ACCIDENT ANALYSIS OF INDUSTRIAL AUTOMATION
PART 2/3

PROCESSING FUNCTION

HAZARDS IN THE CONTROL ROOM!

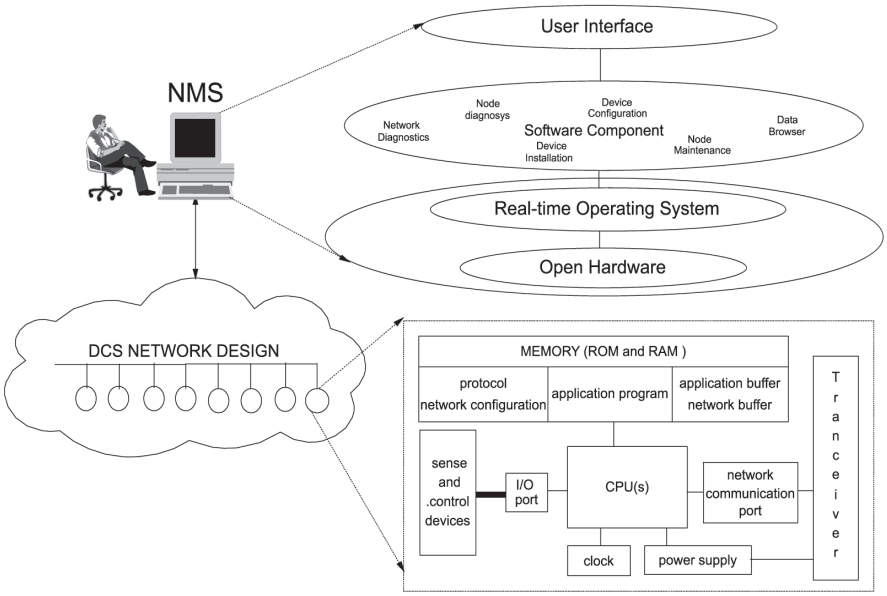
ARIA
dgpr srt barpi

CONTENTS

Cover page illustration : Control room in a fine chemical plant (PAS, Inc., ARR)

Methodology of this synthesis

Second of a three-part series devoted to analyzing accident relative to the use of industrial automated system, the present synthesis will analyse the failures derived from the processing function of automated control systems: the various components of the central unit (power supply, transmission, electronic cards, programs, man-machine interfaces, etc.), as well as the human component, which plays a central role in the execution of automated processes from a control room...



Architecture of the processing function for a distributed control system (DCS)

This synthesis is based on a primary sample of French industrial accidents recorded in the ARIA database, through 31st December 2012, with a sufficient level of detailed information to effectively understand the event (circumstances, consequences, causes). A keyword search relative to the processing function of the automated system, followed by an analysis of the accident summaries, has served to narrow this sample to just those events corresponding to at least one of the 3 following criteria:

- accident caused by the processing function of an automated system;
- accident exacerbated by a process or safety automated system;
- absence of a data processing/centralisation function on an automated system has either triggered or worsened an accident, to the extent that this absence is explicitly stated in the accident analysis and moreover function installation is included in the assigned technical action.

The secondary sample compiles 325 cases, including the accidents caused or exacerbated by a failure in human supervision for production facilities managed remotely, given that managerial and supervisory actions are considered integral parts of the «processing» function for an industrial automated system.

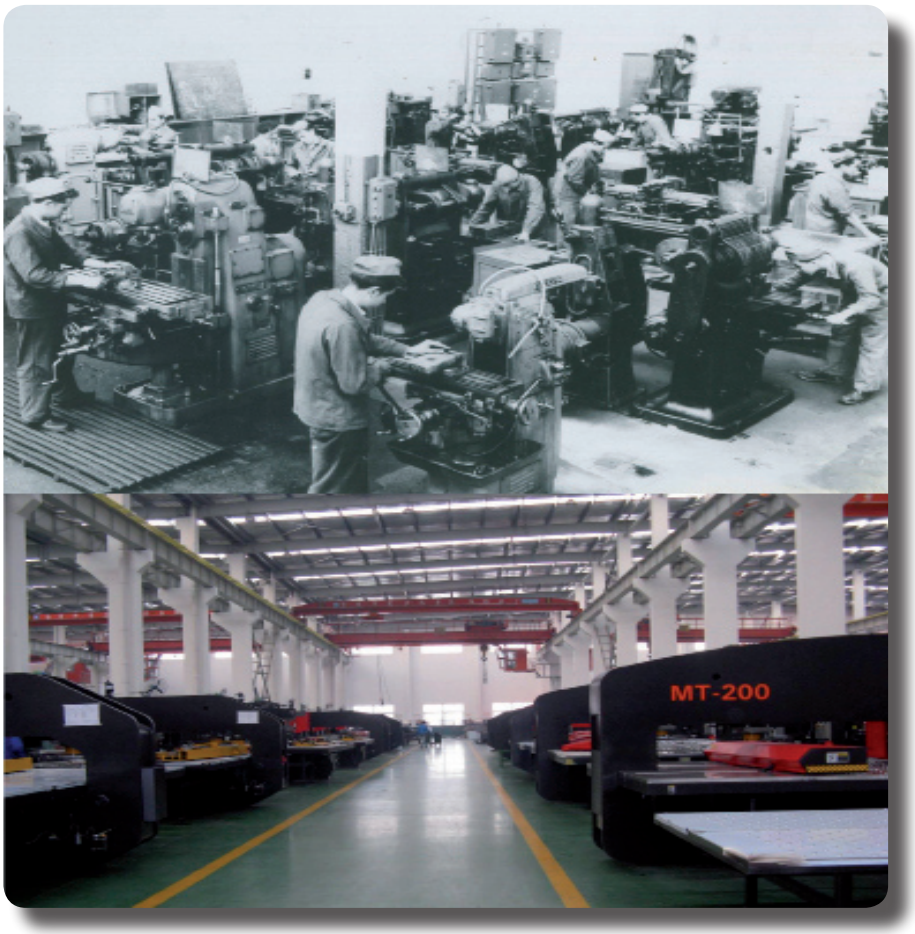
Moreover, since ARIA is an event-driven database and not reliability-oriented (as is the case with the OREDA, PERD, IEEE and EXIDA databases, among others), data collection and accident summaries do not always yield accurate information regarding the level of criticality or technical causes of the processing module defect on an automated system, its technology, etc. It is also possible that bias has been introduced among the sectors of activity under study, as information feedback on accidents may vary significantly from one sector to the next due to: the number of installations operating in France (e.g. far fewer for refining than for chemicals), proximity of relations between the Database manager and representatives of the various sectors, and the environmental authority's level of monitoring of the facilities involved in the accident(e.g. Seveso-rated facilities undergo enhanced monitoring)...

1. Processing function of automated systems

An assessment of existing reliability data, e.g. the OREDA base, indicates that the hardware of an automated system function is rarely a source of failure (8% of all failures recorded between 1981 and 2009 at the facilities of 10 international oil groups). Nonetheless, as opposed to sensors (whose impact on accident rates was studied in a previous report [1]), this function remains dependent on human intervention given the increasing presence of control rooms and display screens at industrial sites. Here lies the first paradox discovered at the beginning of the 1980's [2], when it was widely predicted that as of the 2n^{d} half of the 20th century, plants would no longer require human presence, replaced instead by the machine (according to the concept of the « unlit factory »). While these predictions had taken into account the outstanding efficiency of automated systems and their popularity in process control operations, accident statistics suggested that the hypothesis of eliminating the human factor as an accident source, with fewer industrial accidents as the net result, was in fact unrealistic..

«The factory of the future will have only two employees, a man and a dog. The man will be there to feed the dog. The dog will be there to keep the man from touching the equipment.»

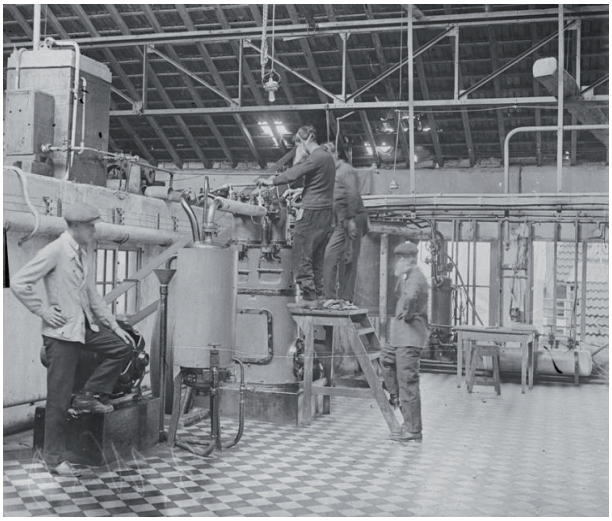
Warren G. Bennis, North American consultant,1996



Example of plant automation changes between the 1950's and 2000's

A second paradox appeared with expanded plant automation: the human factor has not disappeared but merely shifted. As the level of automation increased, the human operator's role became critical by transitioning from simple field operator (opening or closing valves, adjusting a machine, etc.) to supervisor responsible for rather sophisticated processes.

As an accidental cause, the human factor gives rise to more intricate errors capable of involving the operator's physical and mental states, his degree of perception of the process state (bringing into play the concept of situation awareness) and workstation ergonomics. Root causes of accident tied to organisational factors can naturally be identified, like training, task assignment, system design and programming. These observations are also verified outside of industry in fields that have become heavily automated like airline or maritime transport. A substantial body of literature has confirmed this predominance of human and organisational factors in industrial accidents relative to the processing of information delivered by an automated system and, more broadly, in all technological accidents [3].



Reactor inside a French chemical plant in 1917: its loading and monitoring require the close physical presence of field operators

Reactor inside a modern French chemical facility: its loading and monitoring are remotely supervised from a control room

Faced with this situation, industrial site managers responded by thoroughly revising their recruitment criteria, along with new workplace organisation and task assignments. Challenges have appeared and continue to mount in the effort to reduce factory accident rates; while such challenges are admittedly fewer in number, they are potentially more serious, as they arise from man-machine interaction and are not merely technical in nature. Thanks to his judgment, experience and adaptation/perception capabilities, man remains more than ever at the heart of automated efficiency and safety processes. Given the human operator's ability to detect high-risk situations beyond the likely detection possibilities of any current or future controller, the right balance must be struck when automating a process in order to preserve man's central role in overseeing efficiency and safety.

«How can a group of such well-intentioned, highly motivated and apparently skilled operators commit such a combination of errors and procedural violations?»

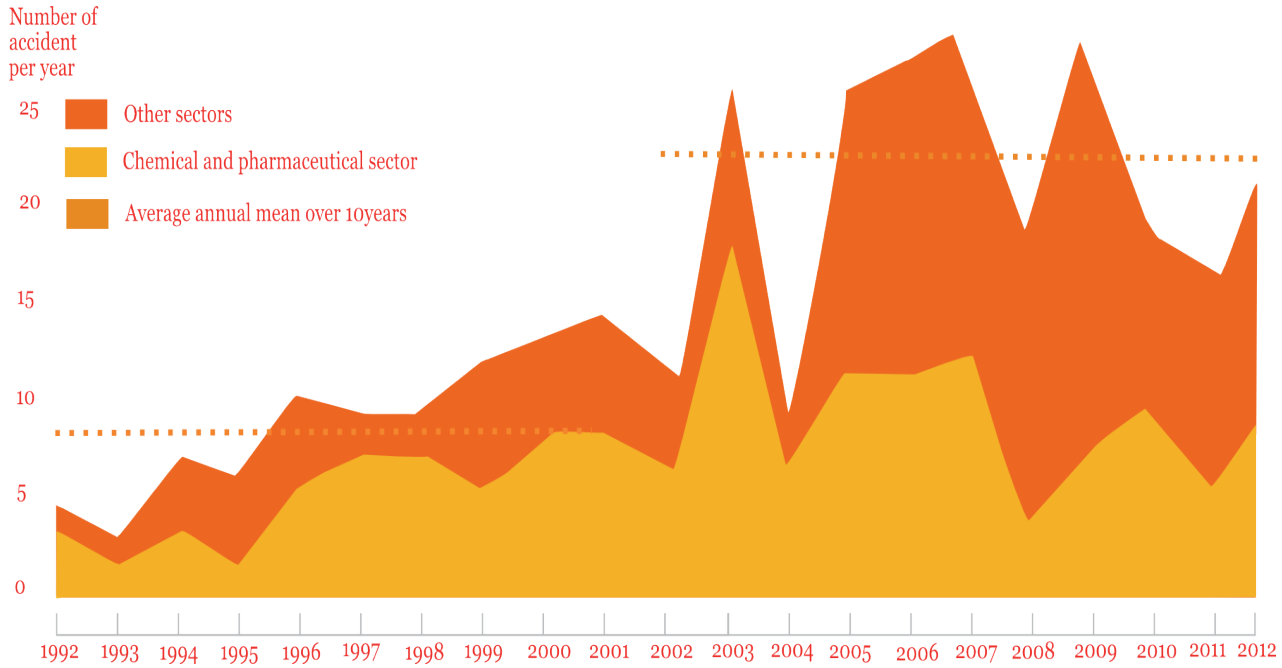
James Reason, psychologist and expert in human factors,1987 (about the Tchernobyl accident)

1.1 Accident statistical overview

Though the impact of introducing automation inside industrial plants has raised a number of criticisms, few today will dispute its benefits for worker and process safety. The operator, now removed from hazardous substances and installations, is still able to gain quick access to all control parameters; automation controllers permanently monitor in real time hundreds of parameters and often react faster than humans if performance deviates or accidental situations arise (see p. 7 for examples of accidents that could have been prevented by an automated system). The influence of quality regulations and standards, in addition to societal pressures exerted to improve safety at industrial sites, has led facility managers to further expand automation in order to minimise the human factor component in accidents or compliance failures. Moreover, from an industrial standpoint, the investment in a technical barrier such as automation is encouraged thanks to its reputation for tremendous reliability, while the investment in managing the human factor (through training, workplace organisation, ergonomics) may seem less promising and more complicated to oversee.

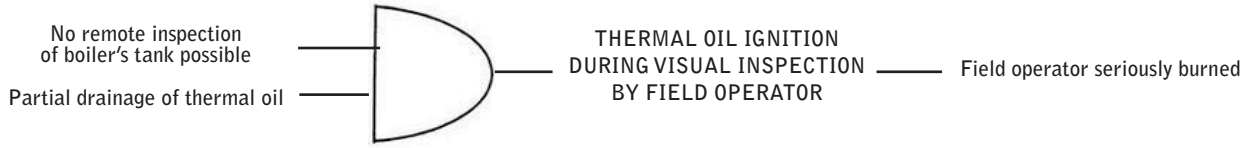
An analysis of the selected accident sample confirms that material components of the processing function tend to be reliable: 1% of all industrial accidents at stationary installations over the period 1992-2012 involved this function, whereas the « sensor » function alone accounted for 3% of all accidents between 1992 and 2011 [1]. In 2009, the *Mesure* magazine corroborated the conclusions drawn by the major reliability-oriented bases: fewer than 10% of hazardous malfunctions of automated systems are due to material components of the processing function, with the other 90% being ascribed to actuators and sensors [4].

