The paradox of control and operation

Andy Brazier
EEMUA

Design and Purchasing

- Hardware
  - Accuracy
  - Reliability
  - Connectivity
  - Data output

- Software
  - Data handling
  - Number of alarms
  - HMI colours, pixel count
  - Automation
  - Cyber security

Internet of Things

- More connections
- More automation
- More data.

Wetware

- Still on Human version 1
- Humans cannot be excluded from our systems
- Miller's law
  - Human working memory can handle 7 ± 2 items
- We can use technology to help
- Human factors are becoming more important.

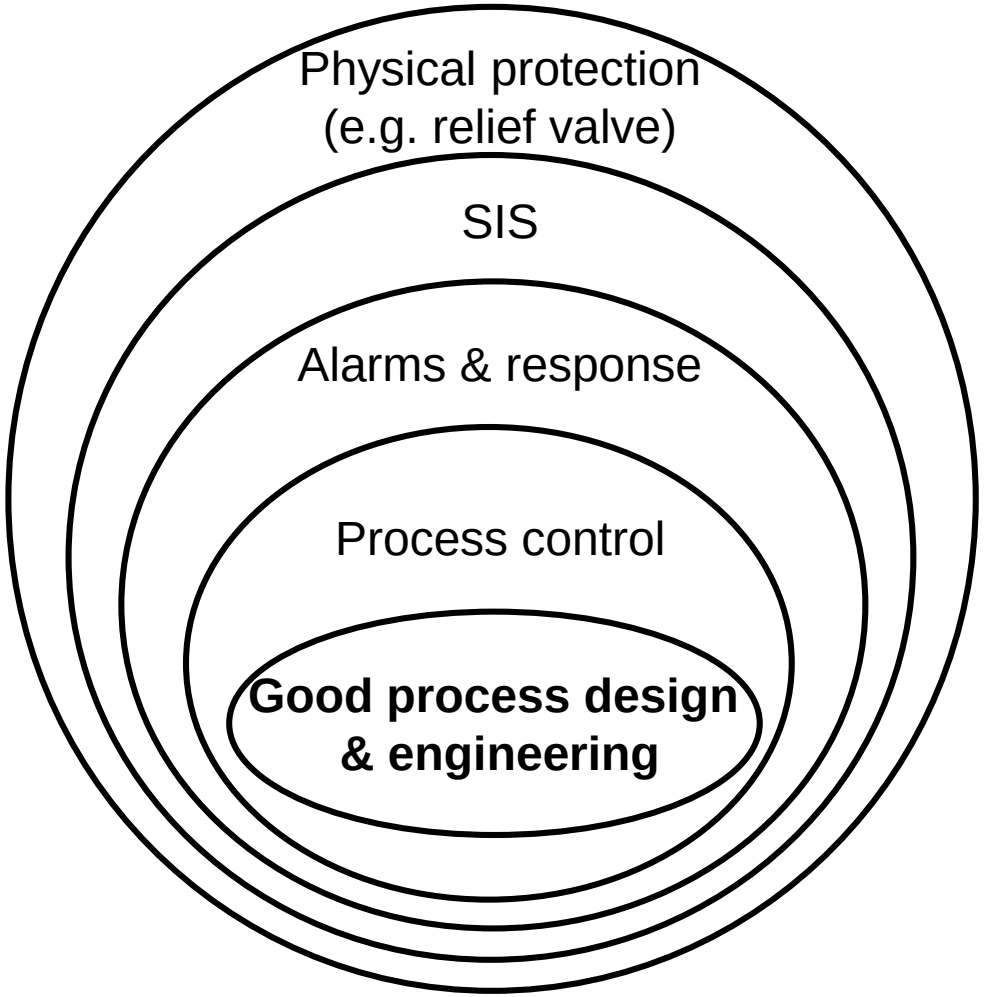
When we have a problem

- Warnings were missed
- Data was misinterpreted
- Wrong decisions were made
- Rarely lack of data

- Incidents are less frequent
- Greater potential consequence.

Balance point has moved

- Multiple layers of protection
- Increased use of active engineered controls
  - Safety Instrumented Systems (SIS)
- Less emphasis on inherent safety.



