Effective HMI Design for Safety-Instrumented Systems

Key Challenges and Requirements for Console Operator Situation Awareness

ASM 20+ YEARS

Dal Vernon Reising
Peter Bullemer
Human Centered Solutions, LLC
www.applyhcs.com

CCPS European Workshop on Process Safety
Keynote Presentation
28 Sep. 2015 / Nice, France

ASM 20+ YEARS

Presentation Sponsor

Abnormal Situation Management

Joint Research and Development Consortium

Founded in 1994

Creating a new paradigm for the operation of complex industrial plants

Developing solutions that improve Operations' ability to prevent and respond to abnormal situations

www.asmconsortium.org

bp

PHILLIPS 66

Honeywell

Human Centered Solutions
Helping People Perform

TEES MARY KAY O'CONNOR PROCESS SAFETY CENTER
TEXAS A&M ENGINEERING EXPERIMENT STATION

sasol
reaching new frontiers

NANYANG TECHNOLOGICAL UNIVERSITY

PENNSTATE 1855

Shell

TOTAL

UNIVERSITY OF ALBERTA

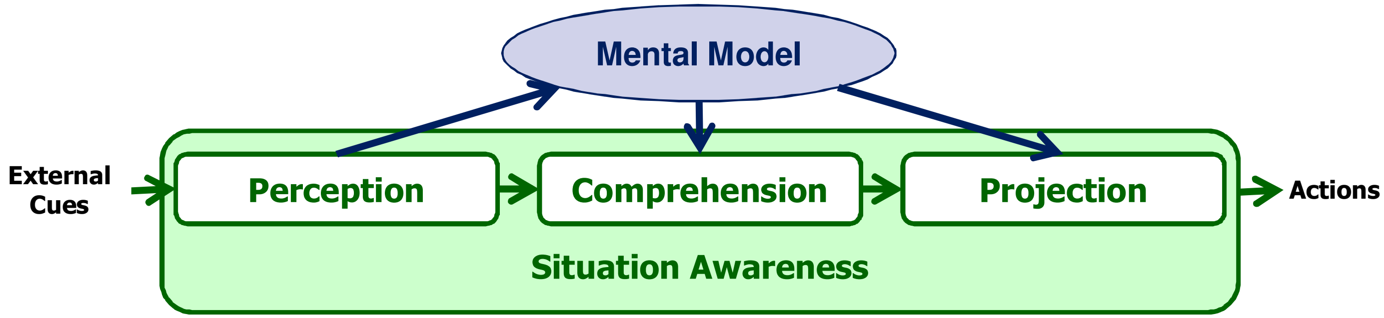
uop
A Honeywell Company

UCLA

Presentation Outline

- Introduction & Project background
- Project Methodology
- HMI Requirements
- Gap Analysis
- Conclusions
- Questions / Discussion

What is Situation Awareness

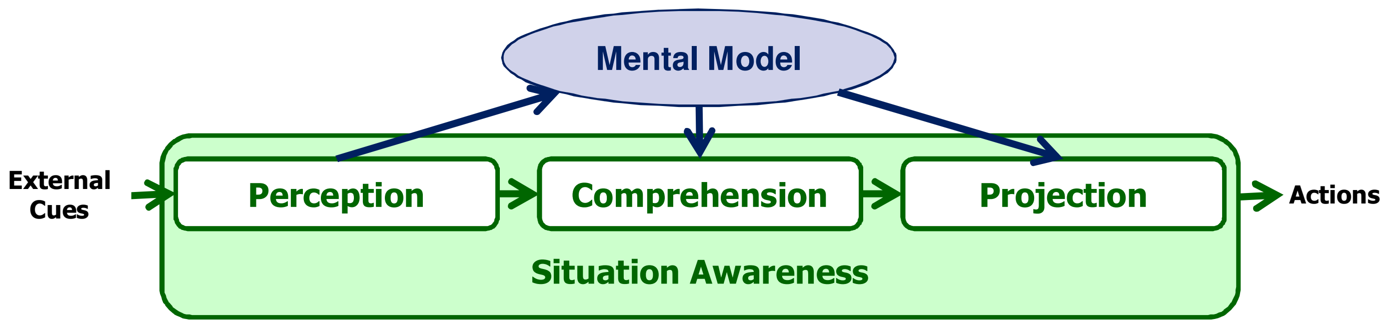


- Put simply, Situation Awareness is "**knowing what is going on round you so you can figure out what to do**" (Adam, 1993)

