4.7 Designing Graphics

Many graphics fail to support the CRO effectively because they have not been designed correctly. Short cuts are often taken so that insufficient thought is given to what the CRO really needs. For example in the process industry Process Flow Diagrams (PFD) are often used as the basis for control graphics and Piping and Instrument Diagrams (P&ID) are often used as the basis for detailed graphics. Whilst this strategy can provide a high level approach it must be remembered that PFD and P&ID are developed for an entirely different purpose and so cannot be expected to create good graphics without significant work. In many cases this type of schematic representation adds very little value to the HMI as it does not convey information that is useful to the CRO but occupies space on the screen that could be used to show more informative graphical objects.

4.7.1 Design Process for Graphics

The design of every graphic should be entirely focussed on providing the information that the CRO will need when using that graphic. This can only be achieved by fully understanding the CRO's tasks and activities, which requires active CRO involvement.

Graphic mock-ups may be a helpful tool to visualise the main parts of a planned user interface. An iterative process should be followed so that the design can be tested and improved as it progresses. One way that this can be facilitated is by using a wireframing tool to produce mock-ups of screens to various levels of detail to ensure that the essential requirements are captured early. Some tools permit user interaction to bring up subsequent screens. This can be useful at later stages in the design when usability in particular scenarios needs to be investigated. Presenting prototypes to the end users and then obtaining feedback from the operations personnel should be undertaken even if the latter group are involved in the design. This can effectively be part of the training process and may have the advantage of gaining 'buy-in' from the users.

4.7.2 Identifying User Requirements

Wherever possible the information a CRO needs to complete a specific task should be visible on a single graphic. Examples may include:

- Inlet and outlet flows to complete a mass balance;
- Multiple temperature readings to confirm a normal temperature profile is being achieved;
- All data and controls used during start-up of a piece of equipment;
- Being able to see levels in all tanks to confirm that only the correct ones are rising and falling during a transfer;
- Being able to confirm the status of all items of equipment providing a similar service so that it can be determined how well the supply is meeting demand and how much spare capacity is available if required.

Designers of graphics sometimes take the view that each data point can only appear once within the graphics pages (which would be the case on PFDs and P&IDs). In practice CROs may need to see a data point on a number of different pages to support the task that they are performing at the time. There is no technical justification for limiting the data point occurrence to a single page; duplicating the same data point on multiple graphics is perfectly acceptable if it helps the CRO.

4.7.3 Basic Rules for Graphic Design

The following basic rules should be applied to all HMI graphics:

- Only show items with control function (except safety critical items which need to be shown for the graphic to make sense);
- Text for explanation and guidance avoided/used sparingly;
- Data density at a manageable level whilst ensuring every item shown is legible;
- Whole control loops shown on single graphic (not split across graphics unless there is no alternative);
- Continuity of design, shape, colour and position across all graphics;
- Process flow logical, normally left to right;
- Lines should not cross if possible;
- Sub functional sections should be grouped together;
- Clear space should be used between sub-groups;
- Topology should be accurate (the way in which constituent parts are interrelated or arranged);
- Clarity and legibility must be maintained;
- Logical navigation between graphics;
- Data on each graphic should allow for a basic mass balance;
- Ensure critical data is not hidden by other windows, faceplates etc.
- The identity of each graphic should be immediately obvious, especially where several graphics may look similar because of duplicate equipment and systems.

A key part of the design process must be formal reviews to confirm these rules have been adhered to, but also to ask if the graphics 'look OK.' Where possible, some form of simulation would be used, where CROs can use the graphics to perform tasks. Reference should be made to any TRA and SCTA completed, as well operating procedures and similar.

Most modern commercial HMI systems allow for multi-windowing capability. For most large process plant, a well-designed graphics hierarchy precludes the need for the use of multi-windows especially when considering some of the disadvantages.

