Safety practice

The effect of control room location, architectural design, systems configuration and human factors on major accident consequence and likelihood

Andy Brazier, UK

Summary

The Flixborough accident reminds us that wherever major hazards are handled there is always the possibility of an accident. Of the 28 people killed in the explosion, 18 of those were in the control room at the time[1]. This highlights the importance of location and structural design of control rooms. However, moving a control room away from the plant to reduce fire and explosion risks has other implications.

The nature of process operations since 1974 has changed, largely as the result of new technology. Whilst learning from Flixborough may have been focussed on location, it is worth considering how the overall design of the control room and associated systems contribute to risks at sites handling major accident hazards in the 2020s. This goes far beyond the colour of the walls, desk height and type of chairs provided. The focus should be on supporting the control room operator (CRO) to perform their critical role of keeping the plant safe and responding to accidents.

The aim of this paper is to summarise the areas where control room design can influence the risks of major accident hazards. Reference is made to an HSE Contract Research report related to remote operation of process plans[2] and the latest edition of EEMUA Guidance 201 related to control room design[3].

Keywords: Control room, human factors, Flixborough

Control room location

The number of fatalities that occurred as a result of the explosion at Flixborough illustrates how important it is to consider where people are working in relation to the hazard. As Trevor Kletz[4] highlighted in his concepts of inherent safety — "People who are not there can't be killed."

Most control rooms are occupied 24 hours a day, seven days a week. Moving them away from plant areas, outside of the hazardous area, means that people working in them are inherently safer if an accident does occur, but it has to be done in a way that does not increase the likelihood of an accident in the first place. This needs to be considered during design and when managing risks of an existing facility.

Locating a control room away from the plant

At a subjective level, CROs may feel less connected to a plant that is a long way away. It can lead to the formation of separate teams that mean the CRO never visits the plant they control. There is a view that "too much time spent operating from the control room may result in a loss of "feel" for plant operation"[2]. This can usually be overcome by rotating members of the operating team between control room and plant roles.

The opportunities for face-to-face communication between the CRO and field operators is likely to be reduced, with radios and phones being relied on more. It is generally accepted[2] that face-to-face communication is most reliable because "it is easier to convey urgency and hence problems are identified more quickly", "things get done better" and "you are more likely to get the correct interpretation of the message"[2]. This applies to general communication throughout a shift, but becomes a more significant issue for the most critical communication events (e.g. shift handover, team briefings) if they are not conducted face-to-face. Accidents including Piper Alpha, BP Texas City and Buncefield occurred after shift handovers where communication had been poor[1]. Although the main failure leading to Buncefield was related to alarms, if the operators knew the tank level was rising, they would have recognised the need to intervene before safe operating levels were exceeded.

Communication with other groups may actually improve. If the control room is closer to offices, it can mean that people outside of the operating team (e.g. engineers) are more able and inclined to visit and discuss issues with the CRO. However, it may also mean they are less inclined to visit the plant themselves, which creates its own issues.

The ability for the CRO to directly perceive plant conditions (e.g. hear, smell, feel) is reduced by distance from the plant. The effect this has is difficult to determine but may be "significantly underestimated, particularly for detecting fault conditions"[2]. Of course, the field operators are still available to use their senses, but this has to be conveyed to the CRO, which is not easy.

To support effective teamwork, it is normal to use the control room as the main hub for all members of the operating team. As distances increase the field operators spend more time travelling back and forth to plant. Although, this can have benefits if they "take a more systematic approach and spend more time on the plant with each visit"[2].

0260-9576/24/$17.63 + 0.00

Locating a control room near to the plant

The benefits and risks discussed above for remote control rooms can be reversed for control rooms close to the plant. However, there are other issues to consider.

Creating a control room that will protect its occupants from accidental events can lead to a perception of 'operating from a bunker.' Although nearby, the reinforced structure of the building may mean the ability to directly perceive the plant is lost. Providing windows to the outside world becomes more complicated (and expensive) meaning they are often not provided (or are blocked up as the result of an occupied buildings risk assessment). This leads to many complaints from CROs who feel increasingly cut off from the outside world.

Proximity to the plant can encourage CROs to quickly 'pop out' to look at something for themselves, instead of asking a field operator to do it for them. This can lead to the control room being unoccupied, with the potential for the CRO to be incapacitated during their brief visit to plant. This is not an issue if an unoccupied control room has been considered in design, but in many cases the assumption is for a competent CRO to be present at all times.