Figure 1 *Annual number of accidents involving the processing function (ARIA base,1992-2012)*



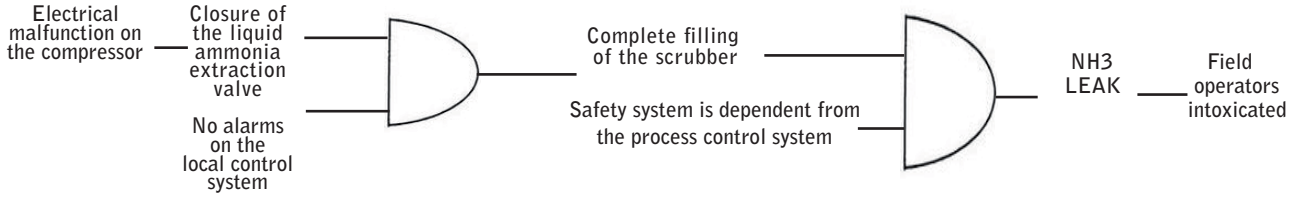
A breakdown of these accidents over time (see Fig. 1) reveals that their average annual -number tripled between 1992-2001 and 2002-2012. More widespread reliance on centralised automated process control since the beginning of the 2000's, spurred by the appearance of more efficient and economical computing component and communication networks, might explain this trend. A study conducted in 2002 by the british *Health and Safety Executive* on a panel of 107 large industrial facilities in England indicated that 81% of sites had already implemented remote automated process controls [5]. An analysis of selected cases concluded that 16% of accidents occurred or were exacerbated due to the absence of an automated control system (50 accidents since 1992). Examples of this type of accident are presented on page 7.

MANUFACTURING INDUSTRY
INSUFFICIENT AUTOMATION (ARIA 42730)
10th September 2012



Around 1 am at a wood panel factory, a field operator was called to service a condensing boiler designed to heat presses. The expansion vessel containing thermal oil at 274°C was 72% full despite the protocol stipulating a filling rate of between 40% and 50%. The field operator drained a portion of the expansion vessel into a tank containing oil at 60°C. After pouring out 2.5 m³ of product, he called the control room, which confirmed that the drainage step could be stopped. As he was preparing to climb back down into the retention basin with his back turned to the tank, hot oil vapours ignited and severely burned his legs, neck and face. He was wearing the appropriate individual protective gear. Vapours emanating from an elbow vent on the tank had fallen into the retention basin. A streak of flames had spread from the bottom of the tank into the circulation pump room before extinguishing on their own. The crew foreman notified first responders and a rescue team attended to the victim. The thermal fluid circuits were drained in accordance with emergency procedures. The victim was helicoptered to a specialised burn unit. The factory operator modified the tank vent by adding a roof hood and **installed a hydrocarbon sensor and air extractor in the retention basin, in addition to a camera to prevent field operators from stepping down into the tank to perform visual inspections.** It was also anticipated to motorise the valves or control them remotely.

CHEMICAL INDUSTRY - INSUFFICIENT AUTOMATION
ARIA 28776
1st August 1997

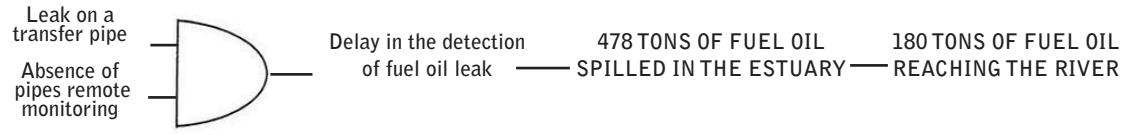


Within an ammonia (NH_3) production unit, a liquefied ammonia leak occurred on a scrubber used to eliminate residual non-condensable gases dissolved within the ammonia. Bothered by the smell, the control room operator sounded the alarm. A manual valve was closed and a water curtain deployed around the ammonia puddle in order to limit spreading of the aerosol cloud. An electrical malfunction had caused the accident: the erroneous relay of an ammonia compressor shutoff signal triggered closure of the liquid ammonia extraction valve on the scrubber, resulting in the scrubber being filled. Then, the local system regulating the release of non-condensable gases allowed liquid ammonia to escape. The installation was modified to improve safety by means of: **replacing the local column level regulation system by a centralised device with an alarm for a more responsive diagnostic; replacing the compressor status relay system by an automated safety mechanism independent of the process automation controller; and improving control room confinement...**

OTHER RELEVANT REFERENCES

missing automation : Aria 24436, 25156, 26430, 28745, 34410, 38674 / incomplete automation : Aria 19964, 26430, 30323, 31367, 32841

REFINING - INSUFFICIENT AUTOMATION (ARIA 34351)
16th March 2008



While loading 31,000 m³ of bunker fuel in a ship, a leak in a refinery transfer pipe resulted in a major oil spill in the Loire estuary. At 4.10 pm, a person on a barge observed the presence of hydrocarbons on the water surface and sounded the alert. A recovery ship was stationed at the mouth of the river while two trawlers recovered hydrocarbon pellets from the river. Investigations revealed that the leak was detected only after 5 hours leading to 478 tonnes of fuel being spilled of which 180 tonnes flowed into the Loire estuary. The operator was required to implement several additional initiatives and measures, among them : **Using a leak detection system along with a remote alarm in the control room to constantly monitor pipes located near the river, Installing a device to monitor the quantity of products leaving the tank and entering the corresponding transfer hose.**

OTHER RELEVANT REFERENCES

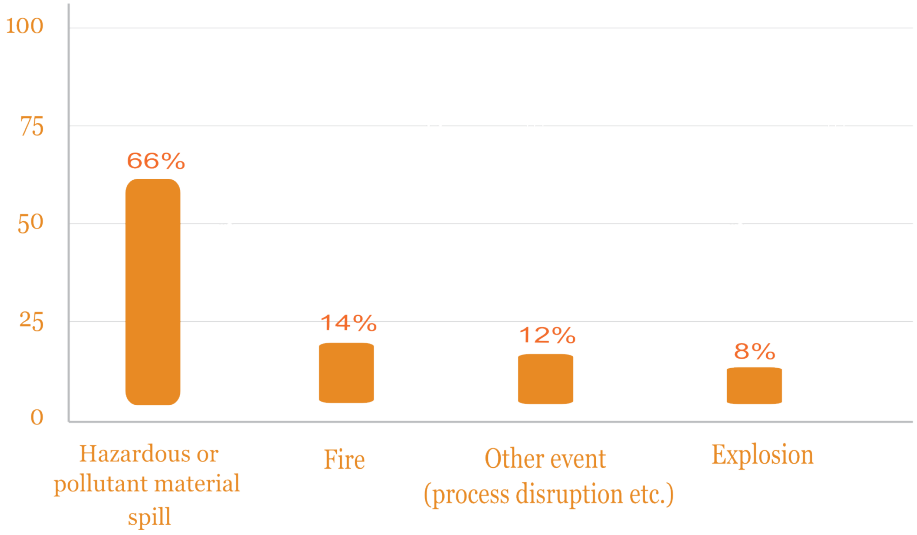
missing automation : Aria 10131 / incomplete automation : Aria 26186, 29903, 31441

1.2 Detailed accident analysis

1.2.1 Types of events

The accidents caused or exacerbated by a processing function failure reveal a typology similar to that of sensor-related accidents [1]: discharges of hazardous substances are most common, far ahead of fires and explosions (Fig. 2).

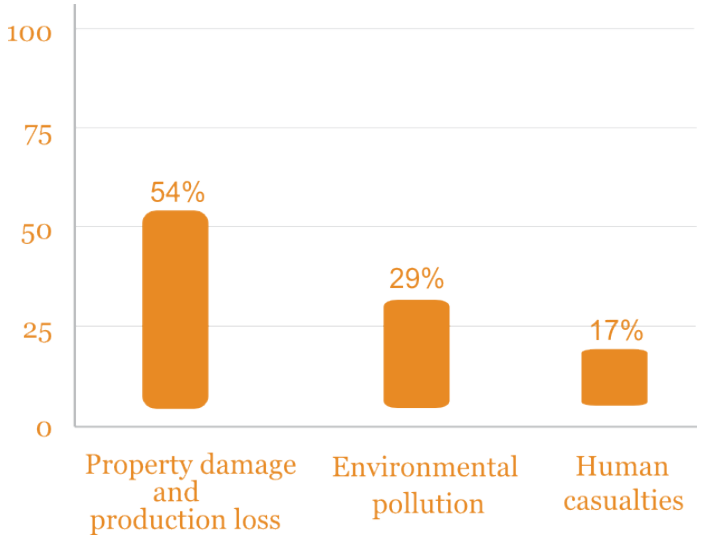
Figure 2 *Breakdown of processing-related accidents by type of event*



1.2.2 Accident consequences

While a majority of the accidents studied exhibit solely economic consequences, nearly 3 in 10 originate from environmental pollution (Fig. 3), resulting from the frequency at which hazardous or polluting substances are released. Victims are most often facility employees working near the affected unit (e.g. see ARIA entries 28776, p. 7, and 32640, p. 25).

Figure 3 *Breakdown of processing-related accidents by consequence*

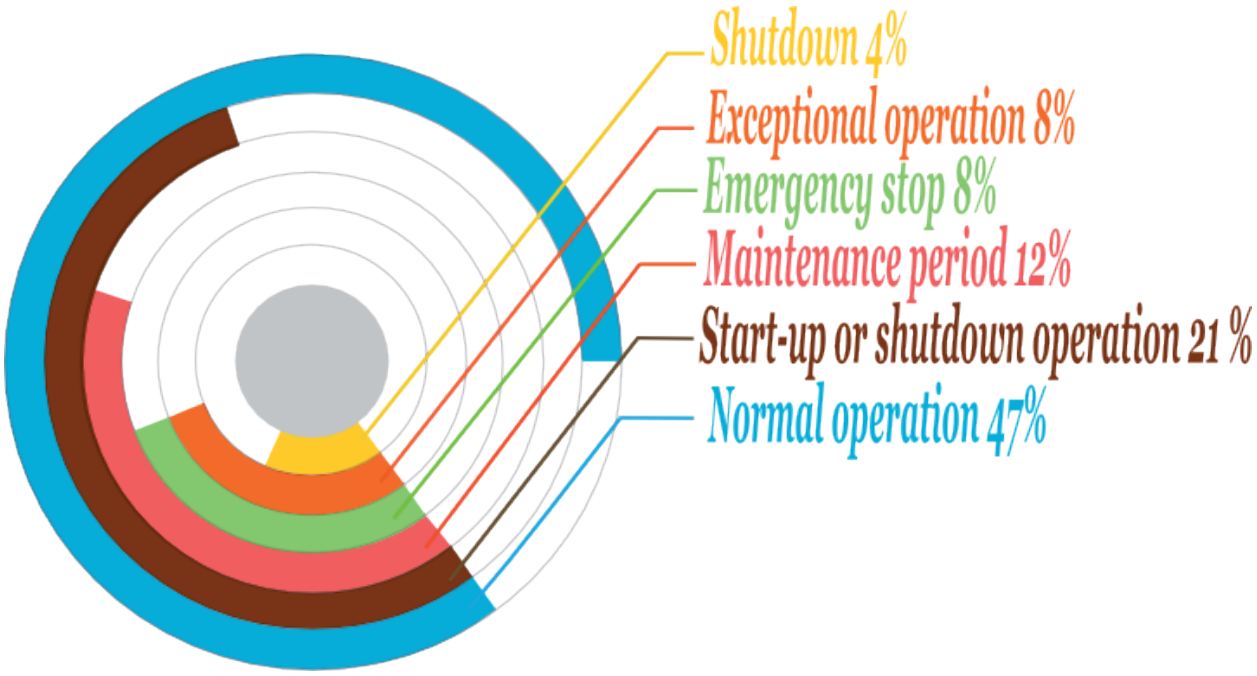


1.2.3 Accident circumstances

An examination of circumstances surrounding processing accidents (Fig. 4) indicates a majority of occurrences outside of normal operating phases, which questions the adaptation of the processing function's components to exceptional operating phases such as. maintenance periods and system restarts, as well as the human operators presence and reactions during such phases (see Chapter 2.2).

Over half of all accidents involving the processing function arise outside of normal operating phases.

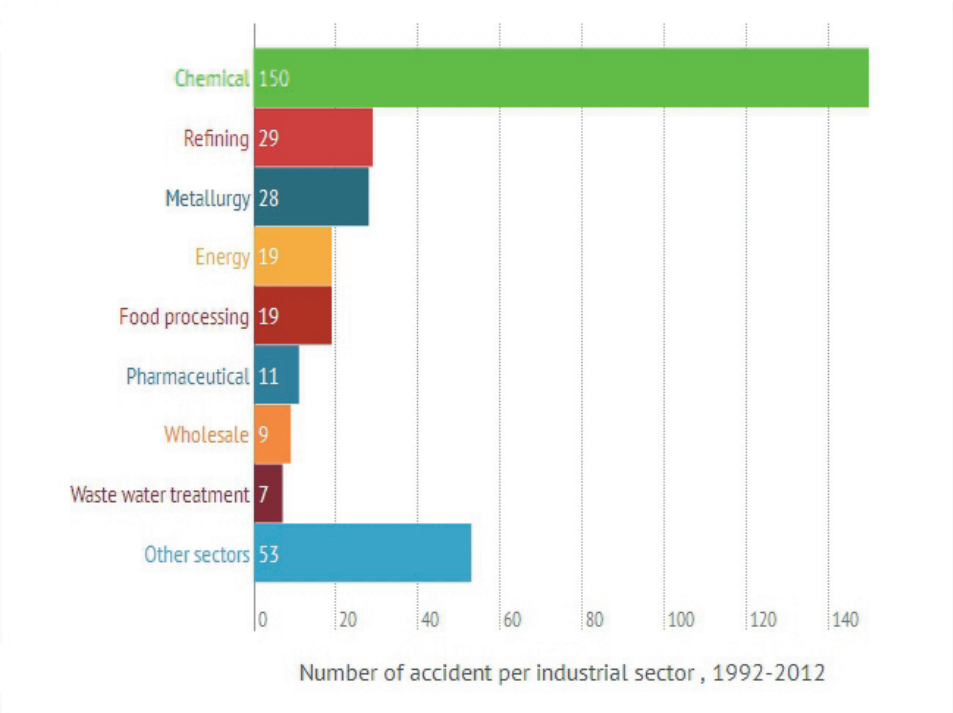
Figure 4 *Breakdown of processing-related accidents by their circumstances*



1.2.4 Sectors of activity

Eight sectors of activity can be distinguished in the studied accident sample, each of which contains at least 6 recorded cases (Fig. 5). The chemicals sector comes out on top with over 54% of accidents catalogued (150 cases). This result can be explained by: the high rate of automation in chemical processes, diversity in chemical processes, and the large number of chemical production sites across France. Moreover, this sector typically receives the most coverage in the ARIA base (12% of classified facilities accidents between 1992 and 2012). Many installations are designed with versatility to manufacture an array of products, which in turn raises the occurrence of accidental situations not anticipated when introducing the automated system or resulting from wrong control decisions. In this sector, better integration of the processing function would have allowed avoidance or at least reduction of the severity of 21% of all accidents arising: this rate is slightly higher than the average for all sectors (16%). An accident of this type is presented in the middle of page 7.