Boeing 737 max

- Aircraft is inherently unstable
- Technology used to correct
- Data available to pilots
  - If they know where to look
  - If they know what it means.
- Two accidents
  - 346 fatalities
  - Significant impact to business.

Alarms are our solution??

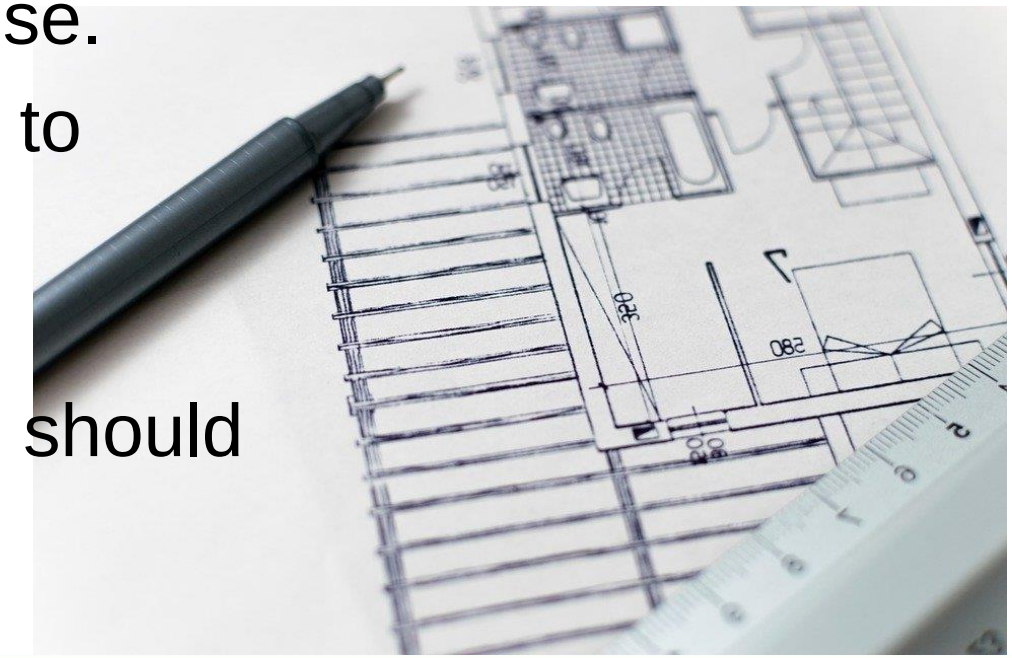
- EEMUA 191 definition of alarm
  - An audible or visible means of indicating to the operator an equipment or process malfunction or abnormal condition
  - The purpose of an alarm system is to direct the operator's attention towards plant conditions requiring their timely assessment and action.
- No shortage of alarms
- But we still have incidents and accidents
  - Operators not aware of the what is happening
  - Do not recognise the seriousness.

Common problems with alarms

- Nuisance alarms during normal operation
- Floods of alarms during process upsets
- Poorly defined or described alarms
- Inconsistent prioritisation
- Response to alarms not defined
- Over-reliance on alarms – failure to adopt inherent safety or engineering controls
- Failing to take into account human strengths and limitations when choosing what to alarm.