Access to fortified control rooms via heavy steel doors and airlocks can be difficult. Power assistance can reduce the effort required to open and close the doors, ensuring an effective airlock is maintained, but often works slowly. Delays may cause problems if operators need to attend to something urgently on the plant and the hassle of using the doors may even discourage people with legitimate reasons from visiting the control room during normal situations.

Accident prevention

The CRO has a critical role in ensuring the safety of operations. They monitor for early signs of problems and intervene to prevent escalation. To do this effectively they need to be alert and healthy, and supported by well-designed systems.

CRO alertness

A CRO who is alert and healthy is more likely to detect and diagnose issues early, reducing the potential for escalation. Given that many work twelve-hour shifts, including nights, this is not trivial. The shift pattern and management of hours actually worked is critical, but aspects of control room design can also have an effect.

Working conditions in a control room including lighting, temperature, air quality and noise will all affect levels of fatigue and stress. Lighting can be very personal, so individuals working in a control room should have control over their own lighting levels. Poor air conditioning can contribute to fatigue and other health issues, and can lead to CROs propping open doors to get fresh air, which can negate safety and security requirements.

Access to welfare facilities including places to prepare and consume meals, toilets and rest areas are important because "Meal and rest breaks can have a significant effect on CRO performance"[3]. This assumes that organisational arrangements are in place to allow CROs to leave the control room to take breaks, which far too often is not the case.

Situational awareness

CROs achieve situational awareness of plant conditions from control and safety systems, communication with colleagues and direct perception. Good system design can assist them to detect and diagnose problems promptly, giving them the opportunity to intervene to avoid escalation. These requirements may not be fully consistent with the 'normal' demands for the CRO, which are more focussed on optimising the process to achieve production and quality goals, and so need to be carefully considered in the system design.

Human Machine Interfaces (HMI) are used by the CRO (and others) to "develop, maintain and use accurate and up-to-date situational awareness of the current, recent past and likely future state of the system"[3]. Whilst there can be a lot of discussion about colour schemes, use of symbols and text font, it is the presentation of data that makes the greatest contribution. Well-designed graphical displays show plant data in ways that is consistent with human capabilities. They should provide the data the CRO needs in a way that they can understand easily without overloading them[3]. Achieving this requires a thorough understanding of the overall system objectives and functions, the tasks performed by the CRO and the information they need to do them. Unfortunately, graphics are often designed simply to show data that is available, without a consideration of the CRO's requirements. Better HMI design could have prevented several major accidents including Texaco Milford Haven, Esso Longford and BP Texas City[1].

Visibility of data shown on screens and panels depends on viewing distance and angle, size of object (text, symbol etc.), and the person's eyesight[3]. Control room designers should have a good understanding of how the CROs work when deciding how many screens are required, their size and locations.

Alarms are part of the HMI and are specifically intended to inform CROs of equipment malfunctions, process deviations and abnormal conditions. Unfortunately, many systems distract the CRO with unnecessary and nuisance alarms during normal operations, and overload them when things start to go wrong. Poor alarm management has been identified as a contributory factor in several major accidents including Texaco Milford Haven, Esso Longford, Cataño oil refinery fire (Puerto Rico) and the toxic release at the La Porte site in Texas, USA[1]. Alarm rationalisation should be an essential activity for any new control room project, and routinely repeated for operational facilities.

Accident response

It is usually someone in the operating team who will recognise that a hazardous situation has arisen requiring a prompt and effective response. The situation is unlikely to be obvious at first and the resources available immediately will be limited[5]. It is noted that over 50% of the accidents listed in the IChemE summary of major incidents[1] included 'emergency preparedness' as a root cause.

Identifying a hazard has occurred

Protective system alarms (e.g. fire and gas detection) handled by systems independent from the control system may be the first indication that loss of containment has occurred. These do not tend to suffer with the same problems as control systems but the way they are displayed to the CRO can have a big impact on how they perceive a developing scenario. During normal operations single gas detectors may be activated due to faults, routine testing or small leaks. Identifying a single activation on an alarm list is quite straightforward. If a large leak ever occurs there will be multiple detectors being activated and being able to interpret the pattern can allow the CRO to visualise the flow of the gas cloud

human factors

0260-9576/24/$17.63 + 0.00

and help them to determine the source and predict the extent of the hazard.

