Human machine interface (HMI) developments in HAMMLAB

SVENGREN Håkan [1], HURLEN Lars [2], and NIHLWING Christer [3]

1. OECD Halden Reactor Project, Institute for Energy Technology (IFE) P.B. 173, NO-1751 Halden, Norway (E-mail: hakan.svengren@hrp.no)
2. OECD Halden Reactor Project, Institute for Energy Technology (IFE) P.B. 173, NO-1751 Halden, Norway (E-mail: lars.hurlen@hrp.no)
3. OECD Halden Reactor Project, Institute for Energy Technology (IFE) P.B. 173, NO-1751 Halden, Norway (E-mail: christer.nihlwing@hrp.no)

Abstract: In this ongoing project a complete set of 30 inch operator work-station screens and two common large screens have been developed and implemented based on experience from a number of lab experiments and usability tests in HAMMLAB (Halden Man-Machine Laboratory). A state-based alarm system is developed as an add-on to the normal alarm list to reduce the amount of alarms when protection signals are activated. A computerized procedure system is included to improve team transparency, reduce the time to perform procedures and to minimize the risk for erroneous operations. A full evaluation of the design is planned to be conducted spring 2015.

Keyword: alarms; computerised procedures; human-machine interface

1 Introduction

Over the last years parts of the nuclear industry has moved towards replacing the traditional, panel-based interfaces with computerized Human System Interfaces (HSIs). Such decisions are motivated by aspects such as future maintenance problems, cost and upgrade flexibility, and not so much by human performance issues. In general, today's computerized control rooms consist of Process and Instrumentation Diagram (P&ID) -based process displays, backed up with traditional trend and alarm systems. There is however a general consensus that there is a great potential for improvement with regards to how information is being presented in such systems.

The goal of the Halden Project is to provide the nuclear industry, i.e. utilities and vendors, with knowledge and ideas for improving information presentation in hybrid or fully computerized control rooms. This goal is being met by designing prototypes which is implemented in full-scope nuclear simulators, evaluating them in user tests and larger-scale experiments in HAMMLAB, and providing lessons learned, design recommendations and technical basis for guidelines to the industry.

Among the concepts that have been developed in Halden are ecological interfaces, task-based displays and function-oriented displays. Many of the concepts go far beyond traditional P&ID type displays, and utilize advanced computer graphics and animations to support operator performance. Experiments and usability evaluations have been performed utilizing licensed nuclear power plant operators, and both subjective and objective data has been gathered during the evaluations.

This paper focuses on an ongoing design project called Innovative Human-System Interfaces for Near-Term Applications. By near-term we mean to address current plants with familiar concepts of operation and that the solutions proposed should be mature enough for near-term deployment. The purpose of the project is to design, and later make a full Human Factors evaluation, of an integrated Human System Interface, which includes Large Screen Displays (LSD), Operator Workstation Screens (OWS), Computer-Based Procedures (CBP), and alarm system and other task oriented support, based on a unified design philosophy.

The design presented in this paper is implemented in the Halden Reactor Project (HRP) Boiling Water Reactor simulator using IFEs HSI tool "ProcSee".

Received date: September 15, 2014

The simulated plant is a Swedish ABB plant with internal recirculation pumps, which was connected to the grid for the first time in 1985, and the thermal reactor power is 3300 MW.

We normally involve operators from the simulated plant or other Swedish plants in experiments and usability tests, therefore the text in the displays are in Swedish language. A full evaluation of the design is planned to be conducted spring 2015.

The HAMMLAB control environment is designed to support a shift-team consisting of a minimum of:

- one reactor operator
- one turbine operator
- two field operators
- one shift supervisor

This paper addresses challenges of computerized interfaces, and how this design project contributes to solving some of these challenges.

2 Challenges and opportunities in computerized HSI

The present generation of computerized interfaces within the nuclear industry is more or less screen-based replicas of the traditional mimic-based hard-panelled interfaces. Although a natural first step, this approach introduces new challenges from a human factors perspective. Generally, it also fails to take full advantage of the new possibilities the new digital medium offers.

As discussed in a related paper from HRP[1] some of the known challenges with present computerized HSIs are:

- *The "key-hole effect":* In traditional control rooms the interface covers a large part of the room's walls and desks. In computerized environments the operator's interface is located on a number of computer screens. The result is that operators often loose overview of the complete process. The interface fails to support the behaviour of "stepping back" to get the "big picture", focusing exclusively on smaller parts of the process, screen by screen, as through a key-hole.

- *Interface management issues:* As the interface is distributed over many displays limited in size, operators will have to navigate through them to access the information they are looking for. The display shown on each screen is chosen by the operator, e.g. mimic-based displays, trends, alarm systems, *etc*. While this flexibility offers some advantages, studies have shown that operators may lose overview and increase their workload resulting from the need to manage screens when looking for particular information.