4.7.4 Evaluating the HMI Graphic Design

The following should be confirmed for the HMI graphic design:

Clarity. The purpose of the graphic should be self-evident. Individual items on the graphic should be obvious. Schematic, text and numeric graphics should be clear, easy to read and it should be obvious to what they refer. Cool and subdued colours should be used in normal operation, to allow bright colours which will stand out to be used in abnormal situations.

Consistency. All graphic indicators, text and colour coding should be consistent, not only within a graphic, but between graphics in the hierarchy. The operation of a control (e.g. hotspot/hot link) should have the same effect on all display graphics.

Variety. A limited variety of display techniques should be used so that operators can become easily familiar with them.

Feedback. Any control or other action on a graphic should give feedback to the operator to give awareness that the system is performing the requested task or indeed is giving an error. The feedback needs to be near instantaneous. Feedback on completion of the action may also be required. Failure of an action should be displayed in a timely and informative manner.

Robustness. Where interface action is taken by the operator, the system should be designed so that it can cope with incorrect key strokes/mouse clicks so that the operator can return to the original position if need be.

Failure. Failure of a graphic or of items on the graphic should be immediately apparent to the operator.

Redundancy. Multiple information display should be avoided (i.e. the same physical input from a number of different signals) as different readings can cause confusion unless this is required to achieve specific reliability requirements or as determined by task analysis.

Demand vs Status. Indications should make clear what values are indicating actual plant status and what are indicating set-points or demanded values.

Spatial Variation. If situations exist where several displays depict similar process units, it can be beneficial to place similar objects in different positions to help differentiate between the units. Note the clash with the concept of consistency.

4.7.5 Are there Enough Screens?

Assumptions may have been made earlier in the Control Room design process regarding the number of screens to be provided. But it is only when the graphics have been designed that these assumptions can be confirmed as correct. This evaluation should ask:

- How many overview graphics need to be viewed?
- What alarm display philosophy is to be adopted?
- How often are simultaneous control actions likely to be taken? (be realistic)
- How much general monitoring is required?
- What level of multiple windowing is to be allowed (if any)?
- What level of redundancy is considered adequate?
- Can screens be used for more than one process or 'module'?
- What future expansion may be required?
- Based on the findings from this evaluation, how will the number of screens affect how the CRO does their job and how will this affect overall system performance?

4.7.6 HMI Evaluation

Before commissioning an HMI it is important to carry out a formal functional Factory Acceptance Test (FAT) or equivalent. This is the last chance to ensure that the HMI is working as required before it is placed into service. This should involve CROs and include checks to ensure that:

- Navigation works as expected;
- All tags from the I/O database, including alarms and alerts, are on a graphic;
- Each graphical object works correctly as specified;
- Correct faceplates are invoked from the correct graphical objects and that they work correctly;
- Indications on graphics convey the correct sense (e.g. an object shown as "off" is really off or one shown as "full" is really full).

Once in service, the CRO should have a formal mechanism for reporting faults and requesting improvement. General performance should also be monitored and action taken to drive improvements.

4.8 Data Entry Consideration

Although there are usually limited requirements to enter data via a control system HMI, it can be critical that the correct data is entered. In particular, when entering a control set-point, an error could have a significant impact on how the system operates.

Reducing the likelihood of error and providing opportunities to detect and rectify errors should be properly considered. Prompt messages such as 'do you want to enter that figure' have a limited impact because people become very used to seeing them and tend to click 'yes' without much thought.

Acceptable data ranges should be programmed to ensure the CRO cannot enter a value that is wrong by a large margin. But this control may have limited effect if a system operates over a wide range of conditions. Allowing small changes to be made by using an increment option (e.g. up or down arrow) can avoid large changes being entered accidentally, which can cause significant disturbance to the system.

Any control or other action on a graphic should give feedback to the CRO to give awareness that the system is performing the requested task or is indeed giving an error. The feedback needs to be near instantaneous. Feedback on completion of the action may also be required. Failure of an action should be displayed in a timely and informative manner.

