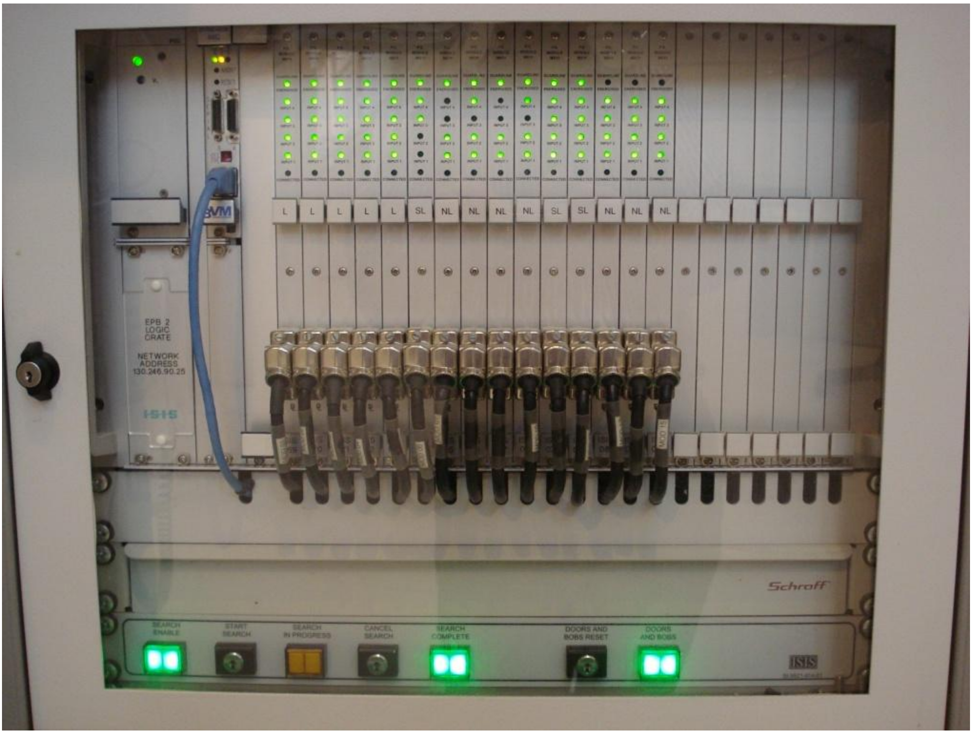
Picture of old PPS



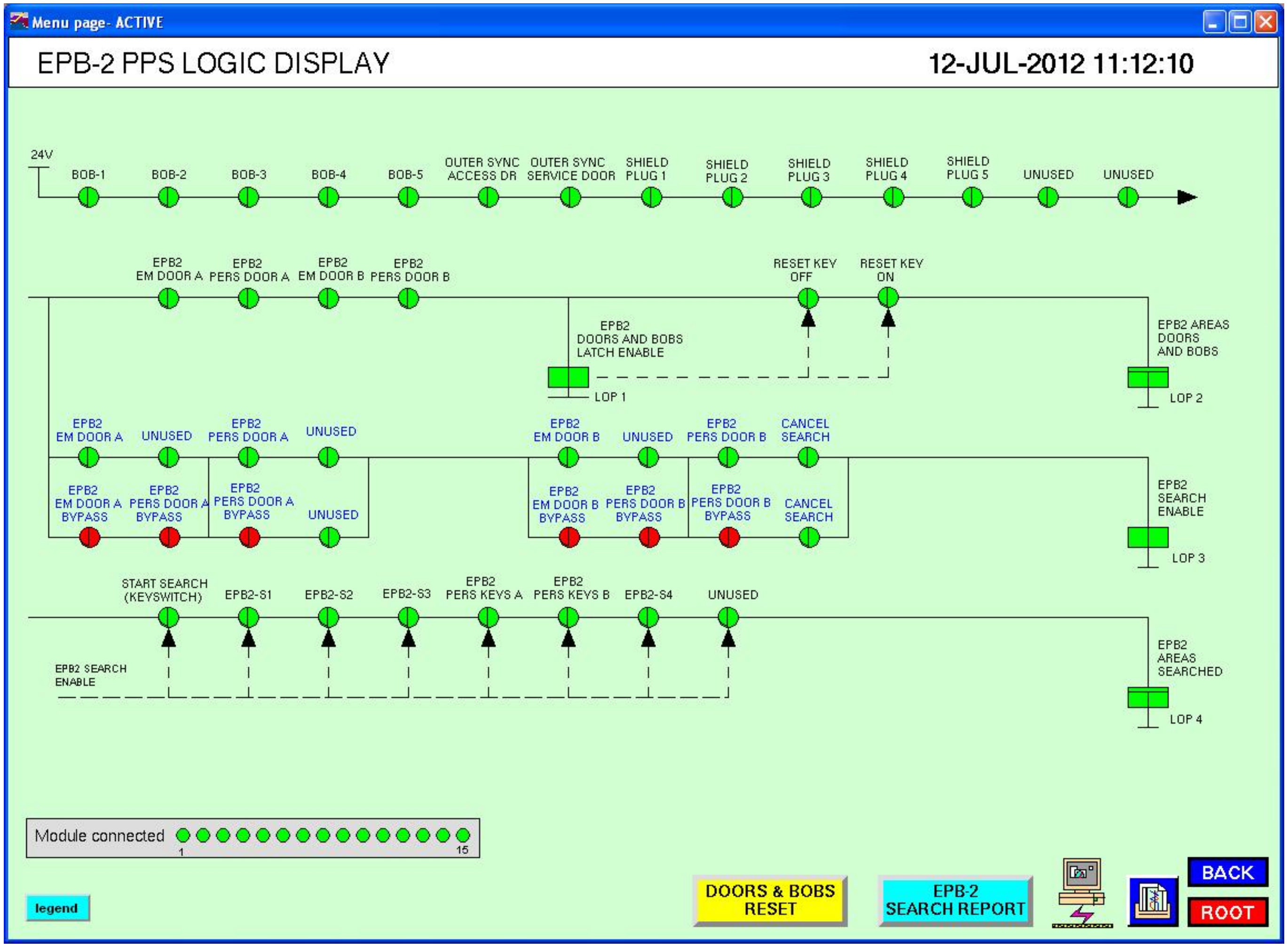
There are no interlocks connected from the LEDs, Tank 1, Tank 2, Tank 3, and Tank 4 radiation monitors . Do not turn the RF Bypass key to the bypass option. See "Interlock Bypass Authorisation" number 364 held in the MCR.

Personnel Protection System (PPS)