- *Visual patterns disappear:* A key feature of traditional panel-based control rooms is that analogue display elements are spatially distributed throughout the room (analogue meters, tile-based alarms with a single lamp representing a single alarm, *etc*.). These and other analogue display units seem to better support fast recognition of overall process status than is the case in their computerized counterparts (numerical digits, alarm lists, *etc*.). For example: Four arrows pointing at 12 o'clock and a number of alarm tiles lighting up in different places in the control room (often with sounding alarms coming from different locations as well) are more rapidly and accurately interpreted than mere numbers and lines of text appearing on a screen.

- *Teamwork transparency:* In a traditional control room it is easy for operators and the shift supervisor to see what others are doing. As every element in the interface has a fixed location operators may conclude with a certain accuracy what colleagues are doing simply by noticing where they are in the control room. In contrast, in most computerized environments the actions of others are often not that evident. Operators are located at desks, acting on displays that are not easy to read from a distance. This reduces each team member's

awareness of others' actions, making coordination more difficult.

The motivation behind all the HSI concepts explored at the HRP can be captured by a few design objectives for ensuring plant safety operation in all plant states: Increase situation awareness, reduce workload and improve team collaboration. These objectives have led us to propose an HSI with main characteristics described in the following sections.

3 Design of large screen displays (LSDs)

By introducing a well-designed LSD many of the challenges mentioned in section 2 can be solved.

Ideally the information at the LSD should include normal operation, disturbances and emergency situations. The reason for that is to show the information on a fixed place in all situations. We have developed a control room vision, illustrated in Fig. 1. There the LSD is showing an overview of the whole process during all plant states. At both ends of the LSD the active Operator Workstation Screens (OWS) of the reactor- and turbine operators (as detected by the location of the mouse pointer) is projected to increase the team transparency. There is also a dedicated space to project any user defined OWS or other information. In the middle there is an alarm summary and the status of protection systems.

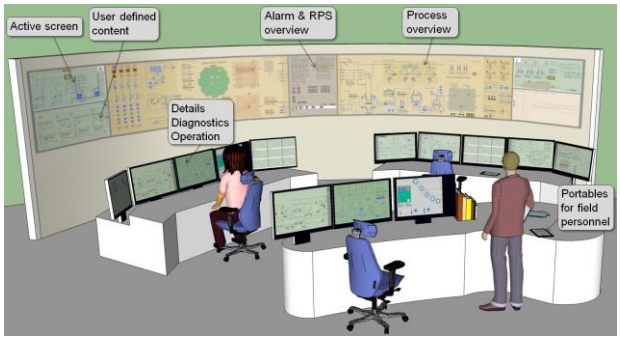


Fig. 1 The projects vision of a computerized control room.

However in HAMMLAB there is limited space to build LSD large enough to include the whole vision (the current LSD is 6.0 meter wide and 1.55 m high with 4200x 1050 pixels). Therefore one LSD is implemented to be used for normal operation and in all disturbance situations when Emergency Operating Procedures (EOP) is not needed (called LSD normal). When selecting an EOP the LSD will change automatically to adapt for the emergency situation (LSD EOP). In addition there is a LSD for use only during outages described in section 3.2.

These LSDs are mainly designed to support a shared process overview, while actions are done from OWS.

3.1 Description of LSD normal

Roughly the LSD normal shows:

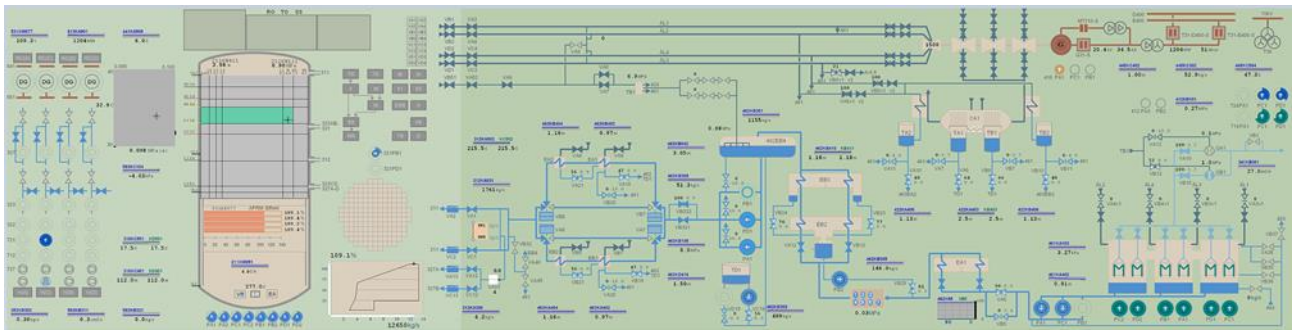
- Status of reactor- and turbine protection system
- Status of safety systems
- Main parameters in Reactor Pressure Vessel (RPV) and containment
- Control rod position
- Balance of plant systems
- Alarm status

Figure 2 (a) and (b) show the LSD normal in two different situations: (a) the LSD at normal full power operation, while (b) the LSD when Reactor Protection Signals (RPS) are activated due to a leakage inside the reactor containment. In addition to this case, there are some other simulated malfunctions in safety systems.