Consideration should be given to any findings from safety studies that indicate an error during data entry could result in a hazard or contribute to an accident. The HMI design should ensure these errors cannot occur or suitable protection devices should be installed to avoid an accident if the error does occur.

5 Accessing the Control System from Outside of the Control Room

Technology allows people to access control systems from remote locations as well as the main Control Room. As well as security considerations (see Chapter 8), there are other issues to be considered when deciding whether to enable such functions and how to implement them.

5.1 Managing Remote Access

The ability to access the control system from outside of the Control Room can affect the CRO. Also, advances in technology mean that a 'traditional' Control Room is not always required to operate a system.

The use of devices providing remote access to the control system should be considered as an integral part of the system and included in the original design. They should not be considered as a separate function. They should either be "read only" or a robust mechanism should be provided to ensure the point of control is clear at any time. An assessment should be made of why people will be accessing the system remotely so that the correct device can be provided. Uses may include:

- Field Operators operating systems locally, allowing them to carry out direct visual monitoring to supplement the data presented on the HMI;
- Supervisors, managers and technical personnel monitoring operations and analysing data;
- Technical personnel being able to login remotely to provide out of hours support that may include diagnosing and rectifying problems;
- Backup if the Control Room suffers an electrical or system failure;
- CROs being mobile, controlling the system from any suitable location.

Security issues should be addressed for any facility allowing remote access to the control system.

5.2 Remotely Located HMI

Most modern control systems will allow the HMI to be located anywhere on a network. The normal reason for this is to allow people to access the HMI without having to go to the Control Room. In some cases the ability to operate the system from any location has meant that a centralised Control Room is not required and the HMI is positioned locally, at the point where the Operator may be performing manual actions. In other cases, such as Normally Unmanned Installations (NUI) the option is required to change the point of operation depending on system status and activities.

5.2.1 Remote Control or Read-only?

The default option for remotely located HMI would normally be read-only functionality. This allows people such as Field Operators and Supervisors to view graphics and other information from a convenient location, for example when managing changes to plant or process, without having to go to the Control Room. This can be very useful for reducing distractions for the CRO, although it can have a negative impact on team work and communication due to reduced personal interaction.

There are relatively few concerns with providing read-only HMI in remote locations. However, it must be recognised that the access to the HMI is often defined by login, so an HMI intended to be used as read-only can often be used to operate if someone with the read/write credentials is logged in at the remote station.

5.2.2 Who is Operating?

Where it is decided that operation should be possible from a remotely located HMI, robust controls should be implemented to avoid any confusion about who is master for operating the system at any time. This can be handled by good communication when handing over operations between individuals. However, this is prone to failure, especially during shift changes. A particular concern is where intervention may be required to deal with an event but a breakdown in communication means that either no one responds or two responses are initiated at the same time that may interfere with each other.

HMI's in different locations can be managed by only allowing one HMI to be logged in with the operate function at any time. All other HMIs would only have read-only function. This requires all HMIs to be logged out before someone logs in to the HMI that they plan to use. The problem with this is that there will be times when no HMIs are logged in to operate and so no one can intervene if required. This can cause a significant delay, especially if someone trying to login has forgotten their password. Also, there can be problems if people have to leave the facility unexpectedly (e.g. in an emergency), the system crashes or someone forgets to log out when they leave. In these cases no one will be able to operate the system. This is particularly problematic on normally unmanned installations (e.g. offshore platforms) as it is not a trivial matter to return to the facility to log out. Mechanisms should be in place to deal with these scenarios.

Another way of avoiding multiple HMIs being enabled for operation at the same time is to use a virtual 'token' or similar. This is a mechanism to pass operation from one user to another without creating a situation where no one has the ability to operate the system. Again there can be issues if operation is not handed back, and again mechanisms should be in place to deal with this, for example by use of timeouts and reversion of control to a default location or a pending applicant who has the right credentials.