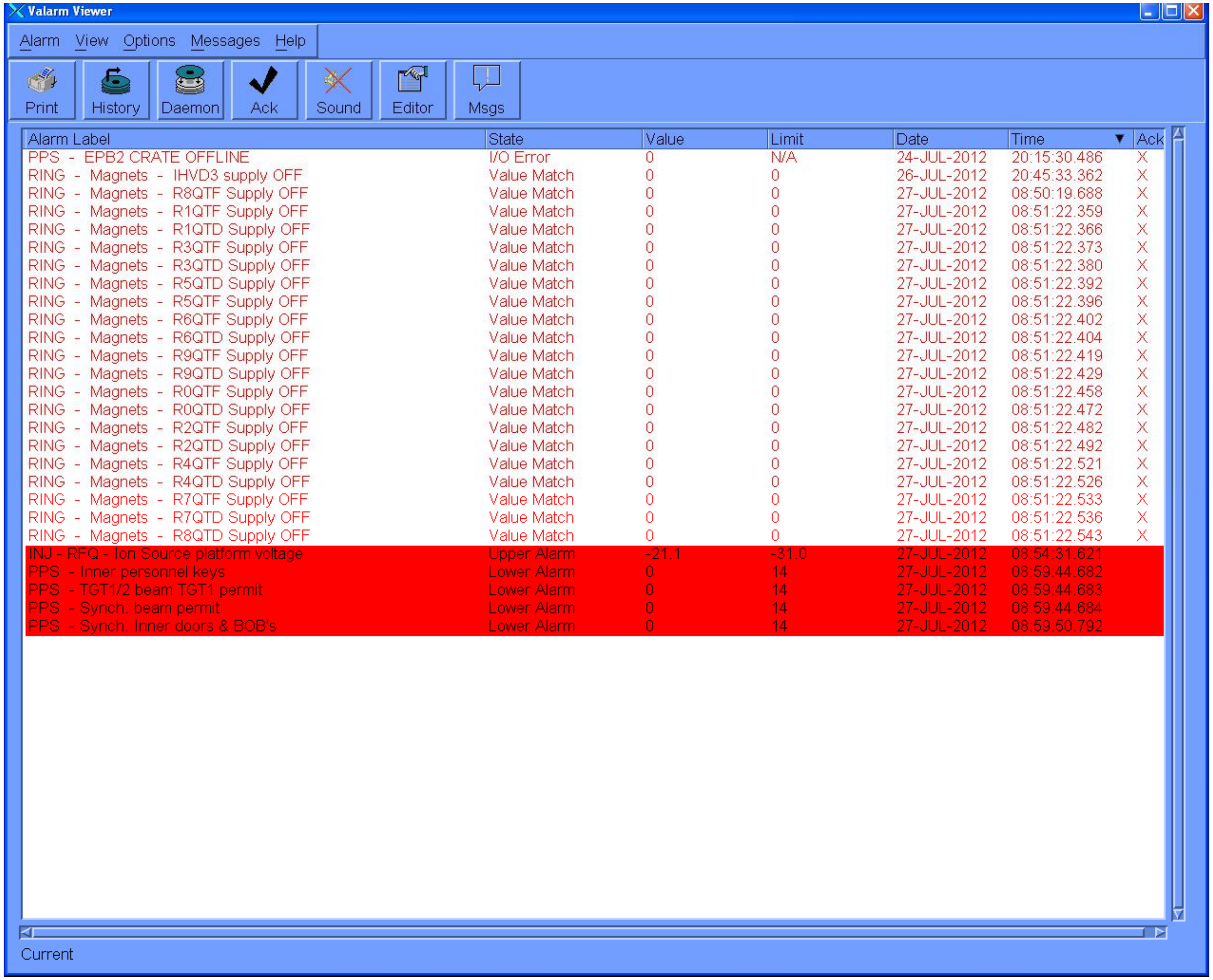




PPS on the control desk

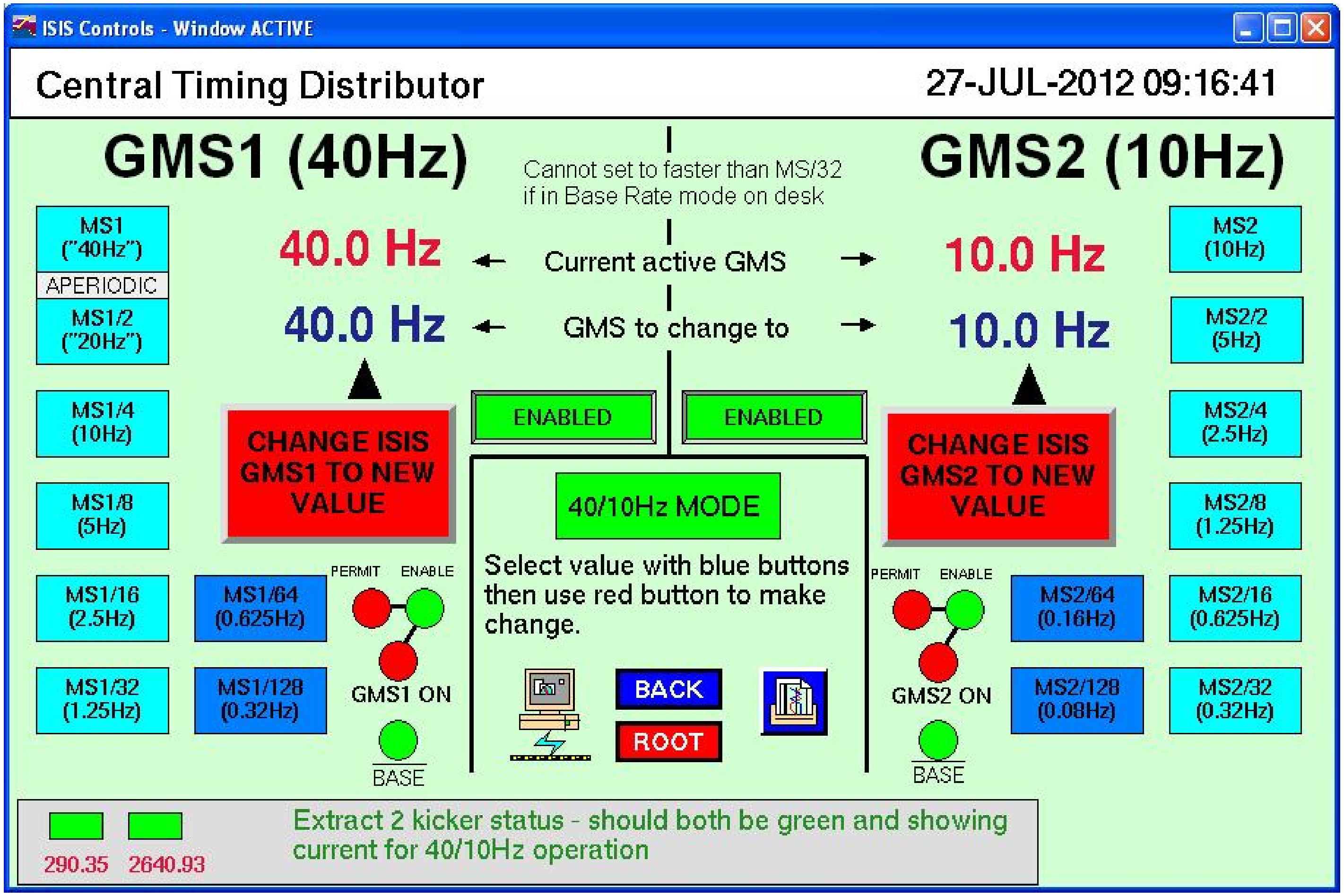


PPS on alarm system



Alarm Label	State	Value	Limit	Date	Time ▼	Ack
PPS - EPB2 CRATE OFFLINE	I/O Error	0	N/A	24-JUL-2012	20:15:30.486	X
RING - Magnets - IHVD3 supply OFF	Value Match	0	0	26-JUL-2012	20:45:33.362	X
RING - Magnets - R8QTF Supply OFF	Value Match	0	0	27-JUL-2012	08:50:19.688	X
RING - Magnets - R1QTF Supply OFF	Value Match	0	0	27-JUL-2012	08:51:22.359	X
RING - Magnets - R1QTD Supply OFF	Value Match	0	0	27-JUL-2012	08:51:22.366	X
RING - Magnets - R3QTF Supply OFF	Value Match	0	0	27-JUL-2012	08:51:22.373	X
RING - Magnets - R3QTD Supply OFF	Value Match	0	0	27-JUL-2012	08:51:22.380	X
RING - Magnets - R5QTD Supply OFF	Value Match	0	0	27-JUL-2012	08:51:22.392	X