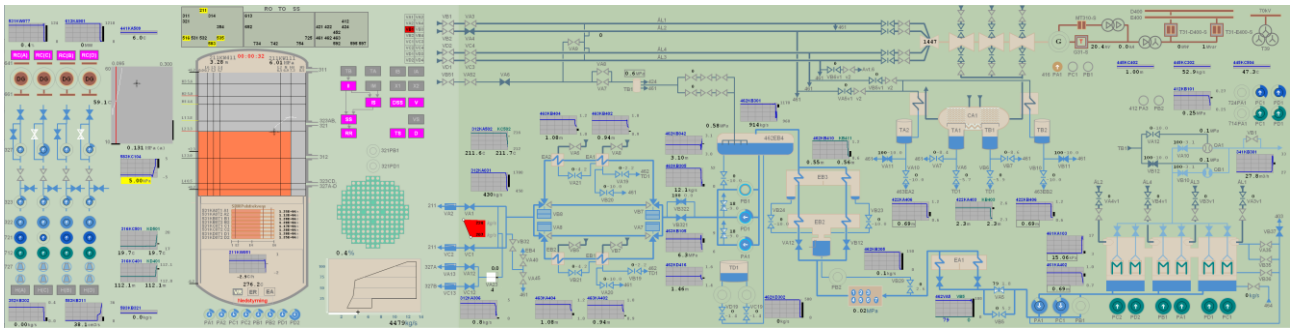
In order to reduce the need for reading digital values and remember normal values depending on the plant status and reactor power, the proposed LSD prominently features graphical process symbols in addition to the digital values. This way operators can easily get an at-a-glance overview of the process, and quickly notice any deviances from the expected state.

System flow after pumps are visualized by using a circular sector partly hidden of the pump symbol. See Fig. 3.

This principle is also used to show the speed of pumps and power produced by generators.



(a) LSD at full power operation and no active alarms.



(b) LSD when reactor scram, containment isolation *etc.* has been activated depending on a leakage inside the reactor containment.

Fig. 2 Two pictures of LSD normal in two different situations.

Fig. 3 Combined pump status and flow from the pump.

This graphical representation also supports operators in getting a quick overview of the most important safety systems after an actuation of reactor protection systems. In Fig. 4 the safety systems are shown in normal stand-by to the left, and after actuation of (RPS) RC to the right. Note that the operator does not need to remember what the nominal flow is and does not need to read any digital values or meters to check the status of these systems. System numbers are displayed to the left and the sub divisions are organized in four columns in order A C B D according to the plant safety concept. In Fig. 4 all four emergency diesel generators have started but only sub B produce power to the diesel backed bus bar. Intermediate cooling pump 721 PC1 has no flow. Residual heat removal pump 322 PD1 has a malfunction.

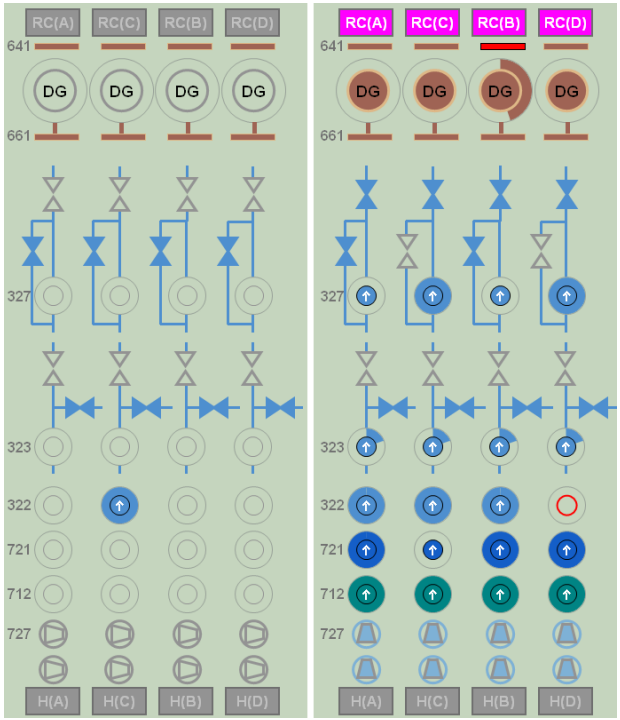


Fig. 4 Overview of the most important safety systems, before and after actuation.

The RPV is shown in Figure 5. The black cross in the green area is an operating point developed by combining the water level and pressure signals. This

makes sense due to saturated steam in a BWR where changes in pressure affect the water level and vice versa. Green indicates the target area for normal operation. The horizontal lines are alarm levels for the water level and the vertical lines are alarm levels for pressure. If the operating point leaves the allowed area the color will change. The white line shows the history to make it easier for the operator to understand what have happened and predict the future. Below is the neutron flux shown with eight bar-graphs.