Figure 5 *Breakdown in processing-related accidents by sector of activity*



In contrast, the refining sector is far less commonly cited than chemicals in the studied accident sample (despite a relatively high rate of automation), though it still holds 2nd place, with 11% of all recorded cases, but represents just 2.1% of all accidents in the ARIA base. The volumes of products and raw materials handled, as well as the reliance on continuous processes requiring considerable machinery, are well-adapted to process automation solutions and a centralised form of unit management, which probably explains this observation. As opposed to the chemicals sector, refinery installations are limited in number (a maximum of 13 sites operating in France over the study period), and moreover, refining processes seem to be more widely standardised. Such conditions provide fewer opportunities for exceptional automation situations during a normal operating period.

The chemicals sector accounts for 54% of all «processing» accidents in the sample, refining 11%, and each of the six other sectors 10% or less.

Metallurgy comes in 3rd with 10% of processing accidents, even though this activity only accounts for 3.5% of all accidents contained in the base. Once again, the processes found here are relatively homogeneous from one site to the next.

With 7% of citations, the energy sector (fossil fuel and hydroelectric power plants) is the 4th most-cited, given its high level of automation and strong reliance on centralised controls: remote supervision of turbines and boilers, inventory management, etc.

Lastly, the food processing sector ties for 4th place (at 7%). While less automated than heavy industry, this sector comprises many sites spread throughout the country and implements highly diverse processes that often make use of hazardous and polluting substances, e.g. ammonia for refrigeration, hydrocarbons for heating and cooking, in discharging potentially toxic organic effluents. The other industrial sectors covered in the ARIA base each account for less than 4% of all recorded processing-related accidents and together represent less than a third of all cases.

1.2.5 Components involved

An evaluation of the 275 accidents involving defects in processing function components reveals the role of harware (calculator, electronic card) in 49% of accidents, followed by man-machine interfaces (MMI) 41% of the time. Transmission-related components within automated systems (data bus, relays) are involved in 14% of all cases. These results reflect the importance of the centralised control in processes (see Chapter 2.2) as well as the criticality of material component defects within the processing function.

Automated industrial gas bottling chain (Emerson Process, ARR)

1.2.6 Supervisory and safety functions

Automated processing functions tied to controls are involved in 80% of cases vs. 25% for functions dedicated to safety, with several accidents actually applicable to both functions when the automation controller handles these two simultaneously. In contrast, accidents caused by the failure to integrate correctly the processing function were nearly equally distributed between process specifications (53%) and safety specifications (47%). This balance was especially noticeable in the chemicals sector.

80% of processing-related accidents involve a process control function and just 25% a safety function. For the chemicals sector however, accidents resulting from inadequate integration of the processing function are divided equally between control and safety.

2. Accident direct causes

This chapter will analyse in greater detail the so-called "direct" causes of processing function accidents. The focus here is on the immediate causes or, more specifically, the «visible symptoms» of accidents that appear during an initial analysis. As a reminder, 85% of the processing accidents studied, i.e. 275 cases, stem from a failure in this function, while the other 15% (50 cases) can be traced to insufficient integration or component. The types of causes have been split into 2 categories:

- **Component failures:** This category encompasses accidents in which a malfunction / failure on a hardware / software component in the processing function has either caused the accident or raised its level of severity. For these accidents, at least one hardware or software component of the processing function has not operated as planned. Chapter 3 will discuss the root causes of these accidents, which also incorporate organisational issues and factors external to the facilities.

- **Monitoring errors:** This category solely pertains to automated processes controlled or supervised remotely, whereby at least one error committed by an operator assigned to interpret information relayed by the automation processing function, whether in the unit or plant control room, has caused or worsened the accident. Chapter 3 will detail the root causes of such accidents, which are mainly organisational in nature.

Figure 6 *Direct causes of processing function-related accidents*

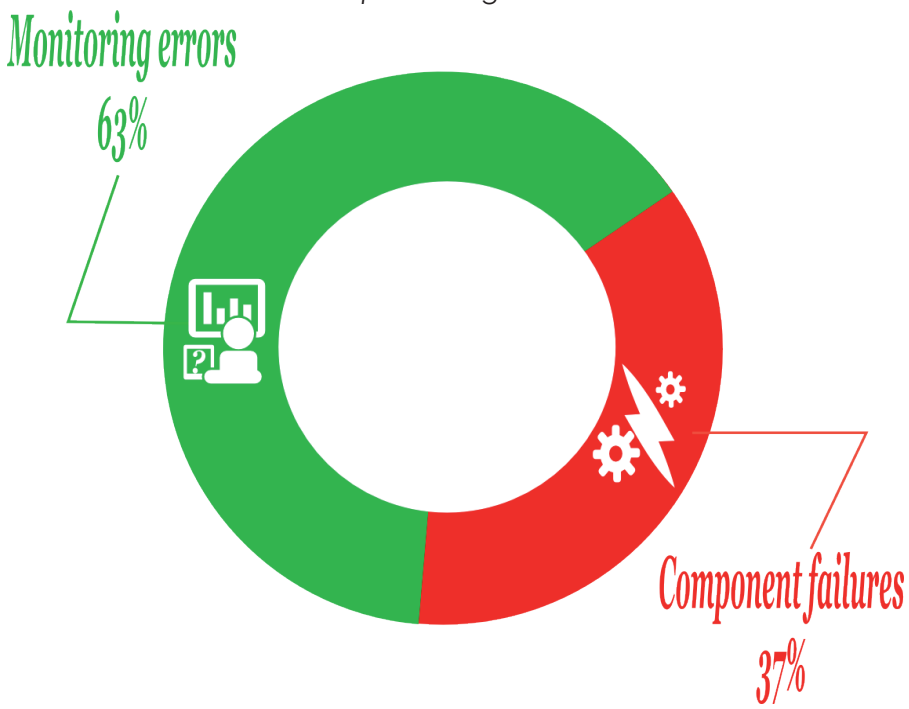


Figure 6 displays the predominance of monitoring errors over hardware component failures. This result confirms the expansion of remote automated control systems at industrial sites [5], with emphasis on the fact that hardware malfunctions on processing chain components remain a major source of accidents.

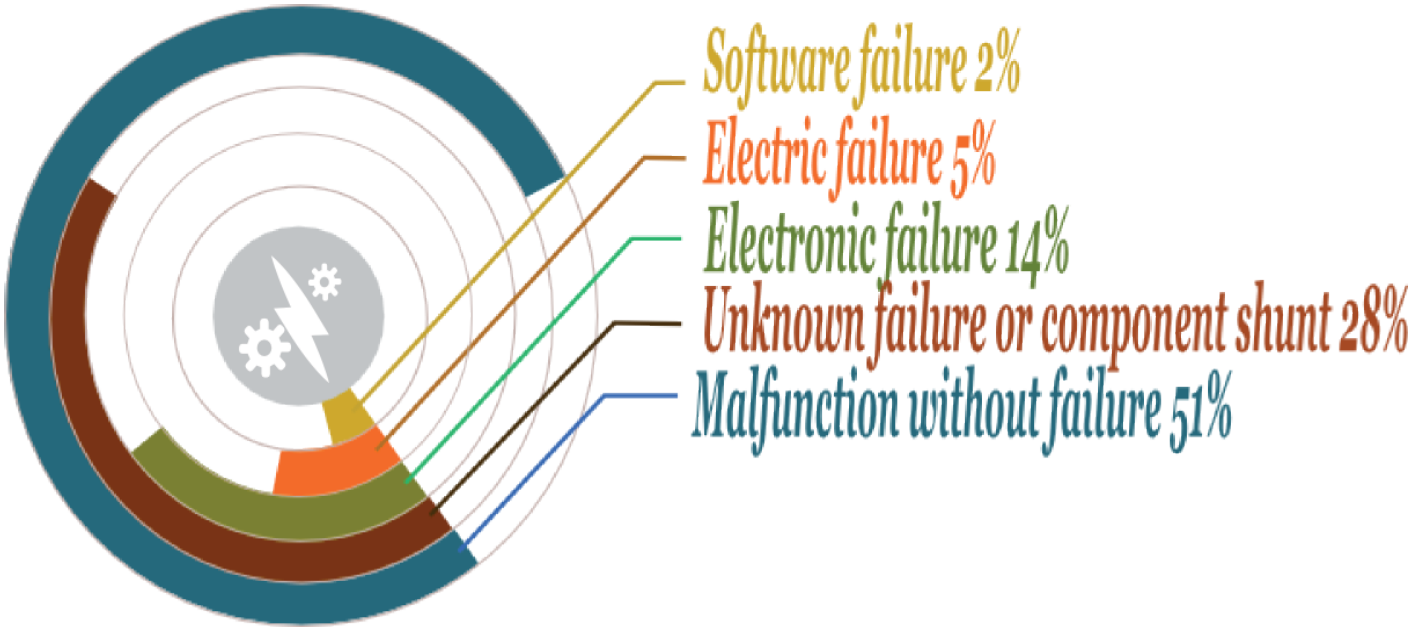
2/3 of the direct causes of accidents involving the processing function are related to human supervision failures, with hardware or software component failures accounting for the other 1/3 of all recorded accidents.

2.1 Component failures

Component failures constitute the leading direct cause of processing function breakdowns (102 cases). While this function is less exposed to process environments than sensors and actuators (i.e. risks of fouling, corrosion and mechanical locking), it is highly dependent on automation programming, which is capable of causing malfunctions without the automated system failing entirely. These factors explain the extent of malfunctions without complete failure in the overall distribution of component failures (Fig. 7).

They also stress how these malfunctions can be difficult to detect for human operators, which underscores the importance of their education and on-the-job training. Moreover, the potential of component failure across the various facilities is cumulative: electronic cards, communication relay switches, cabling, power supply, display screens, central processing units, sound alarm systems, etc. (see accident illustrations on page 14).

Figure 7 *Types of component failures within the processing function*

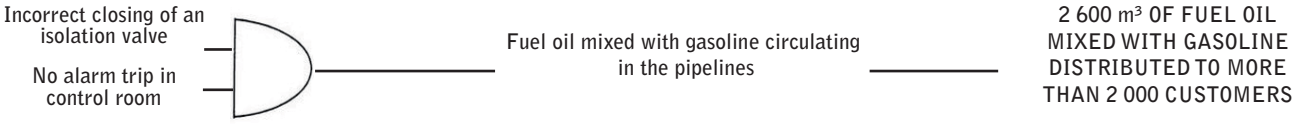


Malfunctions without complete failure account for over half of the component failures of the processing function.

Some of these devices also exhibit vulnerabilities similar to sensors, such as bypasses or electrical power outages. The technology used exposes this component more readily to electronic failures, which are the source of 14% of all component failures associated with the processing function.

MALFUNCTION (ARIA 35774)

15th January 2009

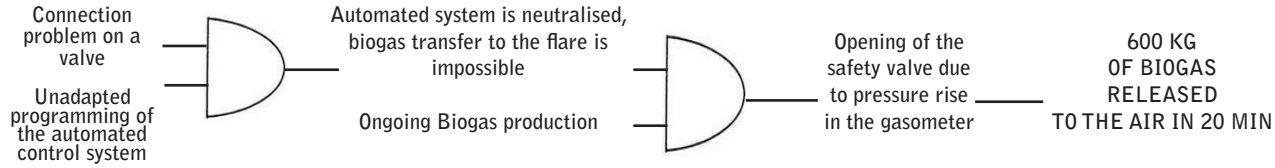


At night, 4,900 m³ of non-compliant home heating oil (containing 17% unleaded gasoline) were delivered by a refinery to a bulk storage company and then partially distributed over the following days to several thousand consumers via a distribution network encompassing 11 departments in north-western France. The fuel oil - unleaded gasoline mix - yielded a 22°C flashpoint (instead of 55°C for «pure» fuel oil), thus leaving it easily flammable and capable of forming an explosive atmosphere in a confined setting (e.g. storage tank). On the same day, a small explosion occurred while filling a delivery truck inside a fuel retailer; the 2 on-site managers sustained slight burns to their foreheads yet did not call emergency services. In all, 2,600 m³ were distributed to 2,070 firms or individuals.A break in the seal between pipelines connecting the refinery to 2 bulk storage facilities caused this incident. **A valve designed to isolate the 2 pipelines delivering gasoline and fuel oil simultaneously to the 2 facilities had not been correctly closed, yet this information relayed to the control room was erroneous.**

OTHER RELEVANT REFERENCES Aria 8885, 18339, 38617, 40986, 41305 , 41736, 41849, 42156

FAILURE DERIVING FROM ACTUATOR (ARIA 38485)

23rd March 2010

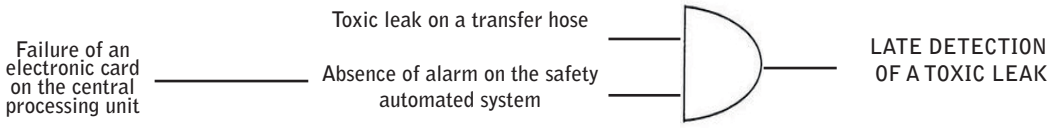


At a Seveso biogas production facility inside a WWTP, a break of sealant occurred at 1:15 am near a gasometer. This sealant loss stemmed from a release of biogas at the gasometer location due to an imbalance between incoming and outgoing flow rates. Once the maximum gasometer capacity had been reached, biogas escaped via the facility's hydraulic safety valve. On the day of the accident, **a physical defect (connection problem) at the end of a valve stroke neutralised the automated mechanism controlling the operational set-up,** thereby blocking the possibilities to transfer or flare the biogas, which when not extracted from the gasometer was subsequently degassed. Incapable of acting remotely, the control room operator travelled to the site in order to manually activate the set of valves on the transfer network, in an effort to rectify the situation. Since one of the valves was «hard» to operate, several minutes of repair time working with a self-breathing apparatus were necessary. The situation returned to «normal» 25 minutes later; 600 kg of biogas had been released (composition: 65% methane, 34% C02, with impurities including H2S at 50 ppm). No adverse consequences were observed outside the facility.
This incident revealed the vulnerability of devices at the end of an operating cycle. The station operator decided to modify system design to increase reliability and extend the detection range. These «hard» valves were replaced to simplify manual handling should the need arise.