Alarm design principles

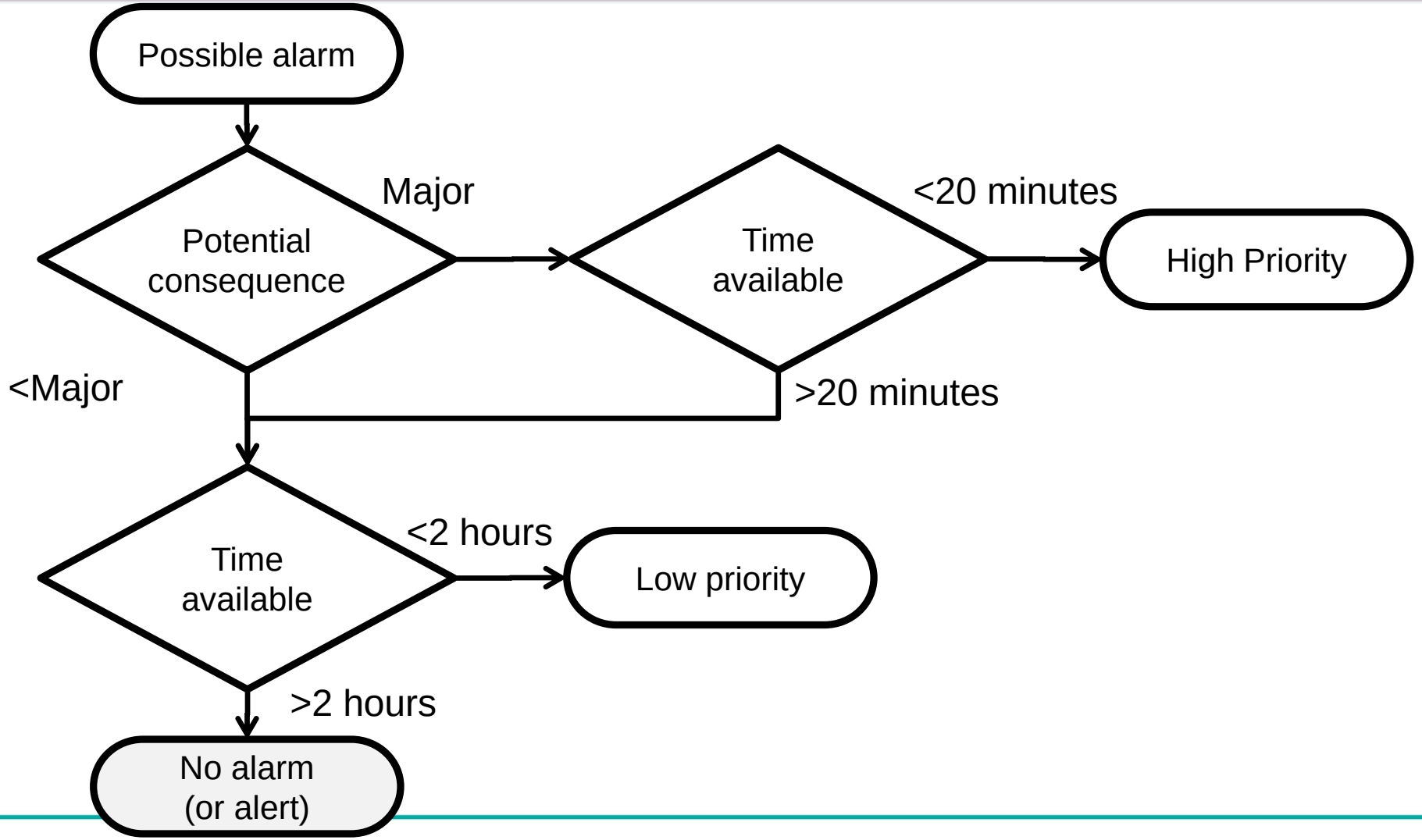
- Each alarm should attract, inform and guide
- Every alarm presented to the operator should be useful and relevant to the operator
- Every alarm should have a defined response.
- Each alarm should allow the operator time to respond
- Nuisance alarms should be avoided
- Demand on automated protective systems should be minimised.



Not alarms – maybe ‘alerts’

- Plant status changes
- ESD trip initiators
- Signals confirming successful operator action
- Duplicate signals
- Events records
  - Operator actions on the system
  - Control system actions
  - Plant equipment automatic changeover.

Alarm review and prioritisation



Operators should not rely on alarms

- Give them the information they need to identify the very earliest signs of a problem
- Human Machine Interface
  - Display data in a useful form
  - Intervene when required
- Allow the operator to maintain situation awareness
- Do not overload the operator
- Support the operator to act reliably.