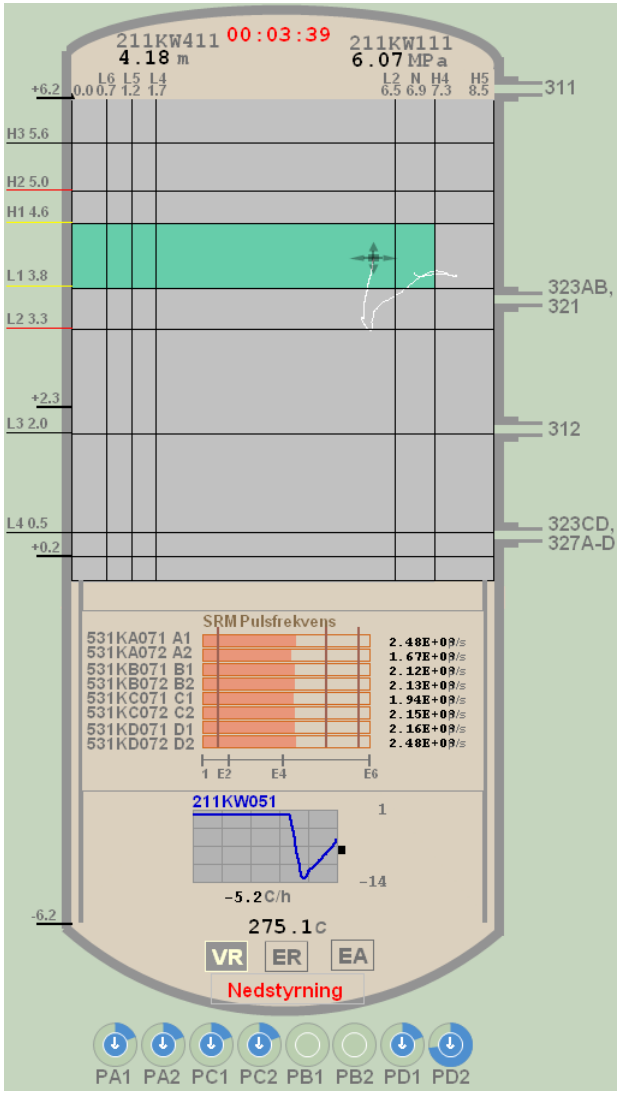


Fig. 5 The RPV (BWR).

Below the RPV is the eight internal circulation pumps shown. The outer circle shows the speed of the pumps. In Fig. 5 the speed is reduced to minimum due to a simulated LOCA. Without reading a single numerical process value operators can easily detect that the pump PD2 has not reduced the speed, and PB1 and PB2 have stopped.

To further support quick overview of the process, mini-trends are utilized to show the most important process values. A mini-trend shows the last 10 minutes and is auto-scaled. Auto-scaling means that the measurement area/scale that is displayed is automatically determined so that even small deviations are easily detectable.

If there is only very small changes of the process values during 10 minutes the mini-trend will be visually minimized.

During normal operation the process is very stable and the minimized trends allows for a calm and organized overview, making it easy for the operators to check at-a-glance that everything is normal. If something is not normal the mini-trends "pop out" to normal size, which is easy to detect, as seen in Fig. 6 where 463KB404 is the name of the measurement and 1.08 m is the actual value. The visible scale is shown to the right. The little black bar graph shows how much and which part of the scale that is visible. There are totally 35 mini-trends in the LSD normal.

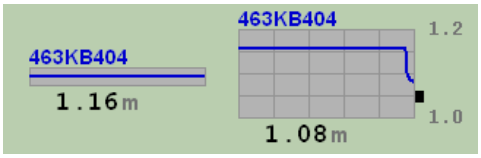


Fig. 6 Minimized and normal size of auto scaled mini-trend.

To illustrate this behavior, Figure 7 shows a part of the main feed water system at normal full power operation when all mini-trends are minimized. In Fig. 8 an external leakage has started in containment from one of the main feed water lines and two mini-trends have increased to normal size due to higher feed water flow.

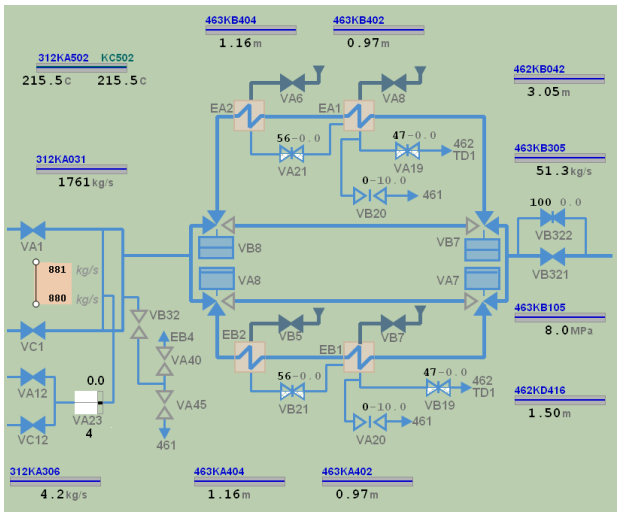


Fig. 7 Minimized size of mini-trends to help the operators at-a-glance check that the main process is ok.

