babcock

trusted to deliver™

CIDAS®

The Development of a New Criticality Accident Alarm System

Contents

Reasons for Development of New System

- Current system uses very old analogue technology
  - Difficult to set up / change components correctly
  - BES cards have several switch and potentiometer settings
- Obsolescence becoming more of an issue
  - Have had to make lifetime buys of components
  - Potential reduction of expertise at suppliers. Babcock are retaining expertise in-house
- Limited audio capacity
  - Systems are becoming larger
  - Current system limited to eight 250W amplifiers
  - To increase audio capacity above the maximum need to link together 2 or more systems - expensive

Requirements for New System

trusted to deliver™

- Minimal setup options, ideally using just switches
- New technology so that obsolescence is less of an issue
- Increased audio capacity to enable delivery of large systems
- Flexibility for different customers e.g. zoning and customised alarm tones

Supplier Selection

- Started in 2008
- Upgrade options
  - COTS
  - Bespoke development
- Supplier evaluations
- BARTEC-VODEC selected.
  - System has no sequential software
  - Experience in life critical oil and gas alarm systems
  - Improved performance
  - Compatible with existing detectors and speakers. Similar architecture (2oo3 detectors, 1oo2 for everything else)
  - Compatible with existing HVPSUs (except 24Vdc RESET).

CIDAS® MkXI versus CIDAS® MkX Design

- No Change
  - Detectors
  - Annunciator
  - Speakers
  - KOWLs
  - NAWLs
- Small Modification
  - HVPSUs

CIDAS® MkXI versus CIDAS® MkX Design

- New
  - Logic now integrated into the BES, not a separate unit.
  - BES electronics uses digital technology; easier to set up; fewer components so safety justification easier; less obsolescence issues.
  - Amplifiers scalable. Unlimited no. of amps. Includes a “hot spare” so if amp fails no need to shut down system.
  - Duplex System based on two separate systems not master/slave, so safety justification easier
  - BES only can be supplied as a single system.
  - BES zoning optional for detection and evacuation
  - UPS

CIDAS® MkXI versus CIDAS® MkX Design

babcock
trusted to deliver™

Amplifiers

- Scalable (virtually unlimited output power) MkXI BES can control an unlimited numbers of audio amplifiers hence much larger numbers of loudspeakers can be used than CIDAS® MkX with max the 1600W audio power (2x 800W)
- The system includes a “hot spare” amplifier so that in the event of an amp failure, it is automatically replaced by the hot spare without having to shut down the system

CIDAS® MkXI Diagnostics

trusted to deliver™

System Diagnostics

- Detectors (with optional built-in check source - MkXI)
- Detector Cable Monitoring
- Loudspeaker Cable Monitoring
- Power Supply Failures
- Logic Failures
- NAWL cabling monitoring
- Amplifier failures
- UPS monitoring

The system has been designed so that no single fault will immobilize the operation

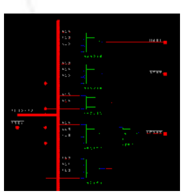
FPGA Development

babcock
trusted to deliver™

- System utilises FPGAs in several of the hardware modules
- FPGAs used to perform logic functions that were previously incorporated in the MkXI logic system
- FPGAs used to generate alarm tones
- Anti fuse FPGAs used
- Can only be configured once. Cannot be re-configured in the field
- Radiation tolerant version of the Actel device used

FPGA Development

- FPGA code needed to be developed to a rigorous process
- IEC61508, in its 2nd edition published in 2010, has for the first time incorporated a section on FPGA development
- Process developed in conjunction with Bartec Vodec & FPGA supplier Actel
- IEC61508 mandates VHDL for the alarm path
- CIDAS® MkXI uses VHDL for alarm path and diagnostics
- New process developed and documented for all CIDAS® MkXI FPGA development



```
MUX: PROCESS(I0, I1, I2, I3, A,
B)
VARIABLE muxval: INTEGER;
BEGIN
muxval := 0;
CASE muxval IS
WHEN 0 => Q <= I0 AFTER 10 ns;
WHEN 1 => Q <= I1 AFTER 10 ns;
WHEN 2 => Q <= I2 AFTER 10 ns;
WHEN 3 => Q <= I3 AFTER 10 ns;
WHEN OTHERS => NULL;
END CASE;
END PROCESS MUX;
```