5.2.3 Who Receives the Alarms?

Whenever two or more HMIs have access to the control system, whether read-only or operate, the handling of alarms should be properly managed. Options include alarms sounding:

- On all HMIs – can cause confusion about who will respond, and may mean no one responds because they assume someone else will;
- On one fixed HMI (typically the one in the main Control Room) – may mean an alarm is received by someone who does not have the capability to operate the system because that has been handed over to someone else;
- On the HMI that currently has operate capability – essential that the HMI is manned for the whole time in case an alarm occurs.

This has serious implications for alarm management (see EEMUA 191[1]) as there are many situations where CROs are overloaded by alarms if they are receiving them from secondary HMIs that have been put through to the Control Room for convenience, even though the CRO may not be formally operating that part of the system.

5.2.4 Non-standard HMIs

HMIs are available for use in challenging conditions (i.e. not in a Control Room or office). They can be weather proof or suitable for use in hazardous areas. Some are simply protected against heavy handed use.

There can be a number of human factors issues with these non-standard HMIs. Screens are not always as clear and bright as 'normal' screens due to protective covers and housings. This can be made worse by local lighting. It can be difficult view graphics and distinguish colours.

Non-standard keyboard and mouse combinations are often provided. These can be difficult to use, especially if people are wearing gloves or other Personal Protective Equipment (PPE). This may not be a problem for simple inputs but can have serious implications if precise mouse clicks or lengthy text or data entry is required via the HMI.

Background noise will mean normal alarms on HMI may not be audible. Load claxons or sirens and visual beacons or flashing lights can be used but these may not be practical or appropriate. Also there may not be enough screen space at a local control point to display alarms as well as the process tasks. This may result in complicated scrolling and error-prone multi-click operations.

5.3 Plant Information Management Systems (PIMS)

PIMS systems provide an interface to a control system, making process data available to standard computers. They allow data to be downloaded from the control system for storage and analysis using spreadsheets and other applications.

5.3.1 Offline use of PIMS Systems

One of the main purposes of a PIMS system is to allow historical data to be searched and analysed in order to identify trends or to diagnose issues that have occurred when operating the system. This can be very useful for optimising processes to improve productivity, quality, safety and environmental performance and to reduce costs and outages. This is usually an 'offline' activity performed by technical personnel and by managers analysing recent and historical system performance.

There are generally no issues with offline uses of PIMS, provided that security and integrity of information are ensured as the information handled may have some value for industrial espionage or cyber-attacks. However, care must be taken to ensure CROs do not feel that their work is being scrutinised by people remote from the operation, who may not be fully aware of the circumstances that may have been present at the time of an event.

5.3.2 CROs Using PIMS Systems

CROs can also use PIMS systems to give them a different view of the data available from the control system. A typical example is to use PIMS to present a set of trends that are not immediately available from the control system HMI. This is possible if the PIMS system is refreshed with data from the control system fairly frequently. In most cases the refresh rate is fast enough that the data is reliable enough for the CROs' requirements. However, this may not always be the case and it may be possible for CROs to be making decisions based on data that they assume is up to date, whereas it is actually not sufficiently recent for the purpose.

PIMS systems are generally not designed to achieve a high level of reliability and CROs should not become overly reliant. In many cases CROs use PIMS because of shortcomings in the control system HMI. It is much better to improve the HMI than to create a situation where CROs rely on an inherently unreliable PIMS system.

5.4 Display Remote Access

Display Remote Access (also known as Desktop Virtualisation) allows people to access a computer system from a remote location via a network. A main 'host' server handles all processing whilst the remote device receives an image of any displays generated by the host. Software provides a means for someone using the remote device to interact with the system, but all processing remains within the host. This has many security advantages and means remote devices only require modest processing capability (in IT terminology, they are thin clients).