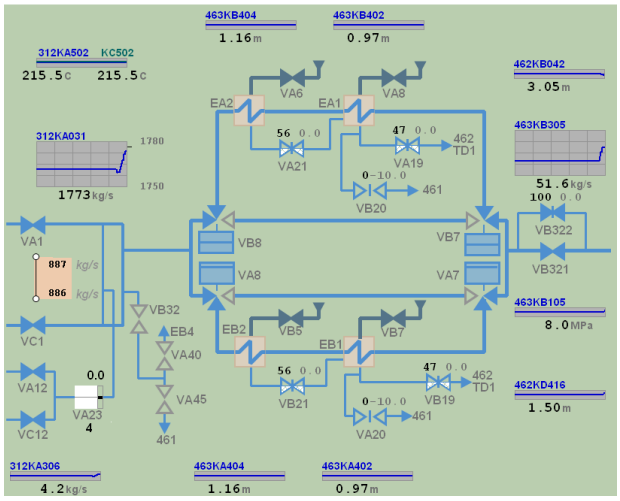


Fig. 8 Two mini-trends increased to normal size to help the operators to detect the deviations.

The status of the reactor containment is supervised by sensors to detect for example leakage. To make it possible to detect from which line the leakage has originated a symbol compares the flow in the two main feed water lines. Normally the flow should be the same in both lines. If the flow differs too much the symbol will change and indicate leakage. See Fig. 9.

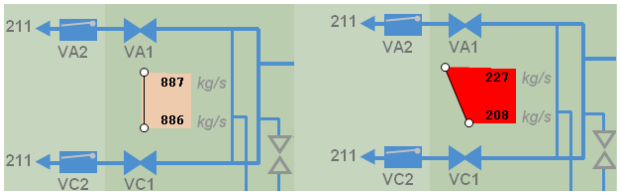


Fig. 9 The two main feed water lines at normal full power to the left and showing a leakage in the top line in right picture.

3.2 Description of LSD outage

During the outage a lot of signals are tested and many systems or part of system are taken out for maintenance. It is challenging for the operating team to keep all system ready for operation according to Technical Specification, in particular the section "Limiting Condition for Operation" (LCO). Therefore an automatic supervision of the LCO and an automatic supervision of the status of safety system are connected to the LSD. This part of the LSD is shown in Fig. 10.

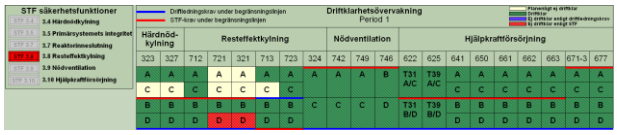


Fig. 10 Visualization of the supervision of LCO and the status of safety systems according to planned maintenance.

To the left is shown the six chapters of the LCO that is supervised. It is emergency cooling, the integrity of primary system, reactor containment, residual heat removal, emergency ventilation and electricity supply. Signals from the process and some manual input from local measurements are used as inputs to the logics that supervise the LCO. See Fig. 11.

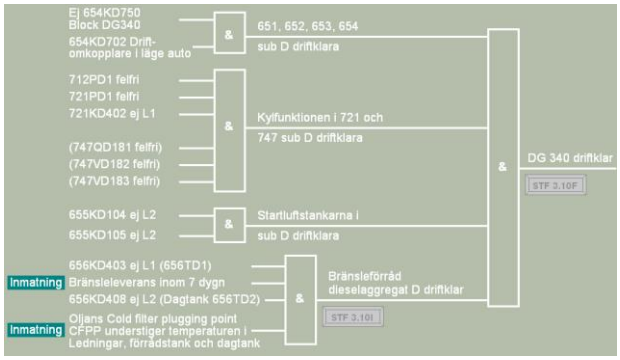


Fig. 11 Supervision of one diesel generator (DG 340). Input signals to the left. Manual input is needed for to signals e. g. specification of diesel fuel.

The diesel generator is input to diesel backed bus bar and the bus bar is input to different safety components. If any requirement is not fulfilled there will be an alarm indication presented on the LSD. The operator can easily check the root of the problem by checking the logics on his OWS. See Fig. 12.

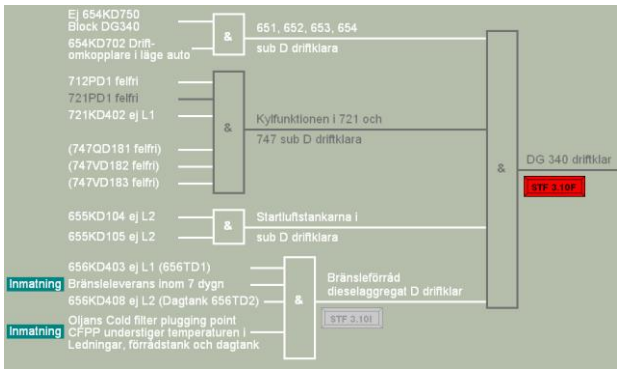


Fig. 12 Cooling pump 721PD1 is not ready for operation and the diesel generator DG340 is not available.