Allocation of function

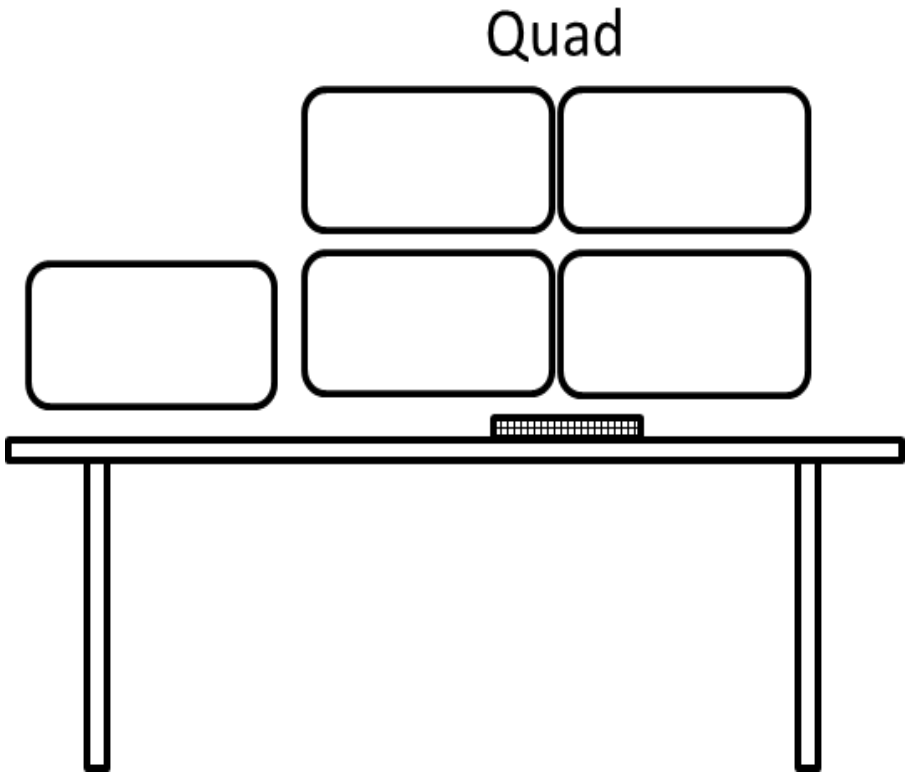
- Humans are good at
  - Pattern recognition
  - Perceiving small changes
  - Recalling relevant information from long ago
  - Working flexibly
- Humans are poor at
  - Processing lots of data
  - Repeating actions with high accuracy
  - Doing more than one thing at a time
  - Staying alert
  - Working under stress.

Human machine interface

- Take advantage of human strengths of perception, shape recognition etc.
- Provide overviews
- Use appropriate symbols
- Display data in a way that is easy to understand
- Show trends
- Minimise numerical data and text
- Use colour in a meaningful and consistent way.

