trusted to deliver™

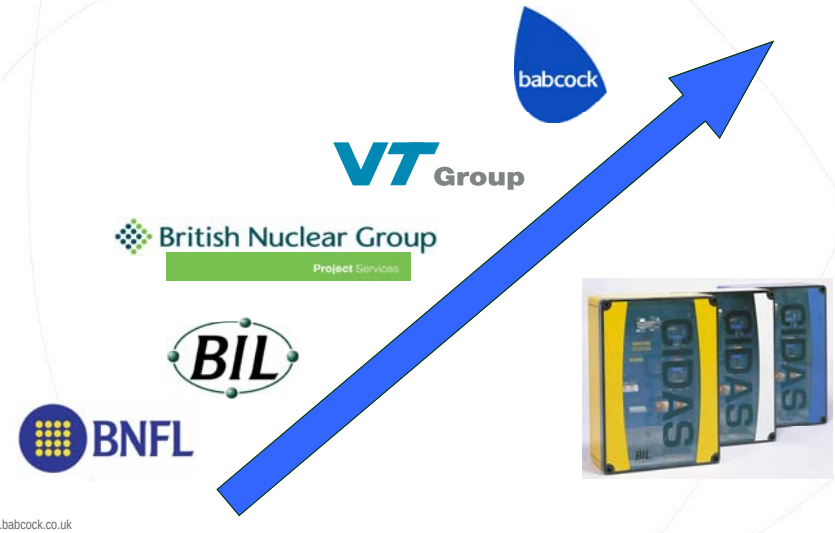
Criticality Incident Detection Systems – How Reliable?

Kevin Freer, Phil Bodman

ICNC 2011, Edinburgh

CIDAS® History

trusted to deliver™



www.babcock.co.uk

Standards

trusted to deliver™

- IEC60860 (1987)
- ANSI/ANS-8-3 (1997, Reaffirmed 2003)
- ISO7753 (1987)

Similar….

"High" reliability and "Low" false alarm rate

Is this a problem?

Different….

Routine testing (signal generator annually or 3 monthly, radiation testing monthly, alarm system 3 monthly)

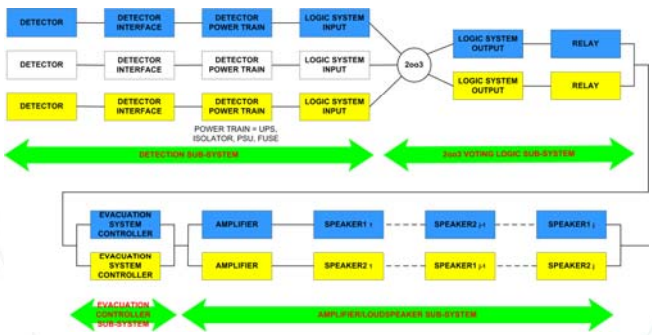
Is this a problem?

Reliability Assessment

trusted to deliver™

- Reliability Block Diagrams (RBD) or Fault Trees (FTA)

  Simple architecture, IEC61508[1] has all the RBD methodology & equations needed (1oo2, 2oo3 including common cause analysis)



[1] IEC61508 – Functional Safety of Electrical/Electronic/Programmable Electronic Safety Related Systems (2010)

Source Data

- Require failure rates of components/sub-systems for dangerous and safe failures and whether each failure is detected by in-built tests, or only at proof test.
- Source can be
  - Real plant data (OK if lots of identical components e.g. detectors)
  - Generic (e.g. loudspeakers)
  - FMEA and electronic component reliability database
  - Engineering judgement

Results

Baseline…..

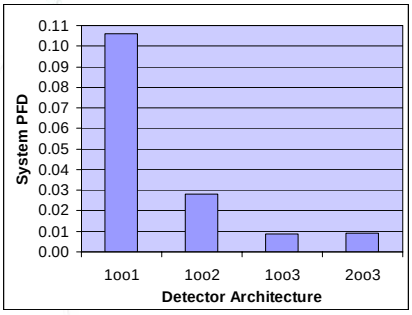
- **Large system** 160 speakers per channel (320 in total) / 30 detectors per channel (90 in total), 1 year proof test interval

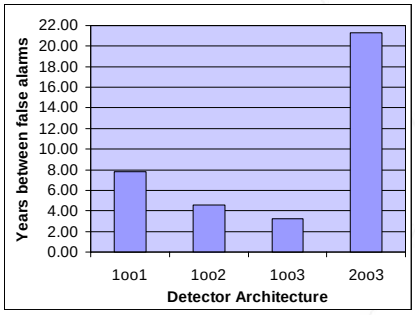
  - PFD = 0.009
  - False alarm = 1 in 21 years
- IEC61508 SIL2

  Design requirement = PFD < 0.010

  False alarm rate <1 in 10 years

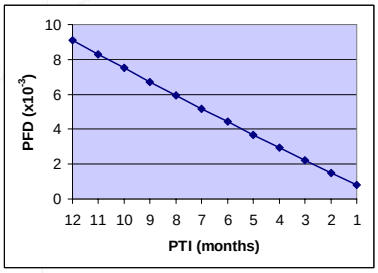
Effect of architecture





Detector 2oo3 gives low System PFD and high time between false alarms

Effect of Proof Test Interval



If 0.009 PFD is accepted then 12 month PTI, but can half this by changing to 6 month PTI.

Alternative Proof Test Interval (PTI) Scenarios

Scenario	PFD (x 10^{-3})
1 year PTI	9.11
1 year PTI except 1 month PTI for **detectors**	8.18
1 year PTI except 1 month PTI for output **amplifiers**	5.23

Standards ask for more regular testing of detectors – in fact for this system more regular testing of output amplifiers is more important.

Sensitivity to Components

trusted to deliver™

PFD of Sub-Systems

Component	PFD (x 10^{-3})
Detection Sub-system	1.02
2oo3 Voting Logic	0.57
Evacuation System Controller	3.25
Amplifiers	4.24
Loudspeakers	0.03
SYSTEM TOTAL	9.11

Controller and Amplifiers are most significant factors

Summary

trusted to deliver™

Quantitative reliability analysis provides significant information about the system

- Quantifies the PFD and false alarm rate
- Allows alternative system architectures to be considered
- Informs the design (where to add extra built-in tests, effect of changing components etc)
- Informs Proof Testing (what to test)
- Allows different Proof Test Intervals to be considered (what components are most important to reliability, and how often to test each)