RING - Magnets - R5QTF Supply OFF	Value Match	0	0	27-JUL-2012	08:51:22.396	X
RING - Magnets - R6QTF Supply OFF	Value Match	0	0	27-JUL-2012	08:51:22.402	X
RING - Magnets - R6QTD Supply OFF	Value Match	0	0	27-JUL-2012	08:51:22.404	X
RING - Magnets - R9QTF Supply OFF	Value Match	0	0	27-JUL-2012	08:51:22.419	X
RING - Magnets - R9QTD Supply OFF	Value Match	0	0	27-JUL-2012	08:51:22.429	X
RING - Magnets - R0QTF Supply OFF	Value Match	0	0	27-JUL-2012	08:51:22.458	X
RING - Magnets - R0QTD Supply OFF	Value Match	0	0	27-JUL-2012	08:51:22.472	X
RING - Magnets - R2QTF Supply OFF	Value Match	0	0	27-JUL-2012	08:51:22.482	X
RING - Magnets - R2QTD Supply OFF	Value Match	0	0	27-JUL-2012	08:51:22.492	X
RING - Magnets - R4QTF Supply OFF	Value Match	0	0	27-JUL-2012	08:51:22.521	X
RING - Magnets - R4QTD Supply OFF	Value Match	0	0	27-JUL-2012	08:51:22.526	X
RING - Magnets - R7QTF Supply OFF	Value Match	0	0	27-JUL-2012	08:51:22.533	X
RING - Magnets - R7QTD Supply OFF	Value Match	0	0	27-JUL-2012	08:51:22.536	X
RING - Magnets - R8QTD Supply OFF	Value Match	0	0	27-JUL-2012	08:51:22.543	X
INJ - RFQ - Ion Source platform voltage	Upper Alarm	-21.1	-31.0	27-JUL-2012	08:54:31.621	
PPS - Inner personnel keys	Lower Alarm	0	14	27-JUL-2012	08:59:44.682	
PPS - TGT1/2 beam TGT1 permit	Lower Alarm	0	14	27-JUL-2012	08:59:44.683	
PPS - Synch. beam permit	Lower Alarm	0	14	27-JUL-2012	08:59:44.684	
PPS - Synch. Inner doors & BOB's	Lower Alarm	0	14	27-JUL-2012	08:59:50.792	

2 targets = effort x 4!



ISIS Controls - Window ACTIVE

Central Timing Distributor 27-JUL-2012 09:16:41

GMS1 (40Hz)

GMS2 (10Hz)