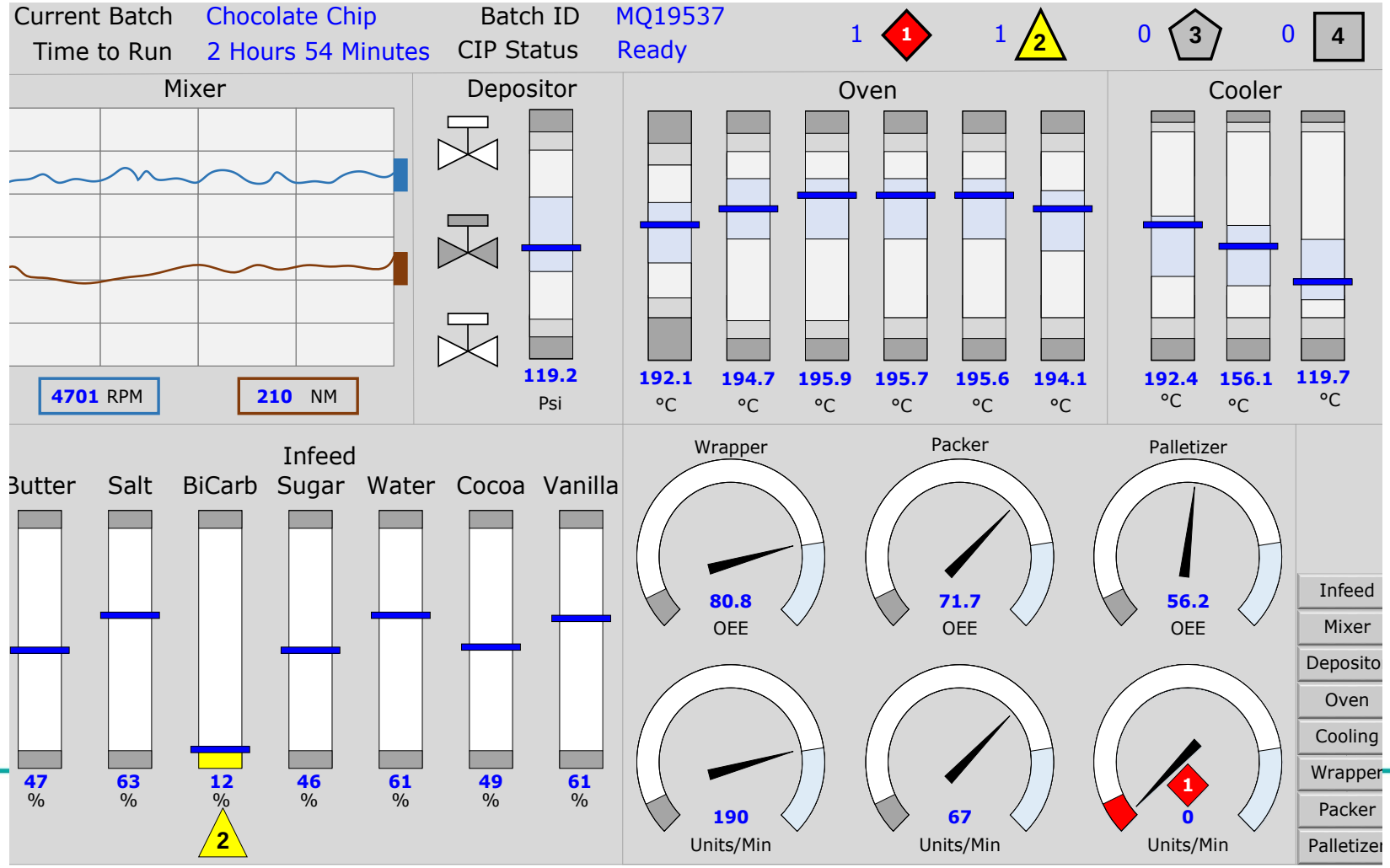
How many screens?

- Maximum of four for operations
- Compact layout
- Remember other screens needed
- Provide a spare workstation
- Large screens usually secondary.