- Research in military and civil aviation has identified that problems with situation awareness were the leading factor contributing to:
  - Military aviation mishaps (Hartel, Smith & Prince, 1991)
  - Accidents among major airlines (Endsley, 1995)

Endsley, M. R. (1995). Toward a theory of situation awareness in dynamic systems. *Human Factors*, *37*(*1*), 32-64.

What is Situation Awareness



- **Level 1** SA = involves **perceiving** important information
  - Failure to perceive important information leads to the formation of an incorrect picture of what is going on
- **Level 2** SA = involves **comprehending** the perceived information with regard to specific job tasks and goals
  - Failure to accurately comprehend what is happening can lead to reasoning with an incomplete or inaccurate picture of what is actually happening
- **Level 3** SA = involves **projecting** where the situation is going
  - Failure to accurately predict what will happen can lead to initiating the wrong corrective actions

Project Motivation

- There is increasingly more extensive use of Safety-Instrumented Systems (SISs) in continuous process manufacturing plants
  - Greater challenge of presenting status and interrelations of the SIS elements on a day-to-day basis, in light of daily maintenance and production demands

- In particular, how to best support an operator's situation awareness of the SIS status and the risk profile in the light of maintenance overrides (MOs)
  - Daily decision-making activities for the operators in terms of
    - » how many MOs are in
    - » how many more MOs can be put in, both overall and in specific equipment areas
    - » what is the coverage of the changing protective envelope

Project Motivation

- Compounded by the common situation wherein the SIS and Distributed Control System (DCS) platforms are not seamlessly integrated
  - Neither physically or via the Console Operator's Human-Machine Interface (HMI) itself
  - Increases the complexity of simultaneously interacting with both systems in the event of a SIS trip or alarm condition

Project Objective

- Develop understanding of key challenges & requirements for the Console Operator's HMI for both
  - DCS & SIS that impacts an operations team's ability to
    - Operate within an expected safe envelope while faced with daily production and maintenance activities
    - Maintain situation awareness of the associated changing risk profiles

Study Methodology

- The study was conducted as a Practices Assessment of four ASM operating member sites
  - 2 sites were located in North America
  - 2 sites were located in the UK

- Assessed
  - Operator-reported challenges
  - Operator-reported use requirements
  - Current DCS and SIS HMI design practices

- Structured Interview format with Operators and Engineers around defined Use Cases

Use Cases

- Operational Scenarios (based on modes of operation or operator activity) were the basis for operator requirements analysis
  - Start of Shift
  - Corrective Maintenance
  - System Testing
  - Respond to pre-trip alarm
  - Verify trip effects
  - Determine trip cause
  - Conduct process unit start-up

Artifacts Assessed

- Collected and assessed
  - DCS operating display examples for equipment with SIS applications
  - DCS HMI design for the operator console
    - Overview display use
    - Operating display practices
  - SIS HMI design for the operator console
  - Maintenance override policies, practices & procedures
  - Trip response policies, practices & procedures
  - Start-up & Permissive management polices, practices & procedures

HMI Interaction Requirements

- Example Requirements definition
  - **Use Case:** Respond to Pre-trip Alarm

Operator Task	Operator Activity	Interaction Requirements
Detect pre-trip active alarm	• Confirm detection of active pre-trip alarm	• Provide control to silence alarm audible and indication of alarm acknowledge status
	• Identify alarm as SIS pre-trip alarm	• Provide indication of #SIS pre-trip alarms, their location and excursion direction (hi/lo) • Provide indication in alarm description that parameter is pre-trip alarm
Evaluate pre-trip alarm	• Determine current PV associated with parameter relative to alarm threshold	• Provide indication as to whether parameter is deviating significantly from other parameters in the voting logic (if appropriate)
	• Determine whether real process disturbance of instrumentation problem • …	• Provide indication of trip threshold for parameter and voting logic (if appropriate) • Provide indication of effects associated with the parameter in alarm