OTHER RELEVANT REFERENCES Aria 5989, 27060, 33423, 43146

FAILURE OF AN ELECTRONIC CARD (ARIA 42931)

2nd May 2012



During delivery of dimethyl ether (DME) at a cosmetics plant, a transfer hose swelled around the fitting leading to the stationary installation and leaked due to incompatibility between the hose material and the product being delivered. The control operator noticed the leak and alerted the truck driver, who promptly closed the tank bottom valve and turned off the truck engine. Pressing the emergency shutoff button activated the transfer station security response, and the plant was evacuated for 20 minutes as a precautionary measure. **The accident cause focused on an inoperable gas detection device due to component defect in the electronic cards of the central processing unit (the cards had not been changed since 2001).** The sensors quickly saturated, emitting an «off-scale» signal that was interpreted as «sensor malfunction», without triggering any special action (even though the «off-scale» notification should normally activate safety procedures).**The card manufacturer had in fact identified this potential risk of malfunction back in 2008 and remedied the situation (by changing cards and updating the software). However, all potentially flawed cards at this plant had not been recalled or updated. The plant management proceeded by replacing all cards used on-site.**

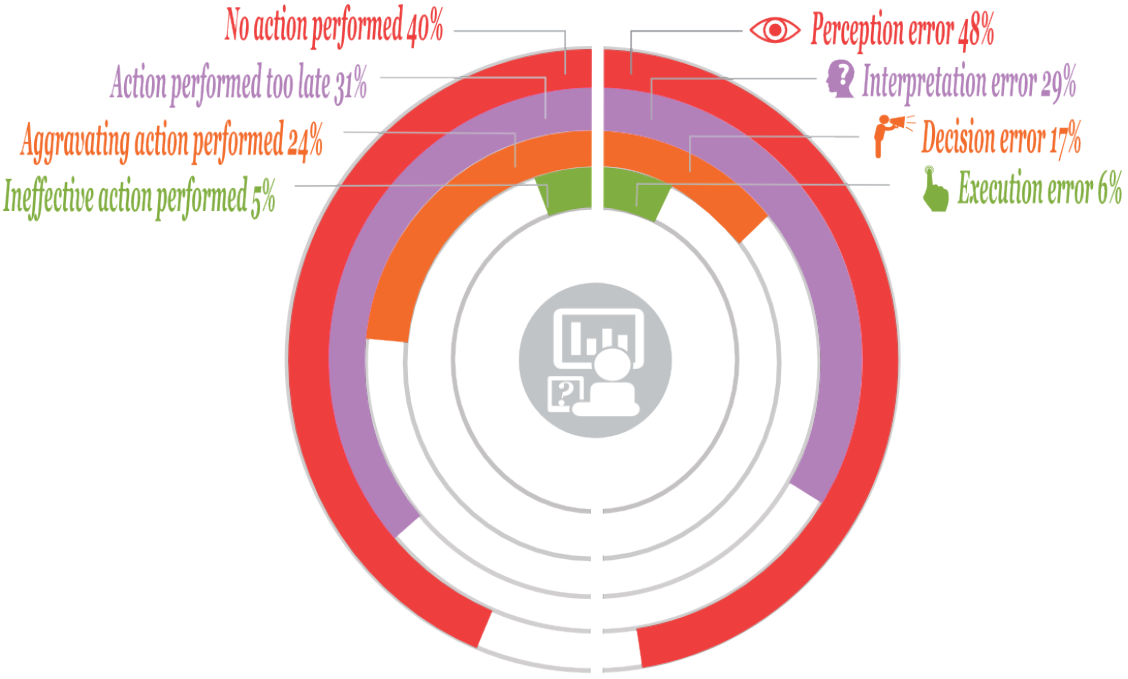
OTHER RELEVANT REFERENCES Aria 3536, 7172, 10064, 21466, 27060, 32624, 39321, 43437

2.2 Monitoring errors

In a context of developing centralised control systems, the role of human operators and supervisors is vital to the successful operations and safety of automated installations. Among refinery employees, the following quip was circulating: «*How many minutes would a refinery keep operating without incident or accident if all employees were evacuated?*». Monitoring errors constitute the direct cause of 63% of accidents involving a processing function failures (173 cases). These failures are most often manifested by inaction or late reaction by control room operators faced with abnormal situations (Fig. 8, left), indicative of root causes tied to control system design, workload, and human operator training (see Chapter 3).

70% of monitoring errors result from the human operator's failure to react or an overly-delayed reaction to an abnormal situation.

Figure 8 *Symptoms (left) and categories (right) of monitoring errors*



To better understand their nature, the various monitoring errors identified have been sorted into 4 categories (Fig. 8, right) as follows:

- **Perception errors*:** The control room operator has not perceived or fully noticed the information sent by the automated system regarding the status of the process or processes under his supervision.
- **Interpretation errors:** The control room operator has accurately perceived the information made available but fails to properly grasp the status of the intended process or processes.
- **Decision-making errors:** The control room operator has fully understood the status of the process or processes yet decides to take action that proves to be inappropriate, or fails to take the appropriate action, with such a decision leading to (or facilitating) the accident or raising its level of severity.
- **Execution errors:** The control room operator has made the right decision but commits an error during execution.

Control room operators' difficulty in perceiving and interpreting information explains over 3/4 of all monitoring errors.

* The notion of perception adopted for this analysis is limited to the availability and display of the exterior signal and does not include the various physiological or mental factors influencing the control room operator's signal perception (e.g. fatigue, on-the-job training, impaired visual or auditory capabilities).

2.2.1 Perception errors

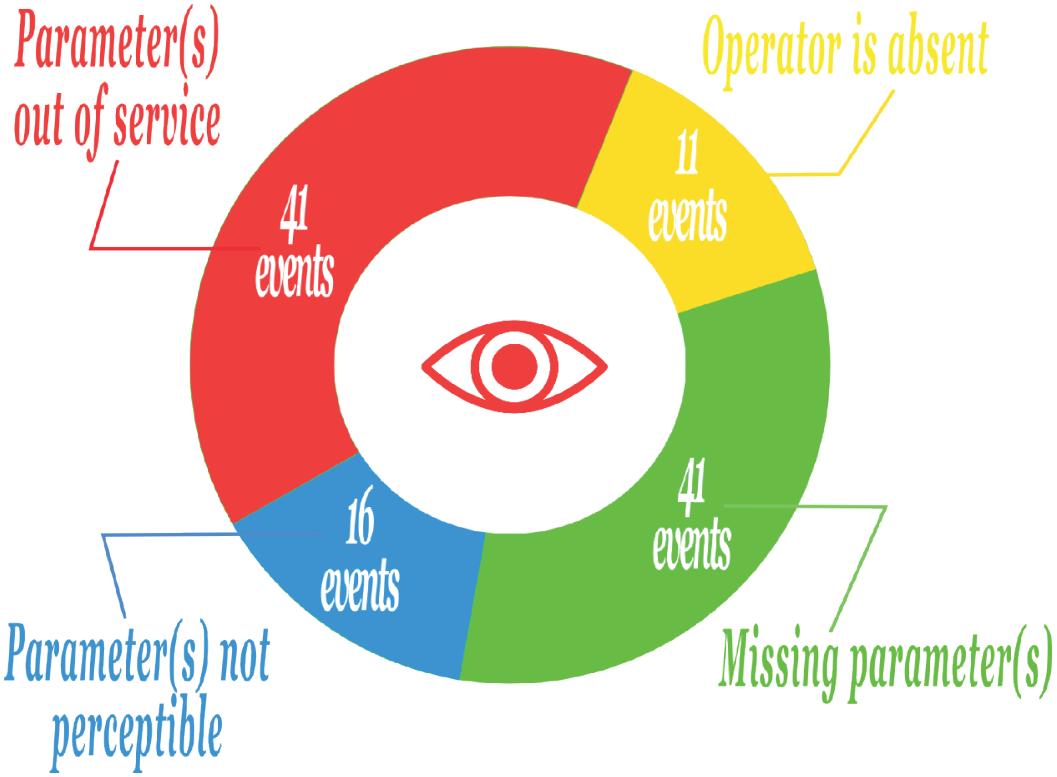
Figure 8 (p. 15) shows that the control operator's perception of information relayed by the automated system is most often the weak link.

Perception problems alone explain half of all processing-related accidents due to monitoring errors.

Perception errors have been placed into 4 subcategories (Fig. 9). This classification reveals that the majority of perception errors cannot be directly ascribed to the control room operator. In fact, some control parameters are unavailable at the time of the accident due to a malfunction or design flaw that has made these parameters impossible to perceive under the control room operator's standard working conditions, or simply because monitoring these parameters had not initially been planned (see: Chapter 3, ARIA 42690, p. 38, and ARIA 12671, p. 43). Moreover, a few perception errors are due to control room operator absence, as the assignment of other urgent tasks has drawn his attention elsewhere. Accident examples involving perception errors are presented on page 17.

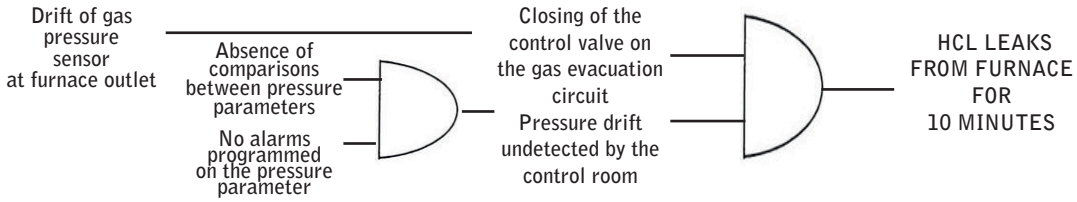
Figure 9

The various types of control errors related to perception



Nearly 80% of control room operator perception errors are caused by a lack of availability of the parameters needed to adequately understand the ongoing situation or make the right decision.

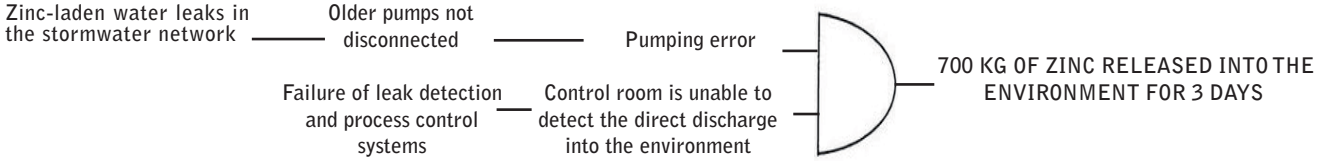
MISSING PARAMETERS (ARIA 30178)
3rd March 2005



In a chemical plant, 0.6 tons of hydrogen chloride (HCl) escaped during a 10-minute period from all furnaces and vents within the potassium sulphate workshop while cleaning the HCl circuits. An employee living adjacent to the site notified the guard house of the presence of a cloud originating from the plant. The emergency sprinkling system connected to the washer was turned on to stop these emissions. Poor calibration of one of the two devices used to measure gas pressure at the furnace outlet (not directly related to the ongoing works), causing the control valve on the gas evacuation circuit to close, was responsible for this incident: since gases were no longer being drawn, they escaped from the furnaces. **The lack of an alarm on this control parameter slowed personnel response, and the absence of any means for comparing the 2 pressure measurements prevented the detection of sensor drift.** To reduce the probability of repeat occurrence, an alarm was installed to detect deviations between the 2 pressure readings; also, a procedure laying out the most sensitive steps, in particular those requiring a supervisor's presence, was issued.

OTHER RELEVANT REFERENCES Aria 4582, 12671, 28389, 32841, 33310, 37825, 41945

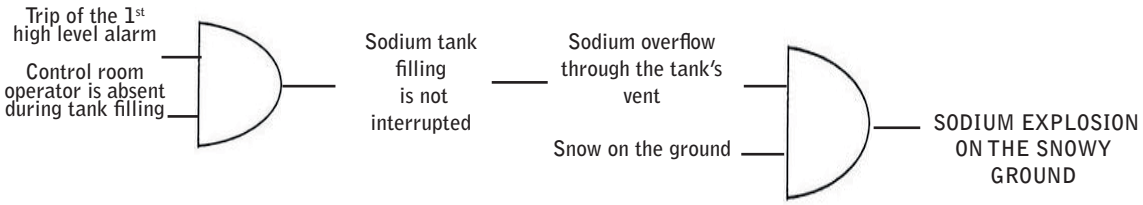
PARAMETERS OUT OF SERVICE (ARIA 26895)
21st January 2004



Zinc-laden water from a metal manufacturing plant was released into a canal during restart operations following periodic maintenance of the lixiviation and electrolysis shops. The establishment is equipped with a polluted rainwater network, connected to a sump enabling it to be transferred to a 5,500 m³ storage tank and a neutralisation-settling tank that had been commissioned the previous year. The sump's older pumps that discharge directly into the canal were kept in place to be used in exceptional situations.. On the day of the accident, leaks on the lixiviation exchangers began flowing into the rainwater network then, due to a pumping error, were released without treatment into the canal for 3 days; 700 kg of zinc were thus released into the natural environment. An inquiry revealed that the operating error was possible owing to the fact that the older pumps were kept locked. A malfunction of the leak detection system and the process control transmission chain to the central computer was also detected.

OTHER RELEVANT REFERENCES Aria 11665, 31376, 32579, 33306, 37041, 41207, 42690

ABSENT OPERATOR (ARIA 15018)
26th February 1999



A molten salt electrolysis plant contained a lower section for carrying out electrolysis and, connected by a salt pipeline, an upper unit where rail cisterns were loaded. In this loading section, two 60-m³ buffer tanks under nitrogen atmosphere and fitted with 3 level alarms had been placed inside a building. Tank filling was being controlled from the lower unit and lasted 2 hours. An upper unit operator was assigned to monitor the filling operation and inform the lower unit should the 1st alarm be tripped. **Occupied by other tasks in another unit on the day of the accident, this operator did not hear the alarm.** Sodium escaped from one of the tank's nitrogen vents exiting outside the building. The sodium exploded upon contact with snow, alerting the lower unit operator, who immediately stopped the sodium transfer. The internal emergency plan was activated. The building's cladding was damaged. In response: the sodium transfer process was hooked up to the alarms; a cold trap was installed on the given vent; and plant procedures were modified.