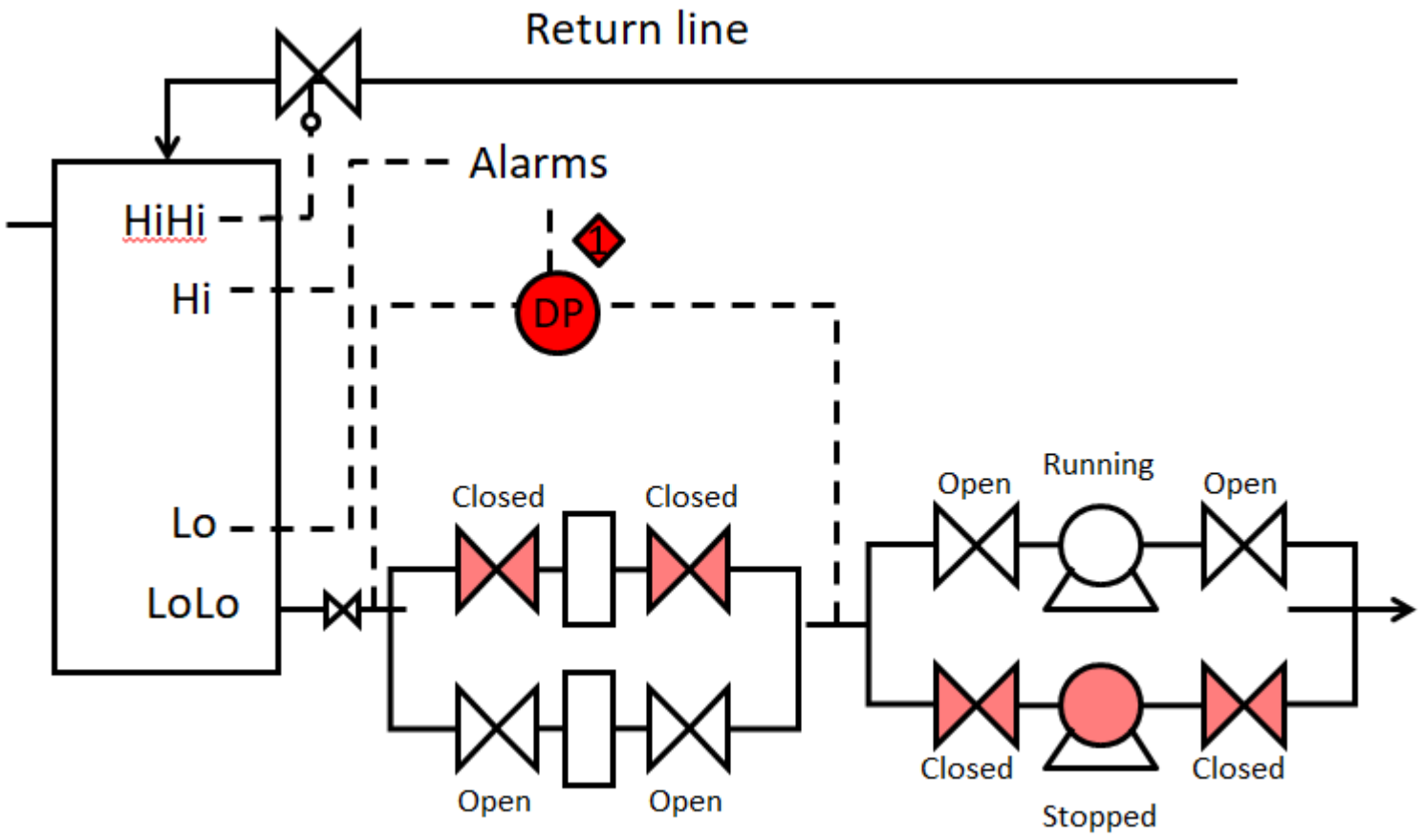


Overview graphics

- High level covering full area of responsibility
- ‘At a glance’ picture of the current state
  - 5 second glance
- Early indication of problems
- Know which screen will be used.