Overview of Requirements by Scenario

	Number of :		
Use Scenario	Operator Tasks	Task Activities	HMI Requirements
Start of Shift	2	4	6
Corrective Maintenance	3	7	21
System Testing	3	4	11
Respond to Pre-trip Alarm	2	7	9
Verify Trip Effects	2	5	7
Determine Trip Cause	2	3	7
Conduct Process unit Start-up	3	6	23

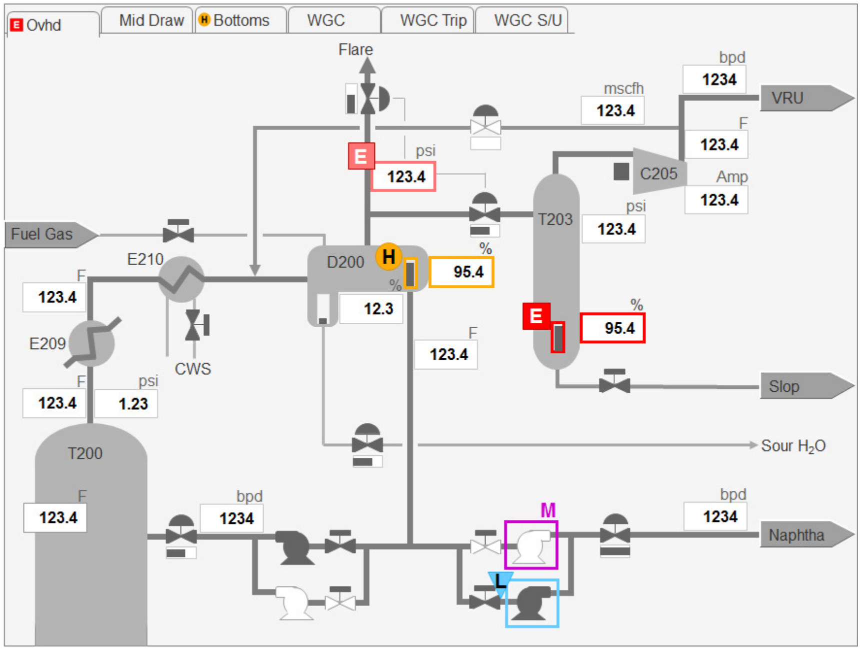
- The number of unique HMI requirements = **43**

HMI Display Formats Observed

- Three basic types of HMI displays were analyze against the HMI requirements
  - DCS operating displays
  - SIS 'Logic' diagrams
  - SIS 'Cause-and-Effect' matrices

