

An HSE field inspector's perspective on IEC 61508

John Madden CEng FIEE

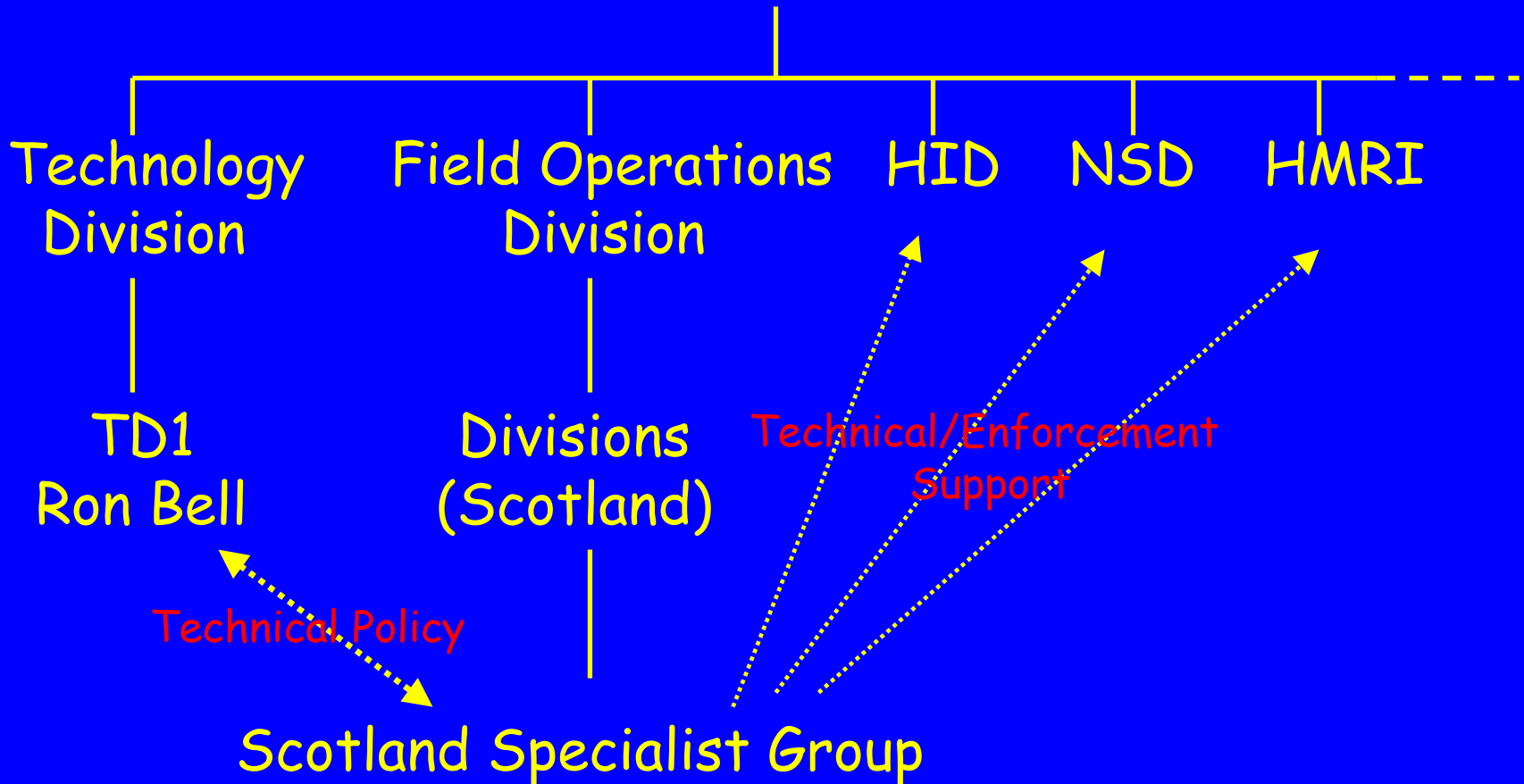
HM Principal Inspector

(Electrical & Control Systems Engineering)

The Agenda

- Where I sit in HSE
- My involvement with the standard
- COMAH Work
- Work in other sectors
 - Fairgrounds
 - Paper making

HSE ↔ HSC



[Other FOD Specialist Groups, with electrical/control inspectors, cover North of England; Midlands; East & South East England; Wales and West England. Other Divs (HID etc) also have electrical/control inspectors]

Responsibilities

- Technology Division
 - Sets technical policy
 - Works on IEC and CEN/CENELEC A&B standards
 - Generates generic guidance
 - Initiates research
 - Has national topic 'deep' specialists

- Specialist Group Electrical Inspectors
 - Investigate accidents and inspect premises/systems.
 - Assess safety cases/reports
 - Carry out or support enforcement action
 - Act as expert witnesses
 - Produce sector-specific guidance
 - Work on C standards development

Status of IEC 61508 in HSE

- ❑ IEC 61508 is used as a reference standard for determining whether a reasonably practicable level of safety has been achieved when E/E/PE systems are used to carry out safety functions.
- ❑ The extent to which HSE will use IEC 61508 will depend on individual circumstances; whether any sector standards based on IEC 61508 have been developed and whether there are existing specific industry standards or guidelines.
- ❑ HSE PES documents (first published in 1987) have now been withdrawn.

Field use of IEC 61508

- To date, my use of the standard has centred on:
 - Assessment of safety reports submitted under the Control of Major Accident Hazards (COMAH) Regulations.
 - Generating guidance on safety-related control systems for:
 - Fairground rides
 - Paper making machines

COMAH Assessment Work

- Operators of sites subject to the Regulations must submit Reports for assessment by the Competent Authority.
 - eg petrochemical & chemical sites; warehouses containing prescribed amounts of HFLs, toxics etc.
- Safety-related control systems content is technically-assessed by HSE's Electrical & Control Engineering Inspectors.

COMAH Assessment Work

- Assessment criterion: “The safety report should describe how safety-related systems have been designed to ensure safety and reliability”
- We look for:
 - Link between MAH risk reduction requirements and required safety integrity of SISs
 - Evidence of systematic determination of required SILs
 - Demonstration of how required SILs have been achieved.
 - Information on requirements for proof testing; maintenance; configuration/change control etc.

COMAH Assessment Work

- It is clear that the use of IEC 61508, and reference to it in COMAH reports, will assist duty holders to make the necessary demonstrations.
- We encourage the use of IEC 61508 in this respect, but do not (and cannot) insist where other valid techniques/standards are used.
- We use the principles of the standard in making our assessments and in taking any follow-up action.

Fairgrounds

- Rides can be complex and are increasingly so.
- Safety PLCs & fieldbus devices are becoming common.
- Our new guidance suggests that safety-related control systems should be designed using IEC 61508.



Paper making machinery

- Many mills incorporate complex programmable safety-related control systems, or are being modified to use them
 - Motor drives; "safety PLCs"; safetybus architectures etc
- New HSE guidance suggests that designers, specifiers and system integrators should use IEC 61508 as the basis of their work for safety-related control systems.



Conclusions

- HSE field inspectors are increasingly using IEC 61508 as a core element of their work on safety-related control systems.
- Not used in all applications, but is where complex programmable systems have safety functionality.