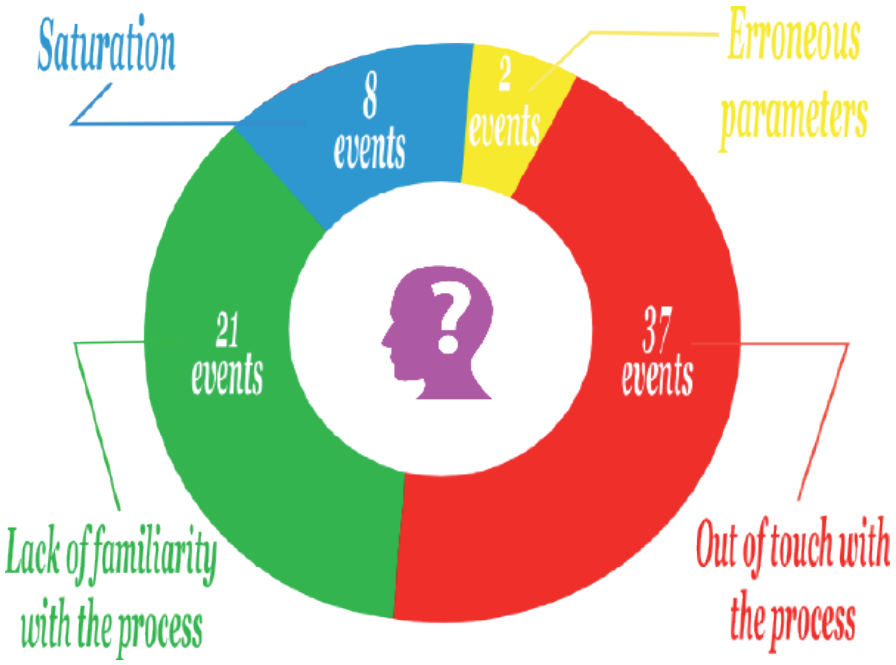
OTHER RELEVANT REFERENCES Aria 7600, 21466, 22988, 24436, 35992, 36061

2.2.2 Interpretation errors

Monitoring errors not caused by the control room operator's failure to perceive essential parameters often stem from problems in trying to understand current conditions surrounding the process under his supervision. The various interpretation errors that arise have been sorted into 4 subtypes (Fig. 10) and expose the root causes closely correlated with the operator's skill level and role in performing assigned control tasks (Chapter 3.1).

Interpretation errors account for over one-fourth of all processing-related accidents caused by monitoring errors.

Figure 10 *The various types of monitoring errors related to interpretation*



- **Lack of familiarity with the process:** This type of interpretation error often arises when a process becomes automated or modernised, or in the event of an exceptional incident on the automation controller. In the case of automation or modernisation, production constraints may trigger rapid service start-up, while control room operators are not yet adequately instructed or trained to oversee a controller. Their professional experience and skill level has not necessarily prepared them to «virtually» supervise a highly automated process requiring knowledge of how to control facilities from a desk, identify key parameters on several screens and build a mental picture of the process situation based on such data. Operators' «field» view of the process is challenged; no longer able to rely directly on their experience, they may become destabilised.

VOICE OF THE FIELD

«My instruction came on the job [...] One of the guys only received training once he had joined the team working the 4x8 shift.»

Testimonial of a control operator at a French pharmaceutical site in 2008 [6]

In an incident involving an automated system, the amount of operator training and practice becomes even more crucial when having to manually override a degraded process situation, thus raising management complexity and requiring quick action to prevent the incident from transforming into an accident (see ARIA 32109, p. 22). An Australian survey conducted in 2005 among a population of control room operators working for railway networks, automated factories and (non-nuclear) power plants found that 51% of respondents felt their level of training to be insufficient; this figure rose to 80% among power plant supervisors [7]. A British survey focusing on 107 automated industrial sites with centralised control systems reported that only 23% of facilities had set up a specific programme to train control room operators in control procedures and emergency situations, 15% included a certification system dedicated to process monitoring, and just 3% possessed a training simulator [5].

Control room in a steel mill during the 2000's

- **Out of touch with the process:** In a highly automated process, the field operator-turned-supervisor isolated in the control room is no longer in touch with the process and has lost the sensorial reflexes (noise, vibration, etc.). His knowledge of the process falters and he risks losing the intimate familiarity he had developed with the components. The process becomes a «black box», with his concentration drawn exclusively to the exposed virtual part, i.e. information transmitted by the automated system in the control room. He must then build a mental image of the process based on this filtered information, thus encountering difficulties to fully perceive the link between activation of a command and the start-up of an component, whose precise location in the unit may not be well known. Moreover, the effects of this command on the process may only be visible on the displays a few hours after his shift has ended, depriving him from an useful feed-back.

VOICE OF THE FIELD

«People swear by what they see on the displays. Young people operate according to computer logic and don't get out into the field. They feel more comfortable in front of their computers.»

Testimonial of a French chemical process engineer in 2008 [6]

The relative «comfort» of the control room (coffee, music, seats, heating, air conditioning) and immediate availability of control parameters on dispalys do not motivate control room operators to make rounds inside the unit to gather first-hand «field» knowledge of the process, which would mean sliding between dirty, noisy or hazardous component when it might be freezing or raining outside. Control room operators lose familiarity with critical parameters, detach themselves «mentally» from the process and ultimately are unable to interpret abnormal situations easily and quickly (see ARIA 43147, p. 22, and ARIA 12671, p. 43).

The root causes of this «loss of contact» appear to be less well correlated than expected with human operators' intrinsic capacities than with the organisational factors that draw him into a routine or limit his capacity to grasp the situation by presenting too many or too few pertinent parameters (Chapters 3.3 and 3.4).

VOICE OF THE FIELD

«At first, the control room was staffed and security officers made rounds in the unit. Little by little, the security people made their way into the control room, leaving us without much knowledge of what's taking place inside the shop. Now, no one knows what'll happen when we hit the button.»

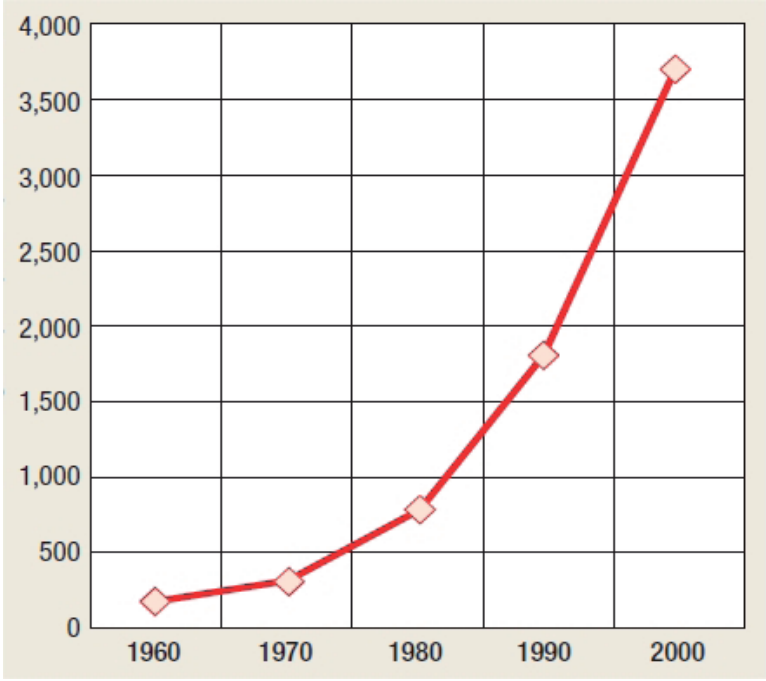
Testimonial of a foreman at a French chemical site in 2008 [6]

«Since we adopted the new technologies and introduced [automated] systems as far as the eye can see, we've lost control over what we're doing.»

Testimonial of a control operator in a Canadian refinery [8]

- **Saturation :** The control room operator, suddenly overwhelmed by unsorted information transmitted by an automated system, is no longer able to draw an accurate assessment of the situation at hand and winds up ignoring the data due to its lack of utility. The most common case is a restart phase with many alarms ringing in the control room and being ignored. Such was the backdrop to an accident in a North American refinery which turned really serious due to inaction by the control room operator, who had to process over 300 alarms in less than 5 minutes [9]. In 1994, the 2 operators working the control room shift at the *Milford Haven refinery* (UK) were overwhelmed by 275 non-prioritised alarms in 11 minutes: they fled the control room shortly before the refinery exploded! A poignant example of control room operator saturation at a French refinery is presented at the bottom of page 22.

Figure 11 *Trend in the number of different alarms an oil platform control operator is required to process between 1960 and 2005 (source: World Oil, September 2006)*



Studies on the topic of control room alarm management undertaken since the beginning of the 2000's (some results of which are listed in Table 1) clearly demonstrate that the operator's capacity is not the problem, but rather the exponential increase in the number of control room alarms, which now by far exceeds operators' processing capabilities (Fig.11). In 2011, a French industrial project manager estimated that just 20% to 40% of control room alarms were really necessary [10].

A 2012 survey conducted in the United States across a panel of industrial sites with a centralised control facility (broken down 52% heavy industry, 33% manufacturing and 15% pharmaceuticals and food processing) indicated that half of the surveyed sites were not equipped with any method for managing alarms, while 70% of respondents recognised that the excessive number of alarms had negative impacts on process production and safety [11].

This survey concluded that the situation had more to do with problems of corporate culture and personnel training than with a lack of methodology, since many well-known alarm management and prioritisation methods are available and some have even been included in international technical standards, like ISA 18.2.

	Oil	Chemical	Energy	Other	EEMUA 191 Standard	ISA 18.2 Standard
Average daily number of alarms	1200	1500	2000	900	150-300	150-300
Maximum number during a 10-min stretch	220	180	350	180	< 10	Maximum of < 10 over 2.5 hours
Average number during a 10-min stretch	8	9	8	5	1-2	1-2

Table 1

Comparison between control station alarm frequencies, as measured in various North American industrial sectors, and the frequency recommended in best practices [12]

VOICE OF THE FIELD

«Information systems currently add a quantity of data that's too much for an operator to fully process.»

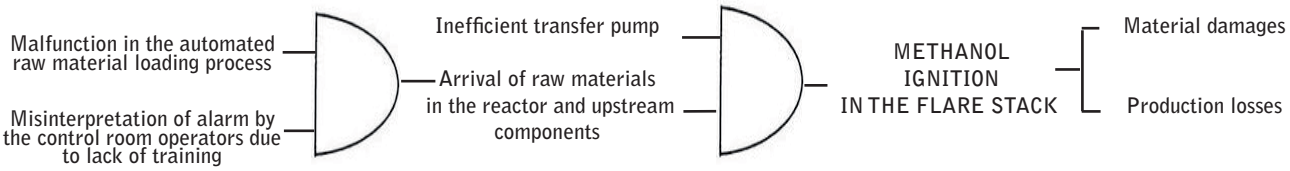
Testimonial of an industrial project manager [10]

«In the petrochemical sector, losses due to false alarms amount to between 10 and 20 billion dollars. The cost of a typical incident: $100,000 to $1 million.»

Testimonial of a North American industrial consultant [10]

- **Erroneous parameters:** This type of interpretation error is much less frequent (fewer than 1/10 of all interpretation type errors). In this case, the erroneous information provided to the control room operator during an accident prevents him from correctly analysing the unfolding situation regarding the process under his supervision (see ARIA 35774, p. 14, and ARIA 40969, p. 31).

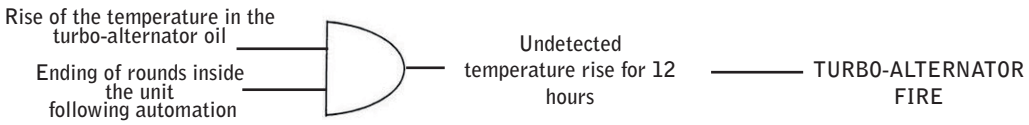
LACK OF FAMILIARITY (ARIA 32109)
12th July 2006



At around 8:30 pm, fire broke out at a chemical plant in a biofuel unit flare during diester production involving the transesterification of vegetable oil by methanol. The installation was secured by means of shutting off both the methanol and gas supply lines. Fire-fighters brought the blaze under control within roughly 10 minutes. The consequences were limited to the flare despite the tremendous heat flow generated; the instrumentation and low-voltage section were destroyed, and the metal parts (pipelines, supporting structures) also sustained damage. The unit located 80 m away was shut down for several weeks and about 10 employees had to be made redundant. Vegetation was charred within a 20-m radius around the flare. A malfunction in the automated raw material loading process (oil, methanol, catalyst) has caused this accident; the reactor and all associated component (condenser, external pipes, buffer tank upstream of the flare, etc.) became filled with the reaction mixture. Though activated by the high level alarm, the transfer pump was unable to lower the buffer tank level and prevent the mixture from entering the transfer line heading towards the liquid methanol flare, which subsequently ignited. Multiple safety device failures and deficiencies were to blame, including: surpassing the very high level failed to trigger the installation security procedure, as just a single control station alarm was tripped; **loading station malfunctions went undetected; and control room operator response was considerably slowed due to a lack of proper training.**

OTHER RELEVANT REFERENCES Aria 2684, 6093, 27585, 33333, 33838, 35432, 41207

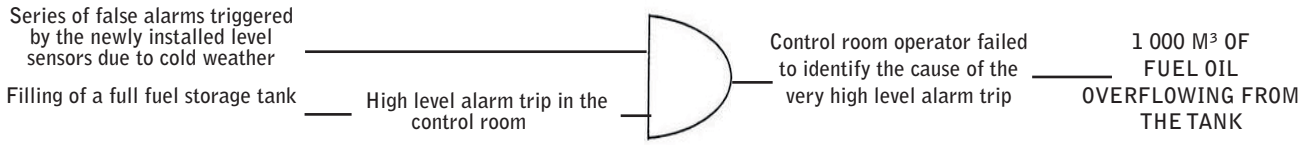
OUT OF TOUCH WITH THE PROCESS (ARIA 43147)
16th October 2002