Cannot set to faster than MS/32
if in Base Rate mode on desk

40.0 Hz ← Current active GMS → 10.0 Hz

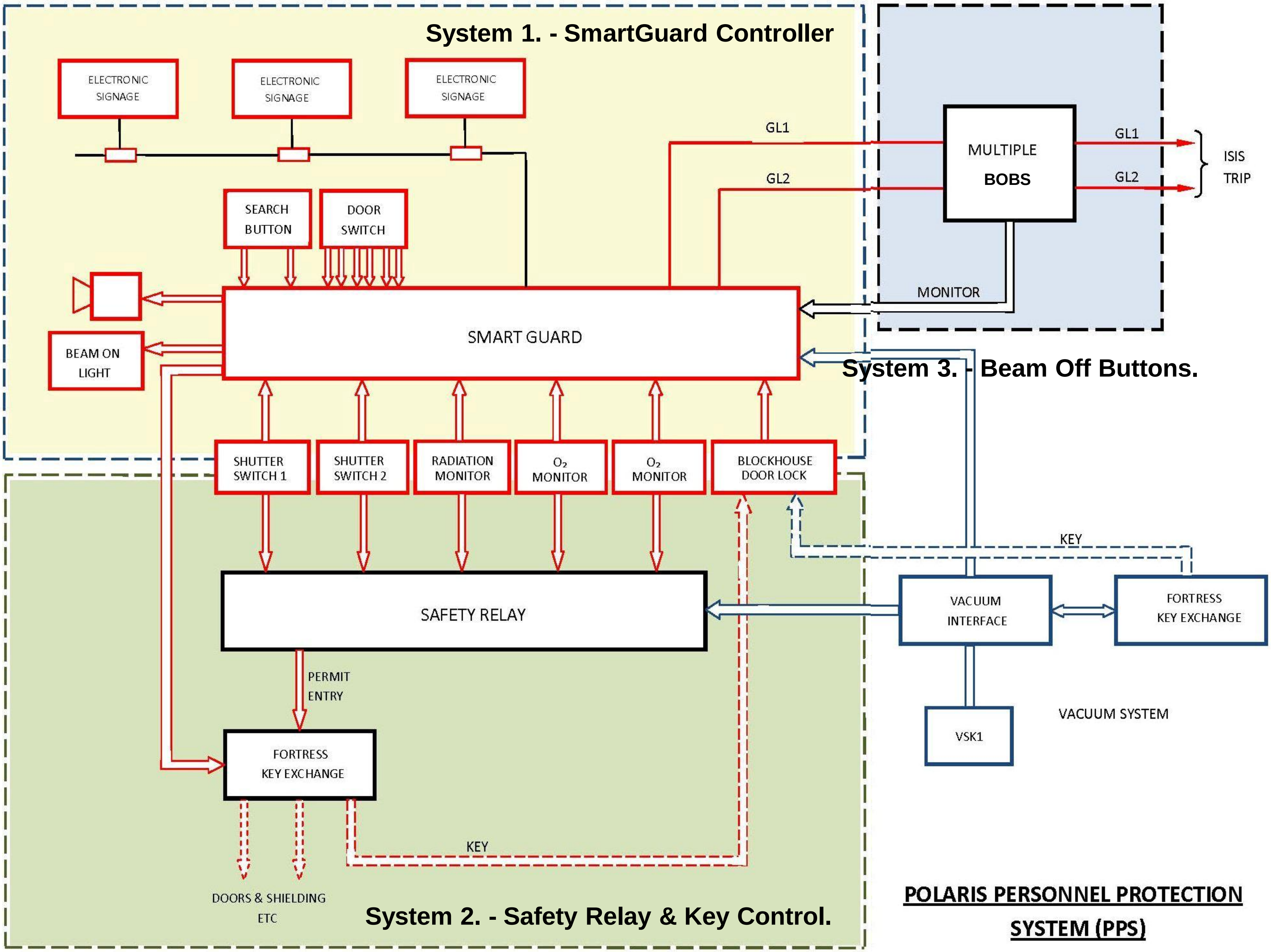
40.0 Hz ← GMS to change to → 10.0 Hz

Select value with blue buttons then use red button to make change.

Extract 2 kicker status - should both be green and showing current for 40/10Hz operation

290.35 2640.93

Target Station 2 PPS



POLARIS PERSONNEL PROTECTION SYSTEM (PPS)

Modifications

- No formal modification process – no 61508
- ISIS Safety Modification Panel (ISMP) 3 tier approach
  - Minor changes (like for like etc.) - noted
  - Operational manager approved – full request and discussion if necessary
  - Full ISMP referral – full discussion and approval (or not) by ISMP
- 30-40 modification requests per year (total)

"*The ISMP operates the formal change control and monitoring function for ISIS Key Safety Related Equipment (KSRE) and some Safety Related Equipment (SRE) on behalf of ISIS Senior Management.*"

ISIS experience

- More than one group doing 61508 work avoids complacency but can lead to inconsistemcy
- 61508 compliance is expensive – what is the business case?
- You will probably need to employ external consultants
- Having no standard to adhere to almost inevitably leads to increasingly compromised safety systems
- Is it worth documenting chosen areas of non-compliance and running a nearly compliant system?

Recommendations

- Single group of experts responsible for Key Safety Related Equipment (KSRE)
- Clear and defensible facility policy on where 61508 is applicable and where it is not and the business case for using it
- Continuing training program for such staff
- Biennial reviews of operation of KSRE
- Auditing of all 61508 systems (and others)