Being able to see the scene directly can give a better understanding of the issue. CCTV can be very useful for CROs in an emergency, and the relatively low cost of systems means there is little justification for major hazard sites to not have it. Whilst a window from the control room is only ever going to provide limited visibility of a plant, the increasing concern of environmentally caused incidents means that being able to see what is happening outside will help the CRO to understand the impact of heavy rain, strong wind etc.

Mobilising the appropriate response

There are some actions that the CRO can take to mitigate an accident. An HMI that allows the CRO to interact with the system quickly and efficiently under all plant conditions can allow them to take prompt action. Beyond this the CRO is likely to be directing other members of the operating team to take action, activating evacuation alarms, mobilising support teams and calling the emergency services. There is a lot to remember and making sure emergency response procedures are readily available and fit for purpose is critical.

As a scenario develops there may be requirements to formulate plans to isolate damaged sections of the plant and vent and/or drain process fluids to safe locations. Access to Piping and Instrument Diagrams (P&ID), and being able to lay them out so that a small group of people can work together is important. Having a suitable table in the control room, with good lighting above, should be considered in the control room design.

The control room is sometimes used as the Emergency Control Centre (ECC). It gives the emergency management team visibility of plant data and allows good communications with the operating team. However, it is also very distracting for the CRO, who has a critical role to play. An adjacent room with visibility into the control room may be considered a preferred option.

Allowing CROs to work safely in an emergency

Although most people on site will evacuate in an emergency, the CRO will normally be required to stay in the control room. Power loss to the site is one common occurrence. Whilst control and safety systems, including associated HMI, are usually supplied with Uninterruptible Power Supplies (UPS), control room lights are not. Designers often consider lighting requirements for evacuating a control room, which ultimately may be required. However, they fail to recognise that the CRO may be required to continue working for some time. "Where possible, full lighting should remain in the control room on power failure. If this is not possible, the location of lighting units with power backup should take into account tasks to be performed during the scenario"[3].

Another consideration is the Heating, Ventilation and Air Conditioning (HVAC) system, which "should be capable of being operated in recirculation mode if there is the possibility of an abnormal situation resulting in the presence of toxic gas in the external environment"[3]. This feature should be considered as being safety critical and receive appropriate maintenance, inspection and testing.

Conclusion

The Flixborough accident highlighted serious concerns related to control room location and architectural design. Subsequent technological developments means that the focus should be on supporting the control room operator (CRO) to perform their critical role of keeping the plant safe. All design is compromise and there is no correct solution but there are resources that can help to identify the critical issues and develop optimum solutions. This paper has tried to summarise the types of issues that should be considered. The following is a (non-exhaustive) list of factors to consider:

- locate outside the hazardous zone or protect against the hazard;
- make sure the most critical communication is carried out face-to-face (e.g. shift handover, control of work);
- make communication devices readily available and high quality (radios, telephones);
- support good teamwork within each team with good links between teams;
- allow and encourage legitimate visitors without causing distraction;
- windows with external views wherever possible;
- working conditions that enhance alertness;
- lighting that individuals can adjust to suit their personal requirements;
- welfare facilities easily accessible;
- time and cover in each shift for the CRO to take quality breaks away from the control room;
- HMI graphics designed to show critical information in ways consistent with human capabilities;
- number of 'normal' and large screens optimised to show plant overviews and detailed displays;
- good alarm management so that operators receive early indication that action is required without causing nuisance and overload;
- protective systems that provide early warning of hazards;
- CCTV for CROs to visually assess what is going on;
- procedures and supporting information (e.g. P&ID) easily accessible with somewhere to lay them out;
- ECC nearby but separate from the control room;
- backup power to all systems including enough lights to continue working safely in an emergency;
- ventilation systems that prevent ingress of hazardous materials.

References

1. *IChemE Safety and Loss Prevention Special Interest Group. Learning lessons from major incidents. (2022)*
2. *HSE Contract Research Report 432/2002. Human factors aspects of remote operation in process plant.*
3. *EEMUA 201. Control Rooms: A guide to their specification, design, commissioning, and operation 3rd Edition (2019).*
4. *Brazier, A. Edwards, D. Macleod, F. Skinner, C. Vince, I. Trevor Kletz Compendium. Elsevier (2021)*
5. *Brazier, A. Emergency Procedures. Loss Prevention Bulletin 254 (2017)*

0260-9576/24/$17.63 + 0.00