As part of the procedure to restart a conventional power plant, the turbo-alternator was placed back into service on 15th October at 2 pm and then coupled to the electrical national network without any glitches. Between the evening of the 15th and the following morning, an abnormal temperature rise caused the self-ignition of oil in the oil tank and a fire around the turbo-alternator. Several remedial measures were adopted, namely: installation of a high-temperature safety feature, elimination of filters (limiting the oil flow rate), and a reminder disseminated to all control room operators regarding rounds to be carried out inside the unit. **The introduction of automated mechanisms to facilitate the start-up and monitoring of heavy machinery during this critical phase gradually led to neglecting the precautions that in the past took field operators for several days to ensure that stable operating conditions had indeed been reached. Monitoring efforts involving filters, a range of temperature readings (especially thresholds) and listening for vibrations had generally enabled adopting remedial measures before the alarm announcing a near certain state of degradation.**

OTHER RELEVANT REFERENCES Aria 12671, 15397, 30920, 32632, 41207

CONTROL ROM OPERATOR SATURATION (ARIA 40584)
28th May 2011



During rounds while changing shifts inside a refinery, an employee witnessed a fuel oil storage tank overflowing at around 5 am. The filling operation was immediately stopped and the tank isolated; moreover, 1,000 m³ of hydrocarbons recovered in the retention basin were transferred to other tanks, as well as to the grease trap system for recovery in recycling tanks. The tank was already full when at 1:30 am it was mistakenly scheduled for filling. The control room operator had requested that the field operator close the manual pouring valve leading to this tank, but the field operator instead closed the tank's recirculation valve. By 4 am, the tank was overflowing its retention basin. Detected by the centralised control alarm system, these unwanted product transfers had not been recorded in time by the control room operator. The radar-type level sensors equipping the northern site's tanks were being replaced due to obsolescence. **The newly-installed sensors triggered many false alarms in the control room on the account of the cold spell, causing higher than normal consumption in the tanks at night.** This problem of adjusting the detection threshold was being resolved when the accident occurred: **the control room operator was unable to identify the alarm indicating an overflow on the affected tank amidst all the very high level alarms on adjacent tanks continually relaying false readings to the displays.**

OTHER RELEVANT REFERENCES Aria 26880, 30406, 30687, 33094, 38617, 43042, 43455

2.2.3 Decision-making errors

Decision-making errors account for just a small share of all monitoring errors studied, yet they often expose faults in the control room operator's interaction with the automated system. Of the 4 types of decision-making errors presented in Figure 12, two involve a decision-making bias due to attitudes held by the human operator regarding the system under his supervision.

The majority of decision-making errors relate to a context in which the control room operator shows distrust of the automation system.

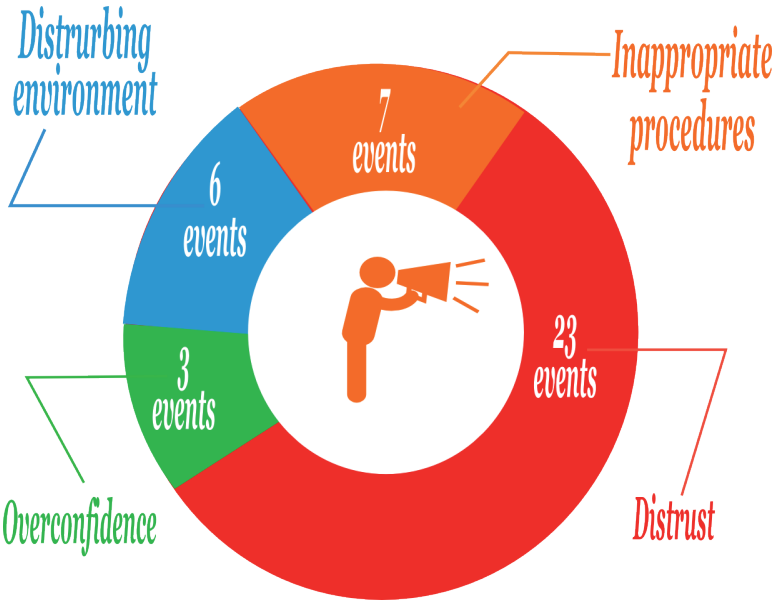


Figure 12

The various types of monitoring errors related to decision-making

- **Distrust towards the automated system:** Present in the majority of decision-making errors analysed, this observation often reflects a schism between «management», which decides to automate process controls, and «staff» required to adjust to new working methods. In practice, the control room operator is assigned to assess the performance of the supervised automated system; should he consider that the system lacks reliability or efficiency, he'll tend to lose confidence in the parameters it relays and rely on his own perception of the situation. Accident statistics reveal that such situations are more likely to arise outside of normal operating phases (e.g. start-up, component failure), when alarms are activated in series or waves, leading control room operators to simply ignore them. This situation may prompt the operator to «bypass» the automated system in order to undertake actions he considers better adapted, yet in reality might turn out to be disastrous. This is typical of situations where subsequent to a series of design flaws, the automated system actually disturb or complicate operators' basic tasks (frequent false alarms) or generate significant production and efficiency losses (see ARIA 37139, p. 25, ARIA 33333, p. 31, and ARIA 21466, p. 41).

  Studies have also shown that a perverse effect may arise when such a bypass causes an accident: it convinces management to further restrict control room operators' freedom of action with respect to the automated system, thus creating an «over-automated» environment that often leads operators to apply an even more complex and riskier strategy to circumvent the automation [13]. Loss of contact with the process, as discussed in Chapter 2.2.2, may exacerbate this distrust, further motivating control room operators to bypass the automated system given that they often ignore the accidental consequences of this bypass.

- **Overconfidence:** This type of decision-making error is the opposite of the distrust exposed above: in considering the automated system to be highly efficient and reliable, the control room operator tends to become complacent and mentally detached, leaving the system to «run» the process without human supervision for extended periods of time, e.g. to perform ancillary tasks, take a small break or recover from momentary fatigue.

A vicious cycle may ensue: as the control room operator becomes more inclined to neglect his supervisor's role, his familiarity with the process declines and he tends to rely on the automated system, to the detriment of his critical reasoning (ARIA 32640, p. 25). An analogous trend has been identified in the field of civil aviation whereby following several disasters, some experts began denouncing *«pilots under the control of automated mechanisms, when automated mechanisms should be under pilot control»*.

«The real danger does not lie in computers taking over man's thought processes, but rather in man starting to think like a computer.»

Sidney J. Harris, north-american writer and journalist

This complacency may lead a control room operator to miss critical alarm signals. In resuming his supervisory role, he needs time to fully understand the situation while the accidental sequence is already well underway. This overconfidence might also result in a loss of critical reasoning and blind reliance on an automated system regardless of the physical evidence at hand (e.g. smoke, abnormal noises, contradictory indicator readings). Such an attitude is not exclusive to novice operators; an experiment conducted in 1994 on experienced airline pilots revealed that half of them continued to use the automatic pilot even as several findings had proven its deficiency. Another study carried out in 1997 indicated that operators on average were able to detect automated system defects only 40% of the time when the system was exhibiting constant reliability and 70% of the time when exhibiting erratic operations [13].

- **Disturbing working environment:** This type of error arises when a control room operator (or group of control room operators) must make a decision in the presence of an atypical, hence infrequent, situation. Some aspects of the working environment will disturb the decision-making process. For one thing, stress is felt from having to make a decision, within a short period of time (in most cases no more than 10 minutes), that will often be irreversible (no margin of error). Also, the decision-maker is under pressure, or places pressure on himself, due to the major stakes involved: risk of worsening the accident, economic losses for the plant or extra work for field operators in charge of placing the process in a safe state or restarting it (see ARIA 28880, p. 28). The results of various studies focusing on the probability of poor decision-making by control room operators faced with an abnormal situation found it to be quite high during the first 10 minutes of a critical situation: 70% on average, with a figure always above 10%, for experienced and well-trained human operators, e.g. according to the THERP method [19].

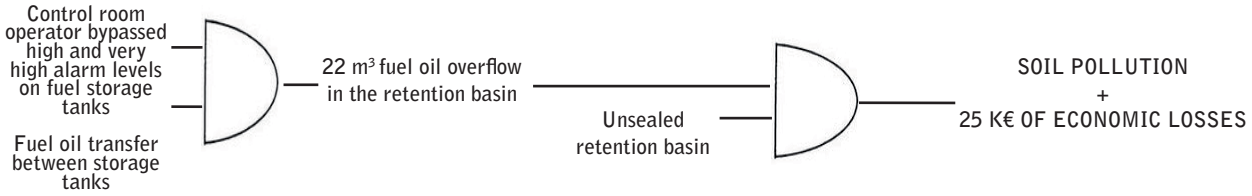
VOICE OF THE FIELD

«It's all beautiful and simple when everything's going right, like a fire-fighter when there's no fire to put out, just running tests or making rounds. But when a problem arises, that's when you've got to make the right decision straight away and that's when the situation becomes stressful.»

Testimonial of a control room operator working at a Canadian refinery [8]

- **Inappropriate procedures:** During an abnormal situation, the control room operator must often refer to written procedures as a decision-making guide. Yet such procedures sometimes turn out to be incomplete or inappropriate for the given situation, which had not been anticipated when the procedures were written. The operator will then base his decision on the applicable procedural guidelines or else use such guidelines to select an option from among several eligible possibilities. Should he be unable to assess the relevance of the given procedure for the abnormal situation playing out (see the concept of «regulated safety» vs. «managed safety» [18]), his respect for the procedure leads him or directs him to make a wrong decision. A 2012 North American study found that 40% of operating errors committed during abnormal or atypical situations in an industrial setting originated from incomplete or poorly written procedures [15] (see ARIA 24639, p. 25).

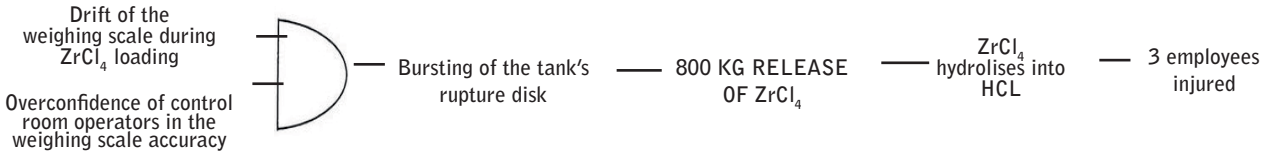
DISTRUST OF THE AUTOMATED SYSTEM (ARIA 37139)
28th July 2009



Inside an electric power plant, a transfer of domestic fuel oil from the primary tank (2,450 m³) to the daily supply tanks, initiated around 4 pm, did not stop automatically even though the high level had been reached. At 11 pm, the watchman noticed an accidental overflow of fuel oil in the retention basin associated with the daily supply tanks. The transfer process was halted. Since the retention basin was not completely sealed, fuel oil seeped out in several places, polluting the soil. In all, nearly 22 m³ of fuel oil had spilled. The plant operator estimated operating losses at €25,000. **A control room operator had forced continuation of the fuel oil transfer by overriding the high and very high alarm levels on the daily tanks.** The environmental inspection also noted: the absence of guidelines for combustible transfers, no sound alarm in the event of overpassing high and very high levels, plus the lack of personnel response upon activation of the supervisory system alarms both on-site and on remote sites.

OTHER RELEVANT REFERENCES Aria 164, 4908, 11107, 15397, 20490, 21466, 36496, 42163

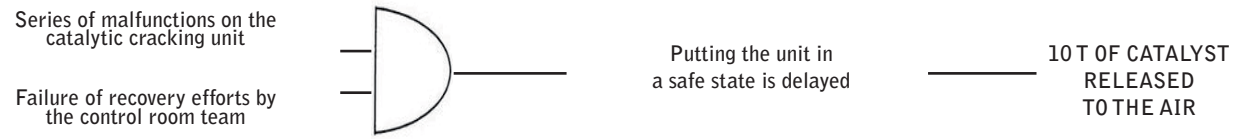
OVERCONFIDENCE (ARIA 32640)
10th January 2007



A spill of 800 kg of zirconium tetrachloride ($ZrCl_4$) occurred around 1 am in the carbo-chlorination unit of a chemical site as the result of rupture of the vent pipe on a storage tank. During clean-up of the $ZrCl_4$ spilled outside, a cloud of hydrogen chloride (HCl) formed by hydrolysis. The process in question used two compactors supplying 3 $ZrCl_4$ storage tanks of 150 t each via a pneumatic transport pipe under nitrogen. During the accident, both compactors were supplying the 1st storage tank loaded at 132 t, according to the weighing scale, while the other two remained empty. At 00:50 am, the high pressure threshold for the 1st tank was being continuously exceeded, thus indicating that the rupture disk had been broken. The HCl sensors of the building exceeded their alarm threshold (5 ppm) 1 minute later. Lastly, the 2nd compactor was only shut down at 1:50 am by staff; the $ZrCl_4$ escaped through the rupture disk and the broken PVC vent pipe. An analysis of the causes of this accident revealed that the instrumentation system associated with the pressure sensor had only been attached to the 1st compactor and had no effect on the 2nd. The transfer of $ZrCl_4$ therefore continued for an hour after both the disk and pipe broke. This situation resulted from poor management of installation modifications: the compactors, initially set up to supply just one tank each, had been changed to allow supplying several tanks through a switch system, without the safety instrumentation being upgraded. **In addition, control room operators did not intervene during repeated activation of the pressure alarms, preferring to trust the weighing scale data, which indicated a fill level of 132 t for a capacity of 150.**

OTHER RELEVANT REFERENCES Aria 22988, 42920

INAPPROPRIATE PROCEDURES (ARIA 24639)
10th January 2003



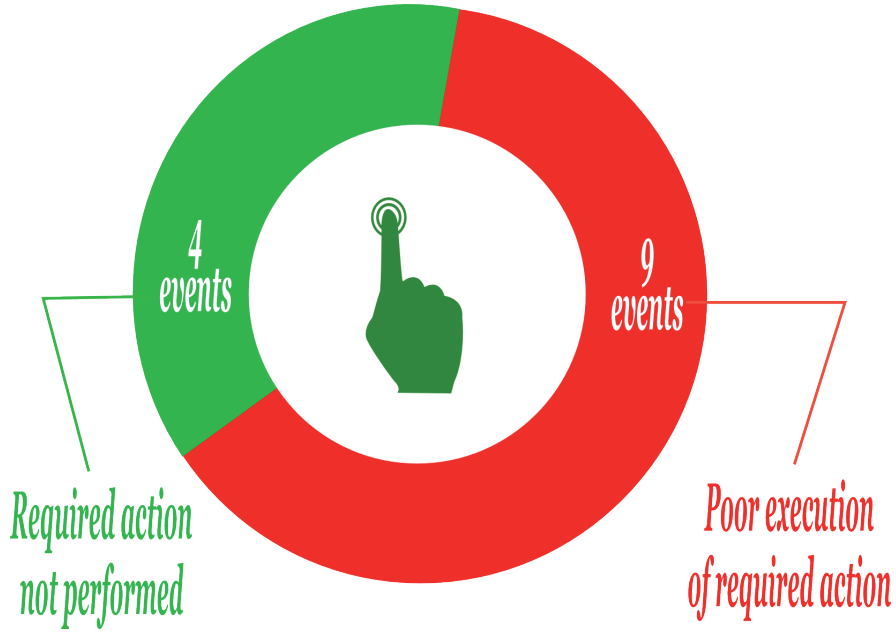
In a refinery, a series of malfunctions on the catalytic cracking unit caused 10 tonnes of catalyst to be sent to the stack. At the beginning of the afternoon, an initial operating anomaly appeared: activation of a boiler involved in supplying air to the regenerator. No anomaly was detected inside the reactor. A half-hour later, a lower reaction temperature was recorded. Pressure at the level of the reactor and regenerator simultaneously dipped, while differential pressure at the cyclone separators increased. The high level alarm sounded on the tertiary cyclone. The catalyst level then dropped a number of times at the bottom of the stripper and regenerator. Control room operators used all variables available in order to restore a normal situation, but given the limited impact thus far decided to apply the emergency strategy developed subsequent to previous incidents and shut the unit down at 6:30 pm. An initial assessment indicated the discharge of 10 tonnes of catalyst to the stack **The effort to normalise the situation had lost precious time and triggered a secondary discharge of catalyst to the stack. The refinery operator revised the facility's inadequate operating guidelines** and lowered the alarm threshold setting on the tertiary cyclone high-level detection.