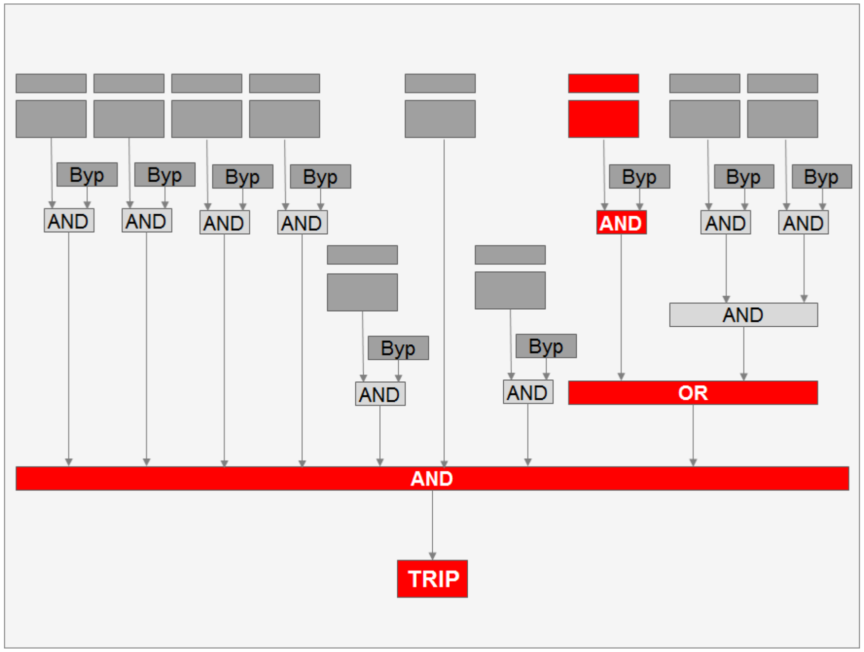
HMI Display Formats Observed

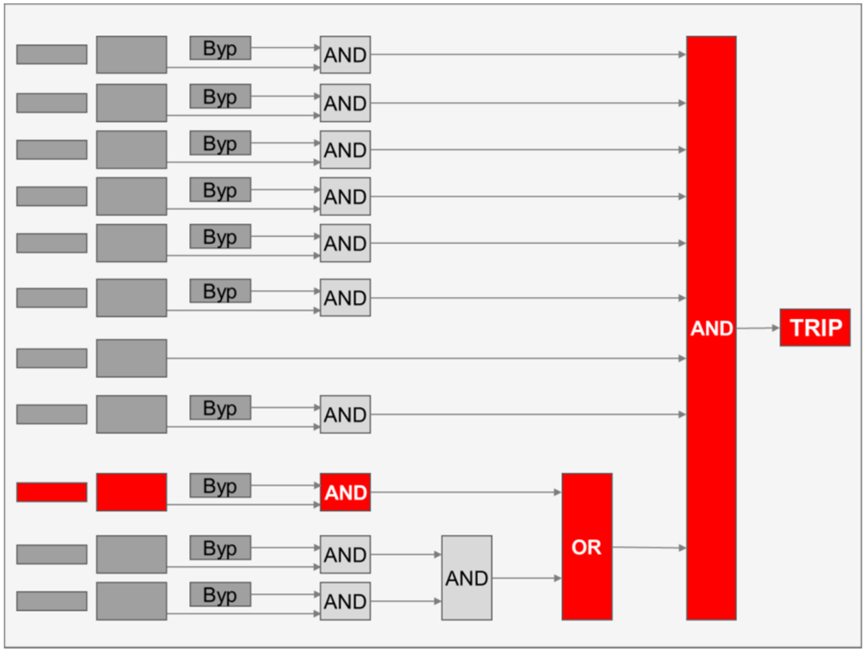
- Three basic types of HMI displays were analyze against the HMI requirements
  - **DCS operating displays**
  - SIS 'Logic' diagrams
  - SIS 'Cause-and-Effect' matrices



HMI Display Formats Observed

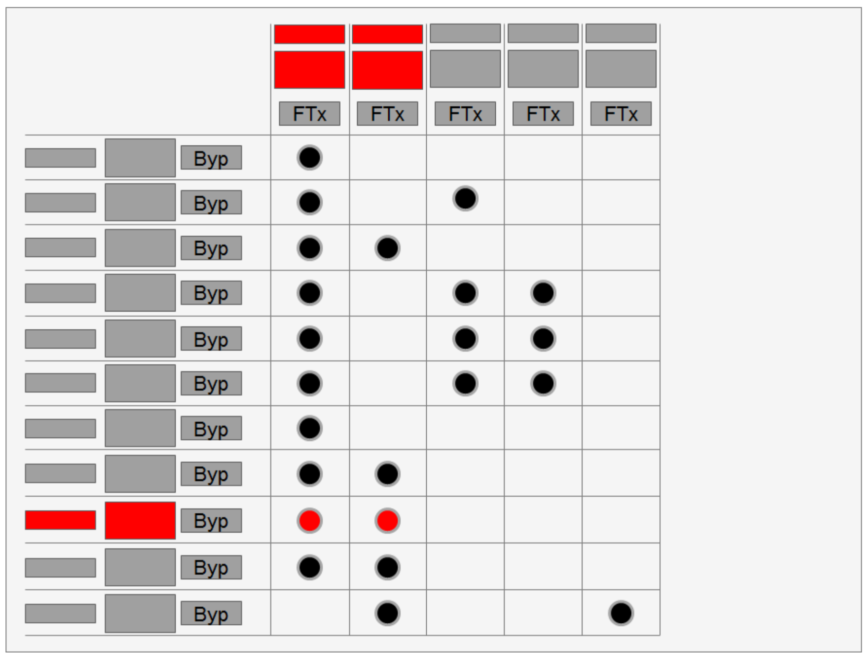
- Three basic types of HMI displays were analyze against the HMI requirements
  - DCS operating displays
  - **SIS 'Logic' diagrams**
  - SIS 'Cause-and-Effect' matrices