Use of colour

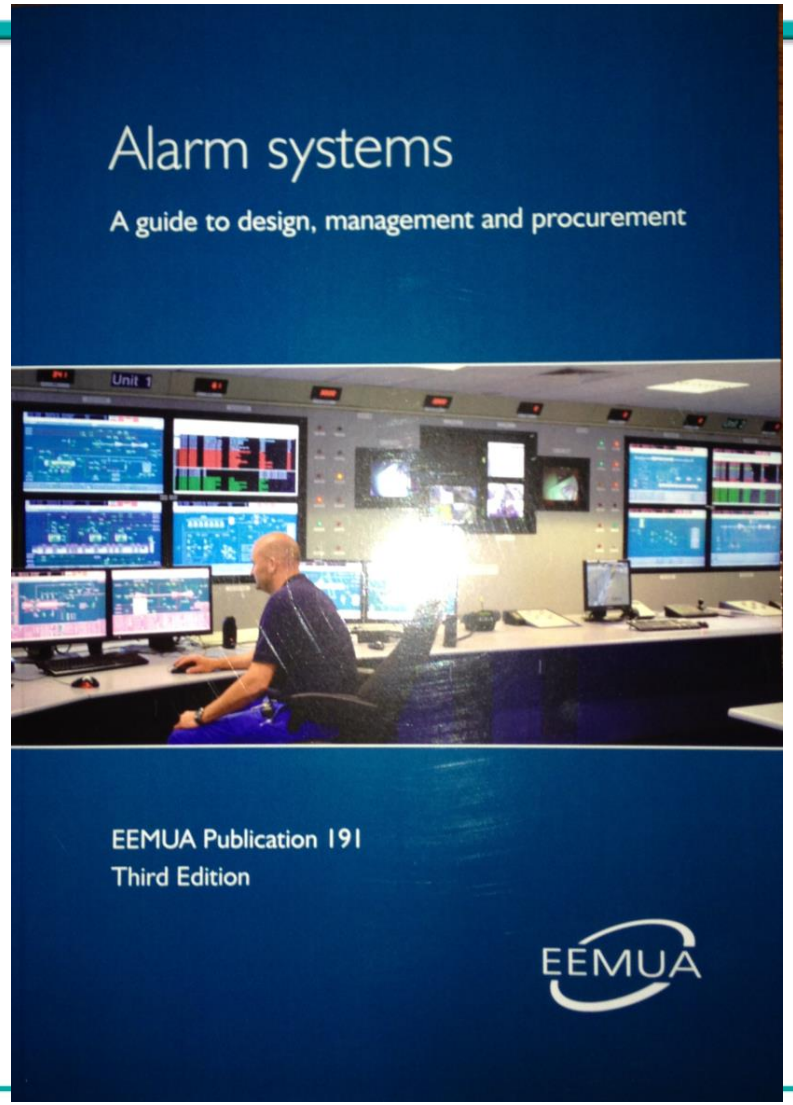


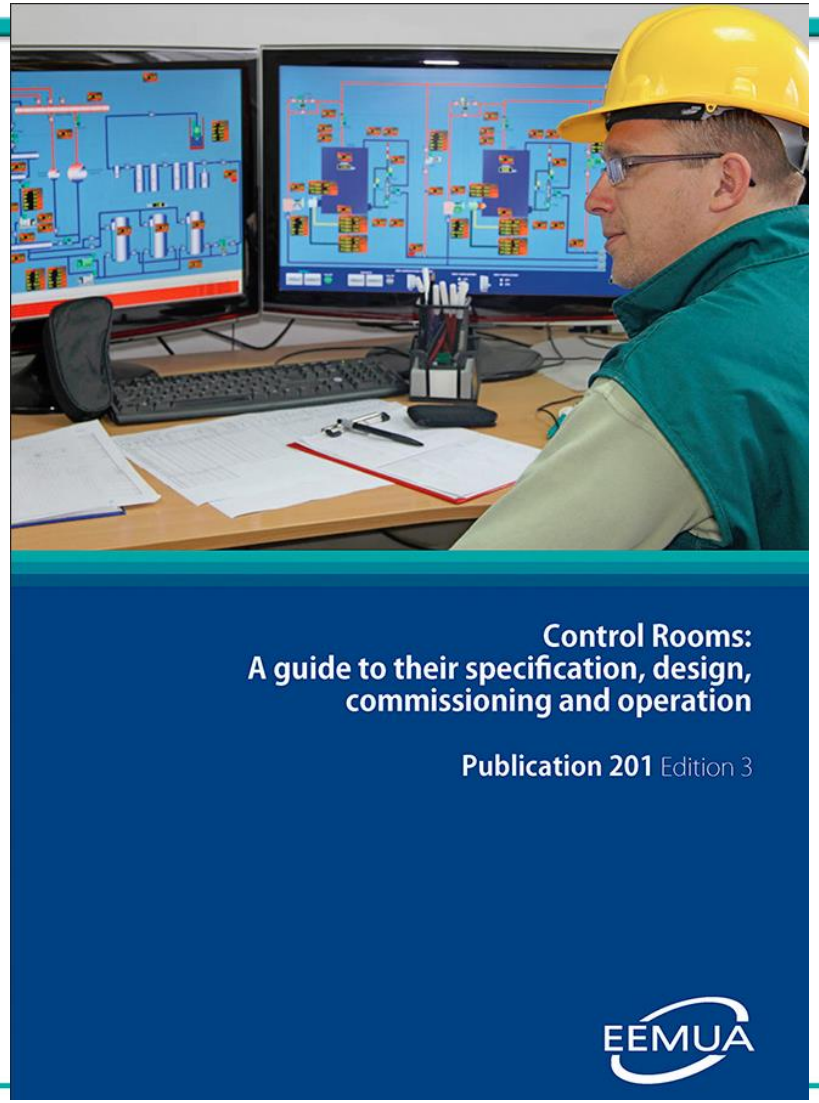
- Vibrant red for alarm
- Lighter colours for status
- CRO preference

But people are not machines

- We need our CROs to be healthy and alert
- Working environment
  - Lighting
  - Ventilation
  - Noise
  - A window!
- Room and workstation layout
  - Access to the items needed
  - Support communication
  - Maintenance and cleaning.