OTHER RELEVANT REFERENCES Aria 21026, 21516, 32632, 33838, 40014, 42613

2.2.4 Execution errors

Monitoring execution errors occur the least often among the accidents studied. This observation can be explained by the fact that such errors are situated at the end of the cognitive chain (see Chapter 2.2), as well as by the fact that control room operators or mobilised staff successfully rectify the majority of this type of error, in spite of its high occurrence rate (i.e. 70% to 80% of human errors [18]). In all cases, these errors pertain to both poor execution of the required action (i.e. manipulation error) and its non-execution (oversight).

Figure 13 *The various types of monitoring errors related to execution*



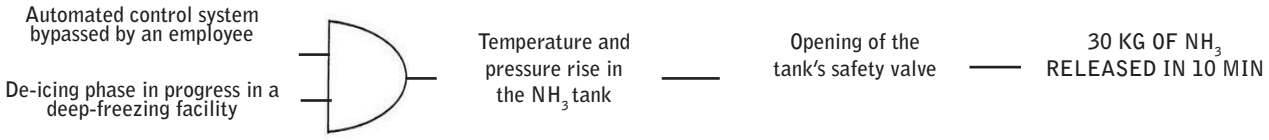
- **Required action not performed:** In many instances, the failure to execute a required action is correlated with an operator dealing with a high level of stress. Control room staff must respond to alarms appropriately, which entails paying continuous attention, to a point of overlooking an action previously decided among the many actions required over a short time frame. The stress level only rises during a solo shift (at night), most likely since automation often serves to drastically cut back on personnel, at a time when a complex situation needs to be resolved (see ARIA 38617, p. 27).
- **Poor execution of a required action:** These errors encompass all those the control room operator is capable of committing during the routine course of his mission, like mistakes (e.g. programming oversight, unintentionally pressing a button) or an incorrect data entry value. An example of an accident produced by this kind of error is presented at the bottom of page 27.

VOICE OF THE FIELD

« Control room activation: in somewhat of a fog, you've got no time to focus, stress is running high, the adrenaline's flowing. To be efficient, avoid all missteps. The indicator lights are blinking, the alarms ringing, the printers rattling…»

Testimonial of a (night shift) control room operator at a chemical plant [14]

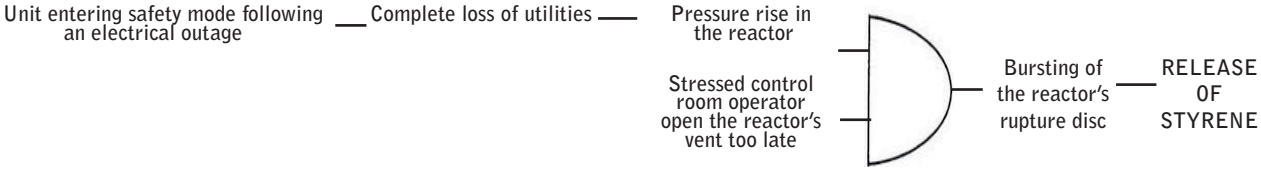
DECISION - DISTURBING WORKING ENVIRONMENT (ARIA 28880)
05th January 2005



Inside a deep-freezing facility, 30 kg of gaseous ammonia (NH_3) were released at 10:08 am for a 10-min period via the safety valve at a refrigeration installation. Slightly intoxicated, 2 subcontractors working onsite had to be hospitalised as a precaution; moreover, 10 plant employees were examined at the scene and another 30 individuals were evacuated. **In seeking to accelerate an component de-icing phase, an employee who had completed the refrigeration specialist training module and was certified to work on this type of installation decided to shift into manual mode to turn off the condenser cooling fans supplying the installation's high-pressure tank.** Though de-icing took place more quickly, it nonetheless did so on an installation operating in an unstable regime: drop in compressor cooling, followed by an increases in temperature and in pressure in the high-pressure tank until exceeding the safety valve pressure.

OTHER RELEVANT REFERENCES Aria 21466, 34477, 38674, 39384, 42163

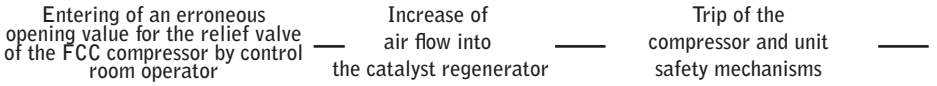
ACTION NOT PERFORMED (ARIA 38617)
14th July 2007



At 10:46 pm during a thunderstorm, an electrical outage interrupted polystyrene (PS) production at a Seveso-classified site. A safety disc broke and styrene was released. To minimise the effects of micro-outages (due to thunderstorms) on PS output quality, the site operator typically switched shop power supply onto the 4 electric generating sets of the facility's Peak Day Withdrawal (PDW) unit. This manoeuvre was performed at 10:20 pm, with 3 sets still available. At 10:43, the thunderstorm knocked out the 1st set. Since the 2 remaining sets were no longer sufficient, the unit entered into safety mode at 10:46, closing all utilities.An employee tried to restart the PDW unit; the on-call electrical maintenance operator was called at 10:53 pm. By 11:05 pm, pressure on the 1st synthesis reactor had begun to rise. As per emergency procedures, gyro monitors started up at 11:15 to remove eventual vapours at the reactor line vent. The site was connected to the grid at 11:18 but the units were only allowed to resume operations a short time later. At 11:20, the disc on the 1st reactor burst at 5.8 bar, spraying a liquid mix containing 10 tonnes of PS and 3 tonnes of styrene.The runaway reactor was caused by the loss of utility service. **The control room operator opened the vent too late, given all the actions required to put the 3 polystyrene lines into safe mode, in accordance with procedures.**

OTHER RELEVANT REFERENCES Aria 2900, 23893, 26363, 41518

POOR EXECUTION - MANIPULATION ERROR (ARIA 33334)
15th July 2007



At 9:03 pm, **the control room operator responsible for the catalyst section of a refinery's fluid catalytic cracking (FCC) unit entered an erroneous opening value for the atmospheric relief valve at the discharge of a compressor blowing the air needed to suspend a catalyst inside the regenerator.** This valve deviated some air flow to the compressor discharge in order to protect the compressor from pumping phenomena. **The operator on duty had input, then validated, an erroneous valve opening control value (less than 10%), when he actually wanted to lower the value from 20% to 19.5%.** This instruction wound up increasing air flow to the regenerator and subsequently tripping the safety mechanism for the compressor and then for the entire unit. The 15-minute unit decompression caused flare emissions, followed by a gradual shutdown. The facility management brought the unit back online incrementally between 11 pm and 5 am, resulting in new flare emissions. The updated guideline requested the panel operator to no longer enter a value, but instead solely use the «up» or «down» arrow commands to increment the initial value by 0.5% or max 1%.

OTHER RELEVANT REFERENCES Aria 4582, 5900, 31307, 33516, 35533

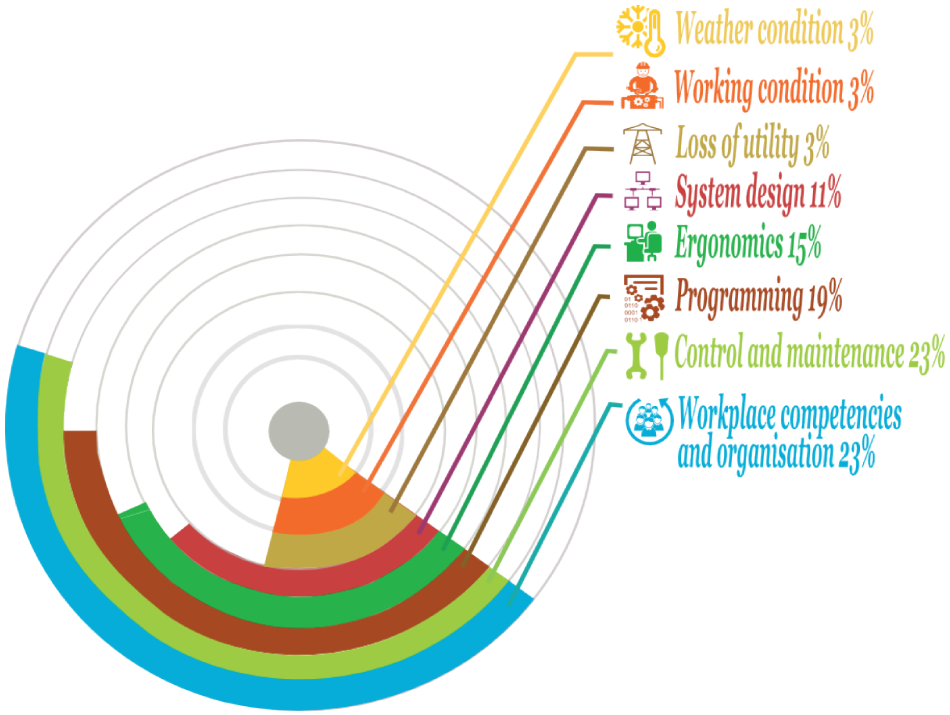
3. Accident root causes

An analysis of the root causes of accidents involving the processing function can be broken down into 8 major categories, namely:

- problems of workplace competencies and organisation
- inadequate control and maintenance
- Programming errors
- unsuitable workplace and interface ergonomics
- system design errors
- loss of external utility
- unsuitable working conditions
- hostile weather conditions

An accident triggered by a (component or monitoring) failure in the processing function may be due to several root causes at once (e.g. an accident involving a hardware malfunction caused by both inadequate maintenance and a control error tied to a lack of proper training). For this reason, the number of accident root causes identified and presented in Figure 14 (i.e. 314 in all) exceeds the total number of accidents with processing function failure (275).

Figure 14 *Presentation of accident root causes involving the processing function*



Two groups of causes, each accounting for over 10% of all catalogued root causes, are evenly split: one group tied to the automated system specification and design phases (focusing on hardware design, programming and ergonomics), the other tied to common operating conditions of the automated system (workplace competence and organisation, control and maintenance).

The 1st group, relative to specifications and design, accounts for 45% of all root causes (vs. at most 31% of causes for accidents involving sensors within the largest, heavily automated industrial sectors [1]). This observation confirms that in order to lessen the risk of accidents occurring to the processing function, which remains the «brains» of the automated system, it is essential to ensure high-quality specification and design for all automation components: power supply, cabling, electronics, software, control interfaces.

The 2nd group, tied to operating conditions of the automated system, accounts for 46% of root causes, while it made up 60% to 90% of the sensor-related accident causes recorded in industrial sectors [1]. The fact of being less exposed to industrial process environments and the predominance of electronic components over mechanical components could lead to reducing the occurrence of problems involving flawed maintenance and deficient component of the automated system.

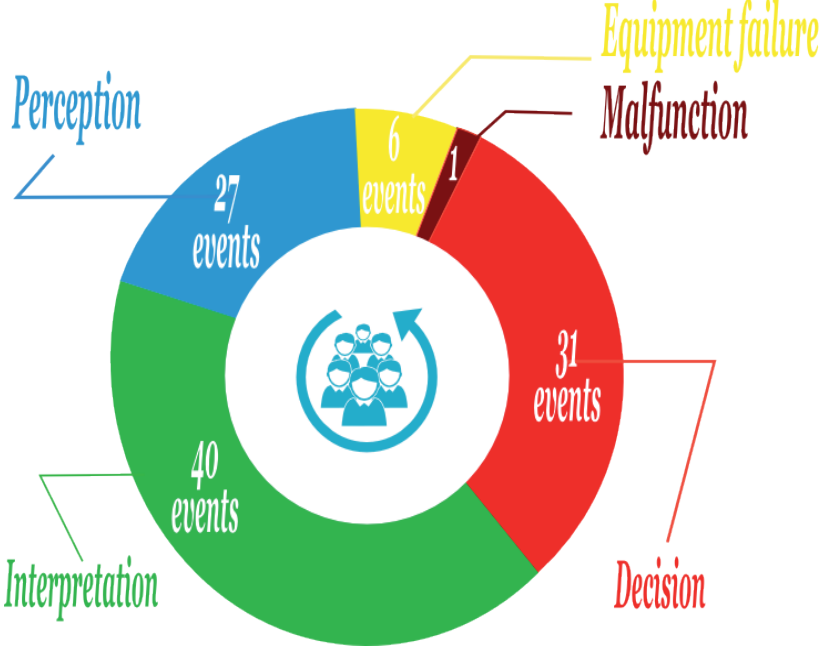
90% of root causes in processing function-type accidents are split evenly between automated system operations (organisation, controls, maintenance) and automated system design (choice of component, programming, ergonomics).

3.1 Workplace competencies and organisation

The «Workplace competencies and organisation» root cause involves, first and foremost, those monitoring accidents caused by inadequate training and hands-on practice by control room operators. These personnel are often constrained to overlook important information or, should the information be correctly perceived, interpret it erroneously or use it to make a wrong decision due to a poor understanding of process operations and the significance of key control parameters (see Fig. 15 and ARIA 33333, p. 31). Moreover, inefficient workplace organisation can lead to assigning the control room operator ancillary tasks that detract him from his primary mission or require him to leave the control room, resulting in a late detection or non-detection of abnormal situations (see ARIA 15018, p.17). The survey conducted by HSE in 2002 across 107 English industrial sites equipped with automated control systems found that 37% of control rooms were not permanently occupied and, moreover, in 90% of those that were occupied, the control room operator on duty was frequently absent performing other tasks [5]. For its part, the North American study carried out in 2012 underscored the contribution of incomplete or poorly written procedures to accident occurrence rates [15].

