Safety & Automation System (SAS) - How the Safety and the Automation Systems finally come together as an HMI

By Ian Nimmo
President
User Centered Design Services Inc.

Abstract

Today we have clear guidelines on how the Safety Instrumented Systems (SIS) and basic Process Control Systems (BPCS) should be separated from a controls and network perspective. But what does this mean to the HMI and the control room design?

Where do Fire & Gas Systems fit into the big picture and what about new Security and Environmental monitoring tasks?
What does the Instrument Engineer needs to know about operators and how systems communicate with them.

The evolution of the control room continues as Large Screen Displays provide a big picture view of multiple systems. Do rules and guidelines exist for this aspect of independent protection layers? What are today’s best practices for bringing these islands of technology together.

This paper will review the topic and provide advice on a subject on which the books remain silent. Today’s practices are haphazard and left to individuals without a systematic design or guidance.

Over the past 20 years the Safety System and the Automation system have been evolving separately. They use similar technologies, but the operator interface needs to be just one system. Unfortunately, due to the nature of the designs, this is not the case.

The automation system has been evolving since the introduction of the DCS and many Human Factor mistakes have been made. As we move towards new standards such as ISA SP 101 a more formal approach to HMI design is being taken.

The past widespread use of black backgrounds which cause glare issues in the control room and are solely responsible for turning the control room lights down to very low levels, or in some cases off, are being replaced with grey backgrounds and a new grayscale graphic standard replacing bright colors for a more plain grayscale scheme only using color to attract the operators’ attention.

In having strong compliance schemes that restrict color usage to just a handful of colors, restricting the use of some colors that are reserved for important information such as alarm status, it appears that the automation system is being standardized and is starting to take advantage of new technology available to control room designers such as large screen displays.

As the Automation HMI progresses the Safety System HMI has not been evolving at the same pace or with any coordination. The systems are often from different suppliers or even within one supplier they are treated as different product lines and no coordination has been provided to harmonize the designs.
The Safety System has used different techniques to display logic status from PLC type Ladder Diagrams, traditional Flow Charts, Logic Diagrams, which may or may not be viewed through the DCS screen as an independent window.

We recognize that maintaining the integrity of the safety system is the first priority so the Automation Systems and DCS have been limited to view or read only access. This is a sensible step; however, providing the operator with multiple HMI’s with different coding is not a good idea.

When we consider the Safety System we often think of Shutdown Systems like Triconix, but we must also consider Fire & Gas Systems (overview & alarm), Burner Management Systems, and Hardwired Critical Alarm Systems that are independent of the Automation System.

With the advent of Large Screen Displays (LSD) and Video Walls, we now have the opportunity to provide a common HMI, therefore it is important that each of these systems is controlled by a common philosophy and style guide.
### Visualization of LSD during Normal Operations

<table>
<thead>
<tr>
<th>CCTV</th>
<th>CCTV</th>
<th>F&amp;G level 1</th>
<th>Alarm list</th>
<th>User defined</th>
<th>FAS</th>
<th>CCTV</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td></td>
<td>Process overview</td>
<td>Process overview</td>
<td>Process overview</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

### Visualization of LSD during Emergency Operations

<table>
<thead>
<tr>
<th>CCTV</th>
<th>F&amp;G level 2</th>
<th>F&amp;G level 1</th>
<th>Alarm list</th>
<th>ESD status hierarchy</th>
<th>ESD blowdown</th>
<th>CCTV</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td></td>
<td></td>
<td>ESD status area</td>
<td>ESD status area</td>
<td>ESD status area</td>
<td></td>
</tr>
</tbody>
</table>
Shell Orman Lang Control Room

1 Photographs and screen layout courtesy of Mark Green – Human Centered Design - Norway
Physical Equipment Layout

Emergency Operations
In the North Sea, the Norwegian Norsok Standard 1-002 Safety and Automation System (SAS) has done a great job in bringing the technologies together into a single system. They define the SAS as “the overall Safety and Automation System. SAS performs monitoring, logic control and safeguarding of an installation. SAS comprises all control equipment as a total, integral concept, either from one vendor or acquired from several sources. Subsystems made as stand-alone units communicating through custom made serial links are also considered as part of SAS.

SAS unit consists of CPU with associated equipment such as I/O racks and cards, bus communication, power supplies, signal conditioning units and termination facilities for field cables. Operator stations and gateways are also considered as SAS units.