Latest good practice

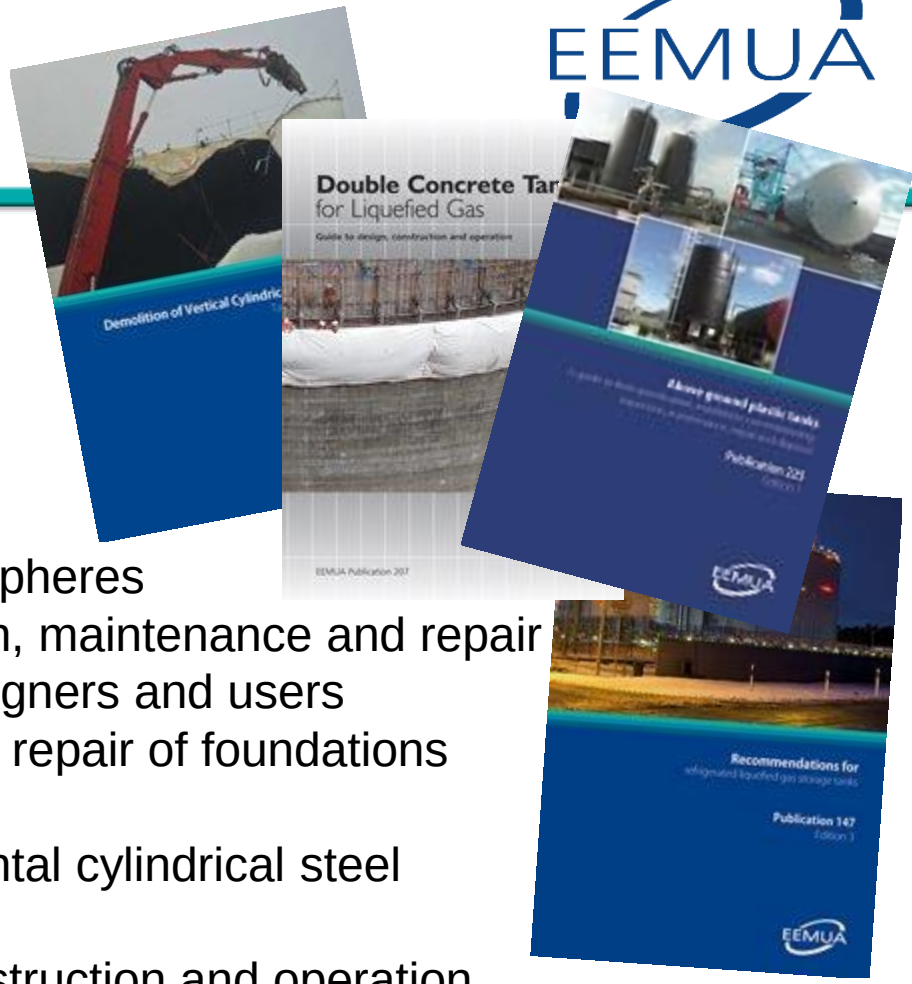




User centred approach

- Requirements
  - Usability
  - Safety
  - Performance monitoring
  - Investment in Engineering
- Achieved by
  - Designing to meet users' needs
  - Operating within users' capabilities
  - Being relevant to operating mode
  - Continuous improvement.

Any Questions?



www.eemua.org

* EEMUA 147 Recommendations for refrigerated liquefied gas storage tanks
* EEMUA 154 Demolition of vertical cylindrical steel storage tanks and LPG spheres
* EEMUA 159, Above ground flat bottomed storage tanks: Guide to inspection, maintenance and repair
* EEMUA 180 Frangible roof joints for fixed roof storage tanks: Guide for designers and users
* EEMUA 183 Prevention of tank bottom leakage - a guide for the design and repair of foundations & bottoms of vertical, cylindrical, steel storage tanks
* EEMUA 190 Guide for the design, construction and use of mounded horizontal cylindrical steel vessels for pressurised storage of LPG at ambient temperatures
* EEMUA 207 Double concrete tanks for liquefied gas – guide to design, construction and operation
* EEMUA 213 Emission reduction from oil storage tanks and loading operations
* EEMUA 217 Safe and effective operation of storage tanks for oil movements
* EEMUA 225 Above ground plastic tanks: a guide to their specification, installation, commissioning, inspection, maintenance, repair and disposal