HMI Display Formats Observed

- Three basic types of HMI displays were analyze against the HMI requirements
  - DCS operating displays
  - SIS 'Logic' diagrams
  - **SIS 'Cause-and-Effect' matrices**



HMI Display Formats Observed

- Three basic types of HMI displays were analyze against the HMI requirements
  - DCS operating displays
  - SIS 'Logic' diagrams
  - SIS 'Cause-and-Effect' matrices

- In terms of practices observed, the project identified
  - **32** design features for **HMI DCS displays**
  - **80** design features for **HMI SIS displays**
  - **3** design features for **Console-mounted hardware**

  Note: More than one feature is typically required to satisfy the Interaction Requirements presented above

Best Practices Observed

- Best Practices observed for DCS HMI displays
  - In "typical" Process Flow / Piping & Instrumentation diagram formats
    - » SIS Elements included
      - **Isolation / Shutdown valves**
      - Indication that there were SIS **measurements associated with a DCS measurement**
      - Indication that a regulatory control **valve received input from the SIS**
      - Indication that the **commanded state was not achieved** (e.g., fail-to-close)

- Best Practices observed for SIS HMI displays indicated
  - » **Pre-trip and Trip limit** values
  - » **Voting logic** (e.g., 1oo2, 2oo3)
  - » Dynamic voting **logic as result of a bypass** (e.g., 2oo3 → 1oo2)
  - » **Active Bypasses** & their impact on the potential safeguards
  - » **First Out indications** for Trip initiation
  - » **Command-disagree status** on Effects elements (e.g., fail to close, fail to start)

Best Practices Observed

- Best Practices observed for HMI Start-Up displays
  - Showing **start-up steps** in sequence
  - Showing **permissive status** for the respective step
  - Permitting **bypass activation**, if required for step

- Best Practices observed for Alarm System design
  - » **Deviation alarms** between redundant SIS measurements
  - » **Deviation alarms** between a DCS measurement and the associated SIS measurement(s)
  - » **Pre-trip alarms** on DCS measurements for associated SIS measurements
  - » Alarms for **command-disagree status** for SIS effects

Past & Current HMI Short-comings

- Integrated HMI System
  - **An overview of where the process is** within the SIS envelope and movement towards an SIS boundary not clearly evident to operator
  - **SIS instruments not easily identified** within DCS HMI system
  - Lack of **HMI consistency** (SIS integration into DCS environment)
  - Not showing **SIS startup up timers, trip limits and permissive logic** in DCS displays
  - Not **providing first out capture** in the SIS
  - Not **transferring first out capture** information to DCS
  - Not **providing shutdown flags to DCS to position control valves** on an SIS trip
  - **Poor HMI representation and navigation** for State transition Logic, Sequential function logic, Voting Logic
  - **Poor Trending capabilities** for SIS inputs—either because those inputs are not historized or no standard trend link/access from SIS faceplates
    - » e.g., Operator forced to enter whole path to trend parameters

Past & Current HMI Short-comings

- Alarm System design
  - Not setting up **deviation alarms** between SIS and matching DCS measurements
  - **Poor alarm rationalization** between DCS and SIS
    - Many redundant alarms on inputs and effects (e.g., DCS pre-trip, SIS pre-trip, trip, motor shutdown, …)
  - Failure to generate **command-disagree alarms** to notify operator that a Shutdown or Trip has not been completed successfully
    - e.g., Shutdown Compressor Vent valve did not Open when commanded to Open
  - Not **transferring** SIS Pre-Trip and Trip **limits** to the DCS