To the right in fig. 10 shows the automatic supervision of the status of safety systems. A part of this is shown in Fig. 13. Sub divisions below the red line should be ready for operation due to the LCO and outage planning. If the management decide to have more margins it is possible to use a blue line showing additional requirements. Each system and sub division is supervised individually. A sub division not ready for operation is shown by color coding. Yellow color indicates that that sub division is taken out for maintenance as planned. Red or blue gives a separate alarm sound and indicates that a sub division is not ready for operation as planned. After the maintenance work on sub A and C is finalized these need to be tested and be put back into operation before entering the next period. Then, sub A and C should be ready for operation and will be put below the red line.

Fig. 13 Status of safety systems due to planned maintenance and requirements in LCO.

The remaining part of the LSD outage is focused on safety systems and residual heat removal. It is presented with the same philosophy and symbols as the LSD normal.

4 Design of operator workstation screens

To avoid too much navigation and reduce the key-hole effect the OWS are quite large. The format is 30 inch and the resolution is 2560 x 1600 pixels.

Reactor- and turbine operator have five OWS each. The shift supervisor has four OWS.

All process displays have some common functions e.g. navigation, selecting and maneuver components and presenting information. Fig. 14 shows a typical OWS. Navigation buttons are placed in the row at the bottom, top and integrated in the displays to make it easy to locate the desired process format. With this scheme we have ended up with a total of about 15 main process screens which are all “one click away” for the reactor side and about the same for the turbine side. When pressing and hold the left mouse button down a pop-up menu will appear and more detailed information about the systems can be selected.

The process mimics are harmonized with similar representations used by the operators (such as P&ID diagrams) in order to ensure familiarity and reduce the risk of misunderstandings.

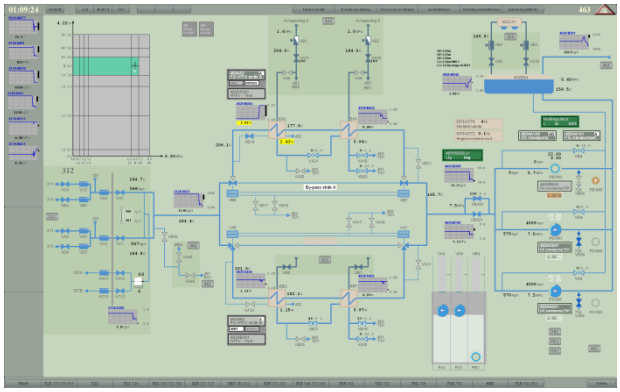


Fig. 14 Typical process display showing main feed water system. High water level in one pre-heater has actuated pre-heater by-pass.

Innovative process graphics such as diagrams, ten-minute auto scaled mini-trends, visual pump-symbols and other ways of visualizing process information or functions are integrated into the displays to supplement the traditional mimics.

In Figure 15 parts of two trains in the residual heat removal system is shown. Cooling systems 712 and 721 are simplified (detailed information is found in another display) shows only the status of the pumps and flow from the pumps. The cooling function is shown by presenting the temperature before and after the heat-exchanger by using bar graphs. If the bar graphs show the same value the cooling function is not working, and the operator can check the cooling function without reading digital values.

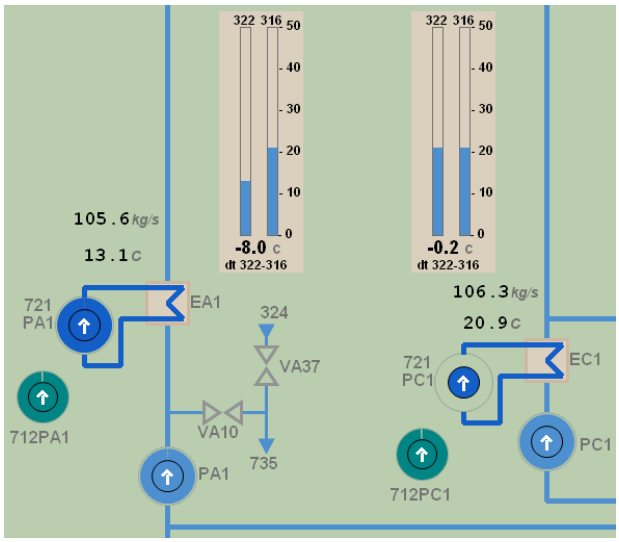


Fig. 15 Part of the residual heat removal system visualizing the cooling function.

