IEC61508 at ISIS

Bob Mannix (Controls Group)
Alan Stevens (Accelerator Operations Group)
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”
Let's 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?
Picture of old PPS
Personnel Protection System (PPS)
PPS on the control desk
PPS on alarm system
2 targets = effort x 4!
System 1. - SmartGuard Controller

System 2. - Safety Relay & Key Control.

System 3. - Beam Off Buttons.
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.”
More than one group doing 61508 work avoids complacency but can lead to inconsistency.

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)