- Some Positives:
  - **Integration** of SIS and DCS through the DCS HMI
  - **Transition diagrams** of the SIS logic in DCS
  - Access to **voter blocks** etc. via DCS

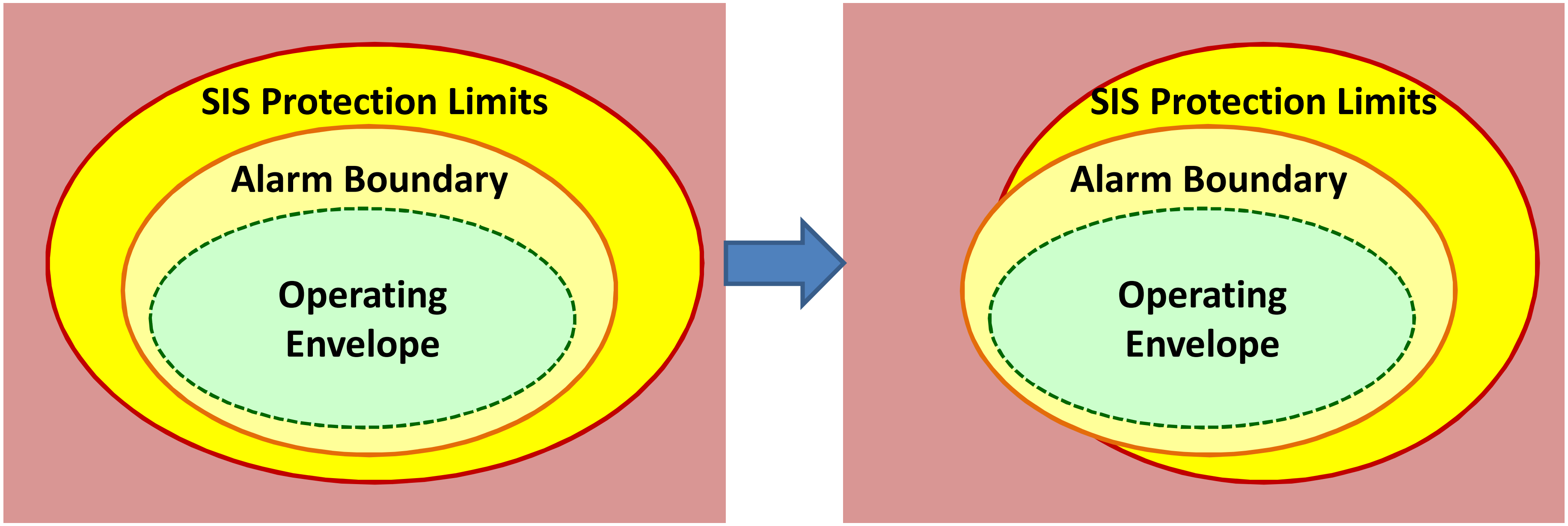
Task-Based Display Solution Required

- This research characterizes the value of identifying interaction requirements for supporting console operator use cases for different modes of operation to design HMIs that include SISs

- Moreover, an industry-typical HMI design format based on Cause-Effect matrices was demonstrated to typically address fewer of the requirements—only 37 of the 43—than a "Best Practice" Task-based layout designed explicitly for supporting operator decision-making and required actions
  - Emphasis needs to be added to non-Trip scenarios for the SIS lifecycle, such as maintenance, testing and start-up

Task-Based Display Solution Required

- Need for continued improvement of supporting "Big Picture" Situation Awareness of where and how close to the safety envelopes operators are working, particularly in the context of maintenance overrides / bypasses



Questions & Discussion

Please ask questions or offer comments

Questions & Discussion

Thank Your for Attending

- **Where to get more information**
  - ASM Consortium – www.asmconsortium.org

Tom Williams, Director

thomas.n.williams@honeywell.com

+1 (804) 536-2532

Dal Vernon Reising

dreising@applyHCS.com

+1 (734) 446-6977

Peter Bullemer

pbullemer@applyHCS.com

+1 (763) 972-2702