Alarm information is also integrated in the operator workstation screens as well as on a dedicated Alarm overview display (see also section 5). All screens and plant manipulations are made accessible from every display to support adaptable reconfigurations of team structure. Also, computerized procedures will be utilized (see section 6) to guide the user from screen to screen during most control activity, and thus further reduce necessary interface management tasks during high-workload situations.

To help the operators to supervise the process and handle disturbances proactively the displays feature integrated mini-trends for key process parameters. In addition, a dedicated trend-display has been designed for supervision support. In this display the operator can trend any measurement, control valve position or control error signals, adjusting the scale and time freely to support detailed monitoring and problem solving. The operator can easily select warning limits by dragging arrows up or down at the scale, as seen in Fig. 16. If a warning alarm occurs it will produce an orange frame around the scale and a summary alarm on the LSD and in the alarm overview display. It is possible to select 24 different measurements in one display.

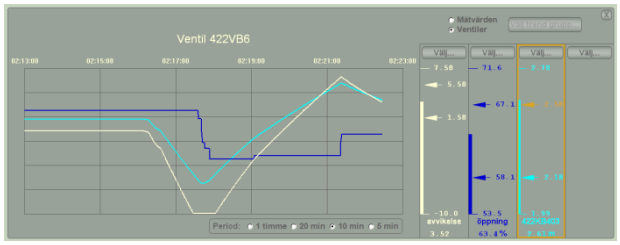


Fig. 16 Manual selection of warning trends.

5 Alarm presentations

In the proposed design alarms are distributed throughout the whole HSI and presented in different ways: Highlighted and summarized on the LSD, integrated in LSD and OWS, and displayed in detail on a dedicated alarm overview display where alarm and event lists can be sorted and filtered in various ways. We have also linked alarm response procedures directly to the alarms icons in the interface to make them as easily accessible as possible.

5.1 The state-based alarm system

To help the operators in incident and accident situations where there are a lot of activated alarms (alarm avalanches) we have designed an alarm system that highlights off-normal events in the context of the actual plant state. This “state-based” alarm system is designed to be an advanced alarm tool for operators, to be used as an add-on alarm system to their ordinary alarm system. The state-based alarm system is based on a number of well-defined process states. Only alarms not normal in the actual process state are alerted in the state-based alarm system, which is shaped to make it easier for the operators to actually use the alarm system during transients by make it easier for the operators to detect real alarms. Of the 2500 different alarms that are defined in the simulator with the ordinary alarm system, there are some hundred that often are repeated in different process states. In such situations, the real deviation alarms in a particular process state will more or less disappear. The

state-based alarms that is associated with the new plant state, e.g. reactor scram or turbine trip, is highlighted.

In the case of the HAMBO state-based alarm system, 19 different process states are defined. The state-based alarm system continuously adjusts itself to the actual process state.

In LSD and OWS the normal alarms are presented by a grey frame and the state-based alarms (not normal alarms at the current process state) are presented by yellow background. See Fig. 17.

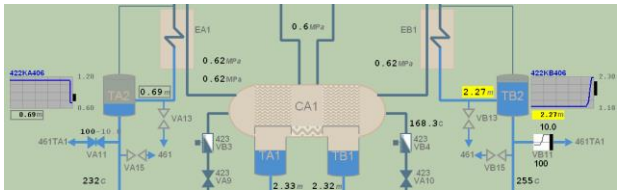


Fig. 17 Grey frames for normal alarms to the left and yellow background for state-based alarms to the right after turbine trip.

The state-based alarm system has been tested with operators from different NPPs and was very well received. Especially the shift supervisor found it useful for keeping an overview of the situation and prioritizing actions.

5.2 Alarm overview display

In the alarm overview display the normal alarm list and the state-based alarm list is presented as seen in Figure 18. In this display the event list is also presented. Above left indicates the overall status of safety functions and protection systems and shows a list showing deviations from actuated safety systems. It is shown in Fig. 18 that the alarm overview display appears when the containment isolation signal is actuated due to a leakage inside the reactor containment. There are some simulated malfunctions in safety systems shown by red color. Above the ordinary alarm list is the interactive alarm status for all systems located. It is possible to select and acknowledge system by system.

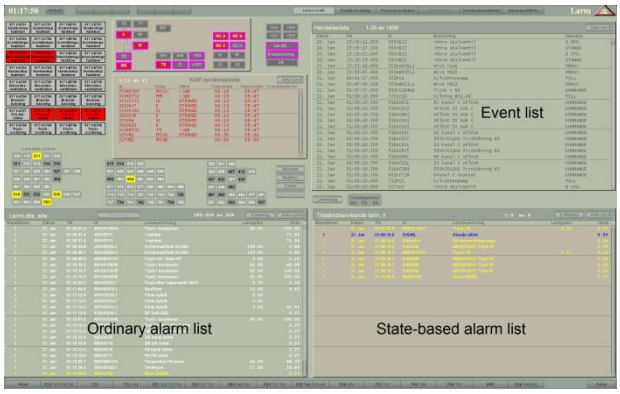


Fig. 18 The alarm overview display at a LOCA in containment.

