

IEC 61508 Methodology in brief

Safety lifecycle Participants

- System definition
 - End user / Consultant
- Realisation phase
 - End user / Vendor / Contractor
- Operation and maintenance phase
 - End user / Contractor

that in any safety lifecycle there will be a number of parties that have to participate. If we look at this in very simple terms, the key ones are System Definition, some sort of Realisation Phase, which is design right through validation and test, and then the third phase is obviously Operation and Maintenance. From the perspective of people who might be running theatres and wanting to buy equipment or build equipment in-house, who's involved in all those stages? You are, as end users. If you're end users, you have to have some appreciation of IEC 61508, because in fact you are in many ways the key player.

"If you're an end user you have to have some appreciation of IEC 61508, because you are, in many ways, the key player."

So why do we need to bother with IEC 61508? There is an interesting bit of research done by the UK Health and Safety Executive. They looked at the primary cause of 34 incidents in various classes of control system. This shows that specification errors are a major cause of incidents, as well as errors in design, implementation, installation and commissioning. There are some problems with operation and maintenance; and, rather as expected, 20% due to changes after commissioning. It's always worth knowing that changing something after you have got a system into service is often where increased risk or even new hazards can be introduced. The major point about

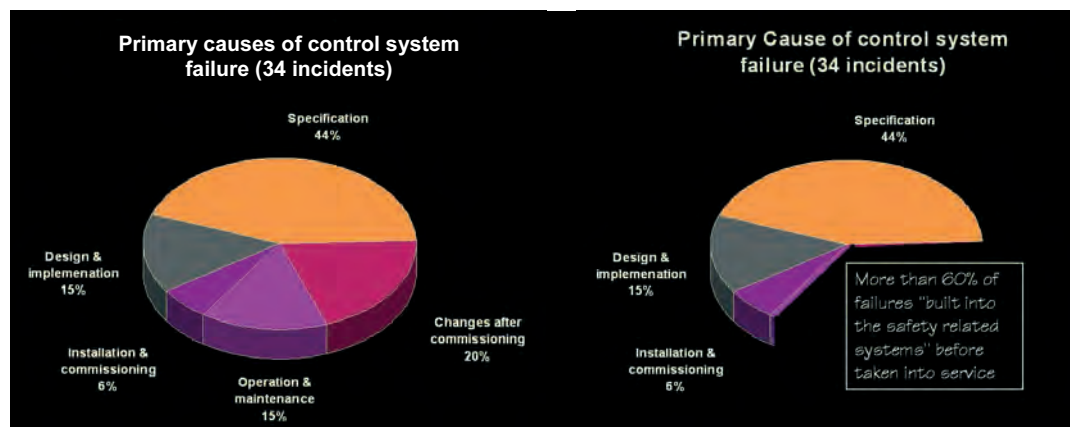
this chart is that it shows you've got more than 60% of the primary causes of failures actually built into the safety-related systems before they were even put into service. That is saying that we need a standard, a methodology, that can reduce that number of mistakes effectively.

So why do we need *more* standards applied to theatres? My personal feeling is that the major reason is that stage machinery is getting more complex, and I don't see an end to this. We have more axes, more moves, more reliance on synchronisation, and we're now getting into areas like having multiple operators. This particular aspect can be quite worrying; there's been some recent research which basically says that the understanding of human factors is fairly good for a single operator working a single piece of machinery, but there's been very little research done on the situation where you have multiple operators controlling many pieces of machinery. This is what we're beginning to see in high-capability systems with multiple control desks and operators scattered all over the theatre.

With this level of complexity you have to

Two leading experts consider the implications of IEC 61508 and Safety Integrity Levels on all aspects of stage engineering, comparing the new regulations with the current German DIN standards and also coming up with many practical points that must be understood by everyone dealing with the safety of control systems. The final diagram illustrates the application of IEC 61508 on a typical theatre installation.

"... more than 60% of the primary cause of failures are actually built into the safety-related systems before they are even put into service."



Source: 'Out of Control' HSE. ISBN 0 7176 0847 6