System Topology Principles as shown below are applicable independent of the SAS size and complexity.
Conceptual SAS Topology

ESD = Emergency Shut-Down System
F&G = Fire & Gas System
IMS = Information Management System
PDCS = Power Distribution Control System
PCS = Process Control System
PSD = process shut-down (system)
The Norsok standard implies commonality in the HMI’s for all the individual systems as it treats all the units as an entire system. This is a major step forward from current practices in the rest of the industry which allow projects to do the integration by placing orders on different vendors and accepting their solutions to each of the individual system solutions. A good project may specify standards per company requirements, however, this is often rare and, if done, it is often done independently of a common philosophy for termination, integration, performance and HMI.

The Norsok Standard addresses all these issues and even defines a testing strategy and time responses:

The SAS vendor(s) shall have available test and/or simulation equipment for the I/O configured. Facilities for measuring of dynamic loads of SAS unit, communication system and Operator Station shall be made available by the SAS vendor(s).

The tests shall be performed hierarchically, starting first SAS unit tests, then system tests and finally the integration test.

All tests shall be documented. All I/O’s shall be tested from the field side of SAS unit(s).

**SAS unit test**
Complete test of hardware and software applications of all SAS units, including applications on Operator Station. The tests shall be performed in accordance with approved test procedures.

**System test**
Several SAS units forming a system shall be tested together. All I/O shall be simulated. System test shall include all inter-unit signals.

**Integration test**
The test shall cover complete SAS including simulation of Control class 2 equipment. In addition to functional test of all systems, dynamic bus and CPU load shall be measured. System fault monitoring shall be tested. The SAS should be alarm and failure free for at least 24 hours.

**Time response**
The system shall be designed to meet the following performance requirements. All requirements are related to 1 second cycle time.

Operator command
2 sec. for acknowledgement of alarms on the operator station (measured
from operator action until acknowledgement is observed on the operator VDU).

Operator command
2 sec. from command to field action (measured from operator action until output card/channel has reached new state).

Closed loop control
Max. 2 sec. from input to output action, i.e. from input signal/ IO module to output signal/ IO module (measured at I/O card terminals). For special control functions shorter cycle time may be necessary in order to fulfil function requirements.

Alarm display text
2 sec. from alarm limit is reached

Picture update
Max. 2 sec. to complete picture on call up for picture containing 100 variables (dynamic objects).

Picture dynamic update
Max. 2 sec. for dynamic objects on picture to show input state/value (measured from input signal I/O card terminals until dynamic point shows same state/value)

ESD initiation from F&G
Max. 4 sec. from confirmed F&G detection to activation of ESD outputs (measured from F&G input signal is in alarm state until ESD outputs are activated).

The time response requirements apply also when the information is transferred via serial communication to/from control systems not fully integrated in SAS.

When utilizing link for data transfer, this link shall not degrade the system performance as if utilizing hardwired I/O (i.e. I/O transmitted by use of serial communication to be treated as if hardwired I/O were utilized).

We have many systems that are intended to provide the operator with status information and, when required, diagnostics to allow the operator to resolve problems. This technology-centered design solution creates a major problem with operator situation awareness.

It focuses on providing data associated with the equipment. It is designed for technology-centered design that takes traditional sensors and systems that are needed to perform functions, then added a display for each system that informed the operator of how well that particular system was operating or its present status. As the design evolved systems kept on being added until the operator displays grew exponentially.

The operator was expected to be able to find, sort, integrate, and process through the vast array of information available, leading inevitably to an information gap. It was never even considered that the human has limitations and that the human could become the bottleneck. As the display of data in these systems is centered on technologies producing
them, it is often scattered and not ideally suited to support human tasks as Mica R. Endsley’s book “Designing for Situation Awareness: An Approach to User-Centered Design” defines.

An alternative was never considered. Engineers were aware that in the old days when they first started instrumentation, they had panels with instruments mounted on them. The instruments were arranged around the operator’s tasks so that the operator would not have to run up and down the panel every time they had to do a task. This was a better solution, though it had limitations in that the panel only had a certain amount of room for equipment and change was a difficult task, so was adding new equipment once the design was complete (built in MOC).