Display Remote Access can be used to allow people to access the control system from a personal computer, tablet or mobile phone. If read-only access is provided the main concern is simply whether the displays will be usable, especially on devices with smaller screens.

Display Remote Access can allow operations to be carried out remotely, but this introduces all the operational issues discussed above (see Section 5.2) for remotely located HMI. Slow network speeds and unreliable networks can cause particular problems as well as operator frustration.

5.5 Handheld Devices Used for Logging Data

Various handheld devices can be used by operators and others when performing routine checks and inspections. Tablets or similar may replace paper checklists. Data still has to be collected and entered manually but can be uploaded directly to a computer making it available in the Control Room and allowing for much easier analysis, and instant responses can be sought from technical experts. Other devices include data loggers, which do not require manual entries. They may be fitted with sensors (e.g. vibration, surface temperature) that take measurements directly to the device or communicate with sensors that are fixed to items of equipment.

All devices used on site must be suitable for the areas they will be used in. This is especially important in areas where a flammability hazard or a potentially explosive atmosphere may be present. This means that equipment should be appropriately Ex certified for the zone, or an individual risk assessment completed before use. The means of entering data also has to be considered, taking into account rules that may require people to wear gloves or other PPE.

Uploading data directly to an electronic device may mean that people are less inclined to notice the readings and so may not detect an abnormality. This can be improved if the device includes an alert function that highlights any discrepancies or trends. Also the fact that the data is available for more effective analysis may be considered as balancing out this concern, provided that people are actually using the data on a regular basis.

However, if the data collected by an operator is considered to be so important that a handheld device is required to collect it, there may be an argument to say that instrumentation should be provided so that the live data is always available via the control system. This would reduce operator workload and reduce the likelihood of operator input error or omission.

6 Training and Competence

CROs require a range of skills, knowledge and understanding and the correct attitude to be effective in their job. This is achieved though selection and formal training, and becomes embedded through experience from hands-on operations and simulation.

6.1 Role of the CRO

CROs clearly have an operational role and require technical competencies. Furthermore, the CRO role will require a range of non-technical competencies that are more concerned with managing information, evaluating situations and directing operations.

6.1.1 CRO Technical Competencies

CROs require technical competencies to operate the system via the HMI. They are required to perform a range of tasks including start-up and shutdown of plant and equipment, adjusting process parameters, changing modes of operation and responding to alarms, abnormal situations and emergencies.

The degree of system automation will determine the nature of the tasks performed. For systems with little automation the CRO will routinely be required to operate individual items of plant and equipment (e.g. opening/closing valves, turning pumps on/off etc.) via the HMI. For more automated systems the CRO will spend more time monitoring processes and supervising systems and is likely to have a range of pre-programmed sequences available that will perform tasks with minimal direct involvement.

At a generic level the technical competencies required by CROs includes:

- Understanding how the system works and knowing how to operate it;
- Ability to use the HMI to monitor and control the process;
- Knowing how to perform tasks, including application of procedures and job aids where available;
- Managing process disturbances and emergencies.

6.1.2 CRO Non-technical Competencies

The CRO is often the focal point of a system's operation. CROs have access to process data via the control system and communication links with other members of the operating team. This means that they have to do more than simply carry out technical tasks, especially with increased levels of automation of the basic tasks.

Their responsibilities may include optimising operations, ensuring compliance with environmental constraints, managing plant difficulties and co-ordination of maintenance. To do this CROs should have a range of non-technical competencies including:

- Good communication, verbal and written;
- Work coordination;
- Situational awareness;
- Decision making and resultant action;
- Workload management;
- Taking a proactive role and being willing to intervene where required.

6.2 Achieving Competence

Competence can be defined as[17] "the ability to undertake responsibilities and to perform activities to a recognised standard on a regular basis. Competence is a combination of practical and thinking skills, experience and knowledge, and should also include a willingness to undertake work activities in accordance with standards, rules and procedures."