6 Computer-based procedures (CBP)

A series of computer-based procedure prototypes have previously been designed, implemented and tested. The overall design approach has been to present a layer of procedural information on top of the familiar process displays, guiding operators through the steps. All the information that is needed when performing each procedure step is presented, and the required screen appears automatically for each step, highlighting the relevant process elements. This reduces the need for secondary tasks like navigation and searching for information. The initial tests show that this approach has been very well received by operators[1].

Based on the lessons learned from previous designs, some improvements have been done and the types of procedures have been more broadly implemented. The purpose of this is to make it easier for the operators to perform procedures accurately within a reasonable amount of time. The current version of the computerized procedure system is divided into four main display areas, presented on two 30-inch monitors. Fig. 19 illustrates the left screen while Fig. 20 the right screen.

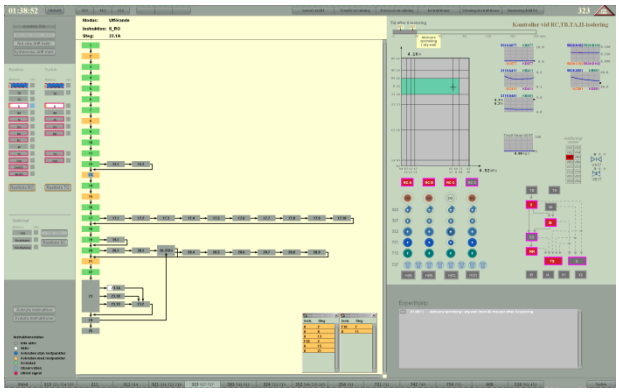


Fig. 19 The left screen for selection and overview.

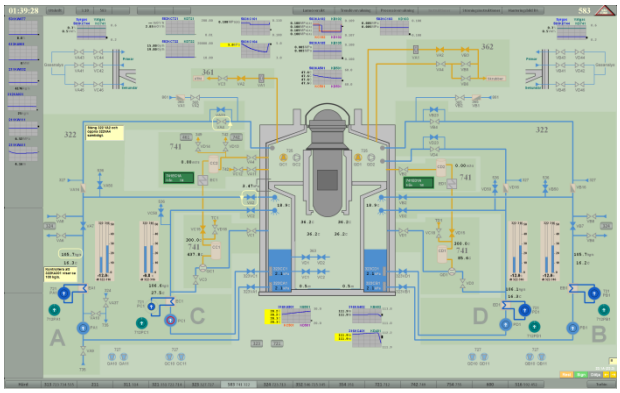


Fig. 20 The right screen for performing procedure steps.

Briefly summarized, the operator selects the relevant procedure to the left of the left screen and an overview of the procedure steps will be shown in the yellow area. It is possible to navigate between the procedures steps directly in the overview. Regular steps are presented vertically and alternative steps are presented horizontally. To the right in the left screen there is procedure dependent information to help the operator to supervise the process. There is also a list of information to help the operator check or act depending on the situation.

In the right screen the operator performs the procedure steps. There is one screen for each step in the procedure. The procedure text is written in textboxes superimposed on normal operating screens using a script language. The text boxes contain instructions that are based on the currently existing paper-based procedures. In addition, all the relevant components that must be checked or operated according to the procedure step are marked by the use of yellow frames. The procedure actions (e.g., close a valve) are made directly in the screen and the operators are able to directly observe the results of the actions.

The buttons on the bottom right in the displays (“postponed”, “sign/ok”, “hide”, “←”, “→”) are constant for all screens. If the procedure step is OK, the operator presses the “Sign/ok” button and then automatically navigates to the next procedure step. When “postponing” a step it will become orange instead of green in the procedure overview in the left screen. Procedure steps that are marked as “Postponed” can be accessed through a “Postponed-list”. The arrows are used for navigation to previous or next step without executing the step.

All workstations screens are updated continuously and the shift supervisor can follow the procedure on his own screen in “observation mode”.

Local procedure steps performed by field operators are also implemented in a portable device[2]. From this device the related information will be send and received to keep the procedure status updated, e.g. performed or postponed procedure steps both in the field and in the main control room.

7 Conclusions

This paper has presented an integrated HSI concept that is being developed for the boiling water reactor simulator (HAMBO) at the Halden Reactor Project. The design is based on lessons learned from a set of earlier HSI-related studies performed at Halden and elsewhere. The planned next step is to conduct a full evaluation focusing on human performance effects of the proposed solutions.

8 References

[1] BRASETH A. O., NIHLWING C., SVENGREN H., VELAND Ö. and KVALEM J. : “Lessons learned from Halden project research on human system interfaces”, Nuclear Engineering and Technology, vol.41 no. 3, pp. 215-224, April 2009.

[2] LUNDE-HANSSEN, L.S.: "A conceptual application for computer-based procedures for handheld devices", Proceedings of the ISOFIC/ISSNP 2014, Daejeon, Korea, Aug. 24~25, 2014.