Reliability Assessment

trusted to deliver™

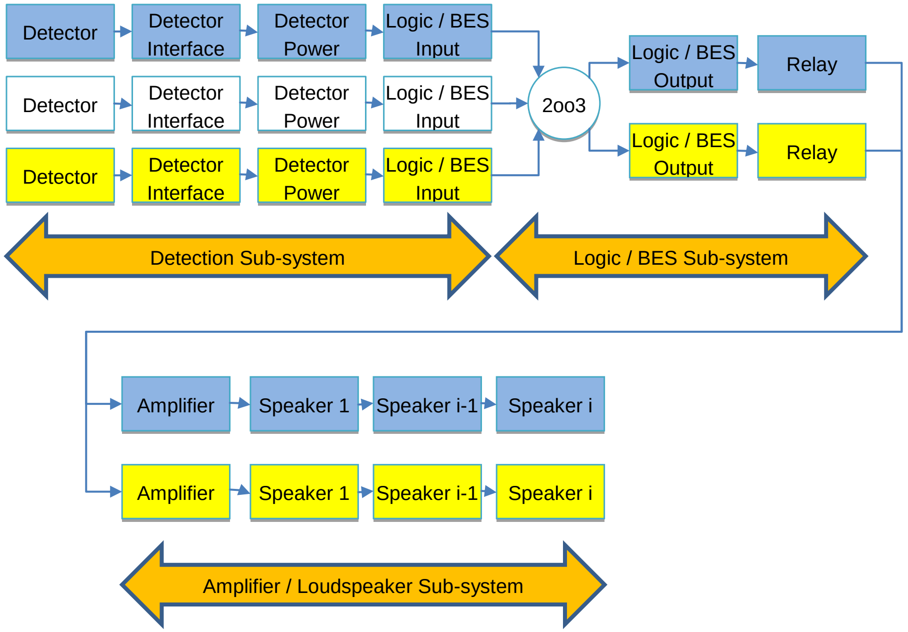
- Expert third-party contracted to perform a FMEDA
- A formal approach to support claims made for system reliability and diagnostic coverage
- Conducted at the hardware component level
- Model system (Reliability Block Diagrams)
- Look at rates of failure of components of the system
- Look at effect of these failures on the system
- Determine which are safe, dangerous, detected, undetected
- Do calculations to determine PFD

Reliability Assessment

trusted to deliver™

- Reliability Block Diagrams (RBD)

  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)

FMEDA

Failure Modes, Effects and Diagnostics Analysis of BES

Failure Type	Definition
Revealed	Confidence tone stopped / started
Unrevealed	All failures other than Revealed
Dangerous	No criticality tone on demand Criticality tone distorted / out of sync with other channel
Safe	All failures other than Dangerous

The BES FMEDA considers one channel + sync signals (so Dangerous Failure = this channel doesn’t alarm NOT both channels fail to alarm).

The Babcock system assessment considers both channels in the CIDAS® system (as Mk X).

FMEDA Findings:

trusted to deliver™

- Some pessimisms are included in the analysis, in particular, all failures of FPGA, its power supply or its clock are assumed to be Dangerous Undetected.
- The loop test on amplifiers/loudspeakers operates less often than the current MkX (in MkXI maximum 6 minutes before fault is definitely revealed, in MkX ~2 minutes).

  [still significantly less than PTI, so is still considered to be a revealed failure]
- There are a small number of “Dangerous Undetected” failures in the BES channel.
- The proof test should be tweaked slightly from MkX.

Dangerous Undetected

- FPGA (chip, power, clock) – unknown outcome, hence (pessimistically) assumes all failures are in this category.
- Synchronisation signal fails – assumes (pessimistically) that tone is distorted + not understood.
- Detector interface signal port or connector fails to send signal to logic
- Amplifier logic input signal conditioning shorts to ground.
- Beacon control port circuitry fails to send signal to beacons.

Proof Test

trusted to deliver™

Additional Tests Required:

- FMEDA analysis assumes Hot Spare amplifier operates correctly. Switching in of this amplifier needs to be included in Proof Tests.
- Confirm PA cannot override Criticality alarm.

Results

Baseline…..

- **Large system** 160 speakers per channel (320 in total) / 4 pairs of NAWLs / 30 detectors per channel (90 in total)

  1 year proof test interval, 8 hour MTTR
- Confirmed that the equipment meets SIL 2 as defined in IEC61508 when used in the standard CIDAS® architecture (2oo3 detection, 1oo2 alarm)

	MkX	Mk XI	**Target**
PFD	0.0092	0.0022 ✓	**<0.01** ✓
False Alarm Rate	0.06	0.08 ✓	**<0.1 per** ✓

Radiation Tolerance Testing

- CIDAS® MkXI system, including the new UPS, shipped to White Sands Missile Range for testing
- Subject of another paper at conference

CE Marking

- System tested at test house for CE compliance
- CE marked to the appropriate LVD and EMC directives
- Gives confidence through independent testing that the system will perform safely and reliably

babcock

trusted to deliver ™

www.babcock.co.uk