Competence is achieved by:

- Selecting the right people;
- Providing initial training;
- Allowing people to gain experience in a supervised environment;
- Refreshing competencies.

6.2.1 Selecting Personnel to become CROs

In many cases a potential CRO will be recruited from an existing pool of Field Operators (or equivalent). The benefit of this is that they will have practical experience of the system and so they have less to learn than someone coming from another site or role. Also, their knowledge of the field means they are better able to support and instruct Field Operators including those relatively new to the job.

A good Field Operator does not necessarily make a good CRO because CROs generally need to have more non-technical skills than would be required for a Field Operator.

A second approach is to recruit CROs experienced in other systems. The challenge here is to train them on the system, as in most cases this requires a fairly long exposure to operations to allow a wide range of operating modes to be experienced. Also, HMI designs can show significant differences so people in this position will require some time to adjust. If they are established CROs they will already have demonstrated their non-technical skills, which is beneficial.

The third option is to select people based purely on their potential, who do not have any relevant operational experience (i.e. neither the system nor the use of HMI). This clearly increases the training load but the main question here is whether personnel selection processes are effective at identifying which people have the potential to succeed, in terms of both technical and non-technical skills.

One of the main challenges to recruiting to the CRO role is finding willing people. Many sites have struggled because the role is perceived to be demanding but often boring. Paying people extra to take the role can be an option, but may not always attract the right people. Good Control Room design can be beneficial because it can make the job more appealing (or less unappealing). Also, a degree of job rotation can reassure people that they are not going to be 'stuck in the Control Room' the whole time, and is usually beneficial to the company because it maximises flexibility of the workforce competent to perform different roles.

6.2.2 Initial Training and Assessment

It is clear that any operator needs to understand the system and the process it controls. The main difference between training a Field Operator and a CRO is use of the HMI. Training should cover two main aspects:

- Generic use of the HMI (e.g. how to navigate, enter data, acknowledge alarms etc.);
- Specific aspects of the HMI to be used (i.e. knowledge of the graphics and other displays).

The time spent on initial training will depend on the background of the person. If they do not have the technical competencies required (i.e. they have not previously acted as a Field Operator or similar) the training can be carried out in a classroom, supplemented with sufficient time on site. This CRO specific training can be performed using a simulator if available or on a live HMI, which may be in the Control Room or another location.

A structured programme should be developed and followed with a suitable mentor or coach in-situ.

6.2.3 Gaining Experience

Initial training can usually be completed fairly quickly but the trainee will not be ready to perform the CRO role. To become fully competent in the role the person should gain a wide ranging experience of what it entails. This can be achieved through on-the-job training where the person performs the role under direct supervision of an experienced CRO. Over time they will start to do more of the role with less supervision until deemed competent.

On-the-job training is beneficial in many ways because it allows people to learn and practice skills on the actual system, which is always very difficult to achieve with any off-the-job training. One of the key difficulties is that for most of the training time there will only be 'normal' routine operations taking place. The trainee is unlikely to see many (if any) non-routine tasks and abnormal events.

Training CROs for abnormal operations requires very careful planning and delivery. Simulators can be used (see below) if available. If not, other forms of simulation should be used.

As with all training, a CRO should be deemed competent via a competency assessment process, which should be based on a clearly defined role profile covering all modes of operation. Competency should not be based on the time that someone has spent in training as this does not account for individual abilities or exposure to the job that has been achieved in that time.

There is often a pressure to get CROs trained quickly to fill vacancies or expected increases in workload. This is another good reason to consider a degree of job rotation for operators so that there is always some 'spare' competent capacity to cover situations where CROs are absent or leave the organisation. It is also important to ensure that the spare capacity is adequate for all expected modes of operation, including major turnarounds.

6.2.4 Continual Learning

It should never be assumed that someone who is deemed competent will maintain it forever. People forget things or become a specialist in only certain parts of the role, and systems change. In any critical role the requirement for continual learning, refreshing and assessment are essential.