However, user-centered design goes much further than this basic concept of task grouping. It considers displaying information in ways that fits the goals, tasks and needs of the user. It strives to achieve optimal functioning of the overall human-machine system rather than information centered on sensors and the technologies that produce it.

One of the first barriers that Endsley defines is understanding what user-centered design is not. This is going to be hard for many engineers, because over the years of developing HMI and graphics, the engineer learned that the operator often had more insight into what was a good graphic than what they were producing, therefore, they either left the design entirely to the operator user or sought operator input into what the graphic should look like. This sounds very reasonable but has been found to be fraught with pitfalls and could be considered a poor practice.

Endsley brings out some important points that should be considered. The first is that operators often have only partial ideas about what might be better than what they are used to. They generally have very limited knowledge of how to effectively present information and design human interactions with complex systems.

The next is that these issues are compounded by the fact that most systems must be used by many different individuals, each of whom may have significantly different ideas on what they would like to see implemented in a new design. The result of this approach is an endless and costly cycle of implementing new ideas, only to have the next team of operators decide they want something different. Design solutions tend to be sporadic and inconsistent across features of the interface and many design problems are not recognized.

The best operator on the unit is often seen designing graphics and although much good thought has gone into the design, inconsistencies can be seen, such as poor use of colors, not reserving colors for coding or using colors for multiple codes, many more than most operators can memorize. Also poor layouts and cramped information are an attempt to get everything that could be possibly be of value onto the display.
Endsley is not saying that the operators do not have valuable input; in fact she states that operators are a valuable source of input providing information regarding problems experienced, information and decision needs, working conditions and functions needed. The unfiltered implementation of whatever they want completely neglects the large base of scientific literature regarding the types of interfaces that work and those that do not.

That is the big one out of the way. The next idea she discusses is the well-meaning attempt to help manage the information overload problem is the idea of information filtering or trying to anticipate the information needed by the operator. The bottom line of this approach is that it puts the operator back in a reactive, rather than proactive operating stance, and influences the performance of both the operator and the system. Finally, her comment is that user-centered design is not making decisions for the operator or doing things for the operator. So what is it? The answer to that question can be found in the book itself.

The operator has quite a task monitoring all the multiple systems which often includes environmental monitoring (flares), CCTV for security and personal safety.

The use of the LSD is an enormous benefit allowing the big picture back into the control room and the ability to display the most critical information helping to reduce tunnel vision and allowing a shared view to others who may be able to help or provide advice.

In light of the new developments of the operator HMI we must consider the physical environment from lighting, the console ergonomics, the number of screens and keyboards and the other physical equipment such as pushbuttons, lamps and indicators.

The situation awareness model also considers distractions, the impact and reduction of stress, fatigue, noise including alarm annunciation, use of mental models, the operator’s memory limitations, attention tunneling, data overload, misplaced salience, complexity creep, and most importantly the out-of-loop syndrome.

We have a great resource in the International Standard ISO 11064 Ergonomic Design of Control Buildings.

However, we will never get to the solutions identified in the standard unless we make each individual system we install a part of a bigger picture. What the Instrument and Control Engineer must realize that anything that requires any operator involvement must be controlled by the common operator HMI philosophy and follow the rules of information presentation as do all the other systems installed.

We have a tradition in industry. Our Engineers excel at implementing standards. We are good at interpreting guidelines but will always take the easy and cheap solution. If no guidance is
provided we do a terrible job and we lack professionalism as demonstrated by previous control room design Alarm Management and many HMI designs.

It is important that every Engineer that does instrumentation and controls be familiar with the International Standards and ISO 11064 in particular. They should understand the principles of User-Centered Design. Be fully aware of the practices for good situation awareness.

The automation and safety systems community need to come together to define a standard for Safety and Automation Systems similar to the Norsok Standard.

Each plant, each operating unit, each individual piece of equipment should be covered by a HMI philosophy and style guideline.

If we are to pursue a policy of safe automation we must address the biggest issue effecting our industry and drive Human Error out. This can only be achieved by having workable standards written by our Country and our industry.

We are 20 years behind in this pursuit and must respond immediately and effectively, we are already 10 years behind the Norwegian industry, and we have the worst track record for catastrophic disasters than any other country in the world associated with the use of this technology.

Ian Nimmo
inimmo@mycontrolroom.com
www.MyControlRoom.com
Tel 623-764-0486
President User Centered Design Services Inc.