Problems associated with training control room operators and organising their tasks account for nearly 1/4 of all root causes and are mainly exhibited by monitoring errors.

Figure 15 *Direct causes stemming from workplace competencies and organisation problems*

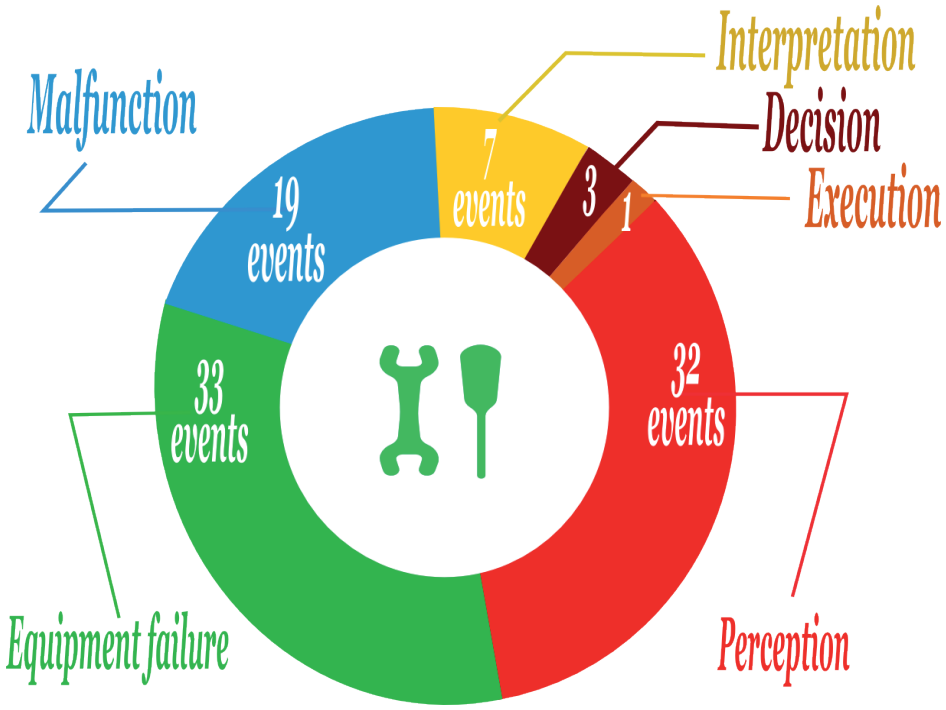


3.2 Control and maintenance

Control and maintenance insufficiencies constitute the other most commonly cited root cause; however, as opposed to the problems of workplace competencies and organisation cited, these insufficiencies mainly give rise to component failure and are largely responsible for downtime and malfunctions (Fig. 16). They may also indirectly lead to monitoring errors when the parameters needed by control room operators are no longer available or perceptible, i.e. data transmission breakdown. This root cause calls into question the organisation assigned to inspect and monitor the automated system's hardware components, in addition to highlighting the vulnerability of the processing function to this type of organisational breakdown. Examples of accidents involving such insufficiencies have been provided on page 31 (see ARIA 22404 and ARIA 40969).

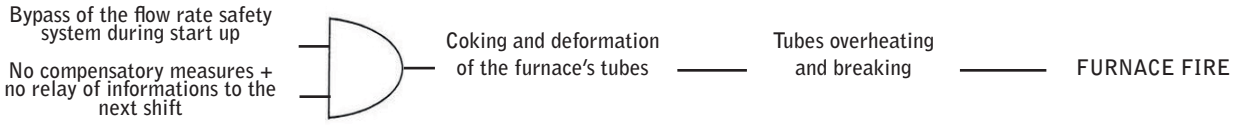
Control and maintenance deficiencies account for 1/4 of all root causes, resulting for the most part in hardware component failure and perception errors.

Figure 16 *Direct causes stemming from control and maintenance problems*



Failure of an automation controller card responsible for an accident

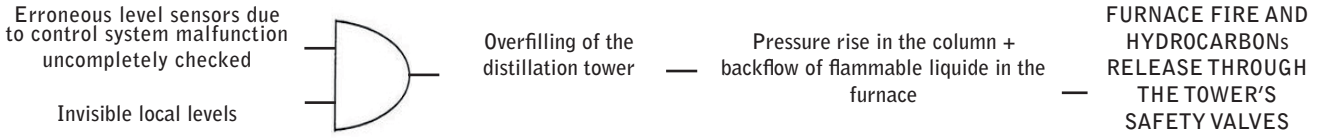
WORKPLACE COMPETENCIES AND ORGANISATION (ARIA 33333)
1st October 2005



Subsequent to a tube break inside a refinery, fire ignited on a furnace. The emergency shutoff system was tripped and the unit became depressurised via the tube that broke inside the furnace. During this incident, the unit was on a return path to its nominal flow rate. Roughly 24 hours prior to the break, following another incident, the reforming unit was operating at an extremely low flow rate over a 3-hour period. The low flow rate safety system had been bypassed without implementing any compensatory measures. The next day, this information was not even relayed to the daytime shift, with the abnormal situation leading to the quick coking of the tubes and accelerating their creep. The fire had originated from overheated tubes tied to an internal coking operation, caused by operating at an insufficient flow rate (in a breach of safety rules). In underestimating the incident occurring the previous day, the subsequent shift had not been properly informed. The environmental agency requested strengthening the refinery's safety management rules and verifying their strict implementation, in addition to installing an alarm management system. The agency also requested: f**ormalising both the resources to be notified in the event of a process-related incident outside of plant operating hours and the rules for overseeing unplanned shutdowns and corresponding start-ups; revising the periodic safety test acceptance protocol; and expanding training and recycling programmes thanks to the Company's new tools, in emphasising furnaces and incident management.**

OTHER RELEVANT REFERENCES Aria 9652, 26880, 30406, 31441, 32109, 32632, 32640, 35432, 38674, 42163, 42920

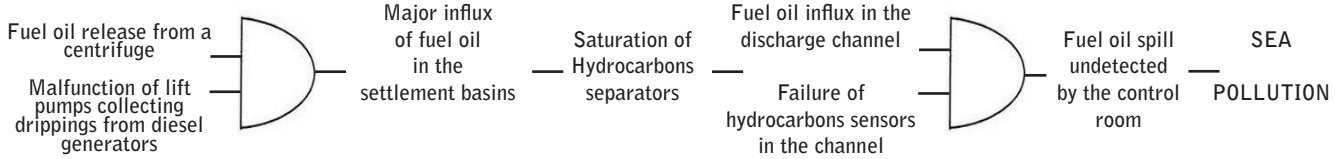
SUBSTANDARD CONTROL (ARIA 22404)
13th August 2009



A fire broke out on the vacuum distillation unit in a refinery during its shutdown. The unit had been restarted the day before following the acceptance of the work, while other job sites were still underway at the site. The reheating operation had begun during the night, and the unit was still in the power build-up phase. At around 9.15 am, thick black smoke was observed coming from the stack (fire in the furnace), with flames shooting from the open explosion vents. This situation was preceded by hammering in the pipes and rising pressure in the tower increase and the opening of valves: hydrocarbons began spilling outside. Following the inquiry, it appears that erroneous level indicators caused the tower to be overfilled then the backflow of liquid into the furnace via the vacuum system (backflow of incondensable materials). A brief summary of the findings: the local levels were not visible, **the chain associated with the control levels in the bottom of the tower had not been completely checked (card),** and the configuration of the system and notably the extraction levels were not correct.

OTHER RELEVANT REFERENCES Aria 7577, 16213, 18051, 29722, 31441, 34923, 36660, 37525, 42557

SUBSTANDARD MAINTENANCE (ARIA 40969)
22nd September 2011



At 6 am, the morning shift inside a conventional power plant detected hydrocarbons in the discharge channel leading to the sea. The supervisor ordered closure of the valves downstream of the channel in order to contain the pollution. The lift pump on the sump collecting drippings from diesel generators did not shut off at its low level but instead continued to operate until its decoupling by field operators on duty. A centrifuge also malfunctioned and released massive amounts of fuel oil. These two anomalies caused a major influx of hydrocarbons into the settlement basins, whose saturated separators allowed pollutants to flow towards the processing basins and into the discharge channel. **None of these anomalies were detected in the control room since both of the monitoring booths continuously measuring hydrocarbon content in the channel had been inoperable since 15th September.** The plant operator repaired all defective component, audited the industrial water treatment installation and ran an awareness building campaign aimed at the entire workforce.

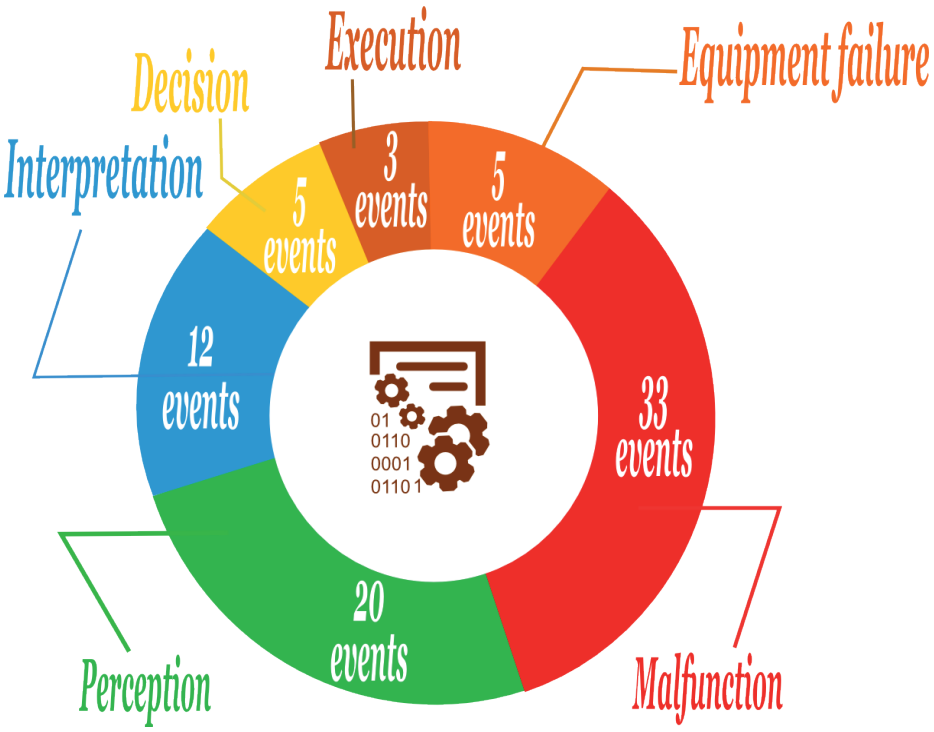
OTHER RELEVANT REFERENCES Aria 6645, 14247, 26895, 34319, 35774, 36193, 41541, 42235, 42931

3.3 Programming

Besides lying at the heart of automated system performance, programming is a field that facilities managers struggle to control internally, with respect to specifications and design (which is not their core technical profession) as well as to maintenance (with code updates and modifications requiring a level of expertise rarely available in-house). Programming flaws equally lead to component falilure and monitoring errors mainly deriving from perception and interpretation problems (fig. 17).

Programming flaws account for 20% of the root causes of processing accidents; they also lead to automated system malfunctions and monitoring errors.

Figure 17 *Direct causes stemming from programming flaws*



Some hardware defects stem from errors ascribable to a single programmer: computer bug, activation sequence on the wrong component, input of erroneous activation thresholds, programmed action opposite what was requested, etc. Nonetheless, hardware defects and the monitoring errors caused by flawed programming can often be traced to a poor understanding of specifications or incomplete knowledge of process components and risks by external suppliers selected to design and programme the automated system.

VOICE OF THE FIELD

« We were asked to make modifications in a moment's notice and we tried to produce too quickly. We were asked to modify the acceptance step by producing when a shutdown was necessary.»

Testimonial of a control room operator at the time of modifying an automated system [6]

This would include: unanticipated situations, processing of contradictory information, oversight of control parameters, breakdown in alarm relay to the processing function, unwanted activation of certain component under special circumstances (incorrect valve position, pumps creating water hammer effects, inappropriate alarm thresholds, see examples on p. 34 and ARIA 42690, p. 38). Moreover, production constraints may warrant shortening the often lengthy and complex validation phases, resulting in neglecting programming errors (seeARIA 36437, p. 34).

During the specification and design phase, it appears to be essential to allocate time for exchanges between management, supervisors, control room operators and the «subcontracted» programmer so that the programmer fully understands the operating principle expected of the automated system as well as process specifics. Given the system's importance in process control and safety, time must also be allocated to test the system following any modification, especially for exceptional operating sequences like shutdowns, start-ups and operating in degraded mode.

During the operations phase, the control room operator is often given the authority to tinker with system programming. It is important to closely evaluate this level of authority since it can also lead to monitoring errors committed by operators:

- Given too much authority, the control room operator may freely modify controller settings and bypass (either out of convenience or faulty manipulation) key thresholds for process safety or quality, e.g. alarms (see ARIA 37139, p. 25).

VOICE OF THE FIELD

« From a supervisory point of view, this system was too open-ended, too dangerous. Control room operators are upset because they adopted bad habits, and I'm not sure they're aware of the potential consequences should they commit an error.»

Testimonial of a supervisor after the automation of his unit's process [6]

- Given too little authority, the control room operator might be unable to correct an incident through utilising his experience and judgment skills since he would need to act in accordance with the operating rules and timelines imposed by the automated system. Such restrictions are not always adapted to the dynamic and specificities of an abnormal situation playing out before him (see ARIA 38617, p. 27).

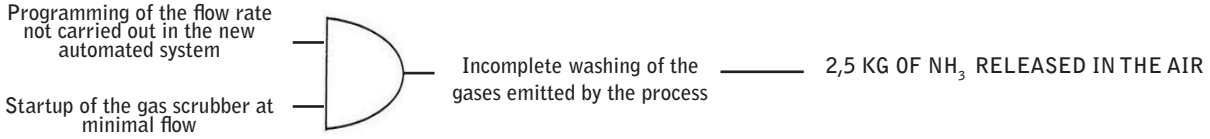
VOICE OF THE FIELD

« It's the system taking over, whereas in the past some of the component would be bypassed as a step to manually controlling the situation.»

Testimonial of a control room operator in a refinery [8]

Programming of an automation controller (Control Engineering Asia, ARR))

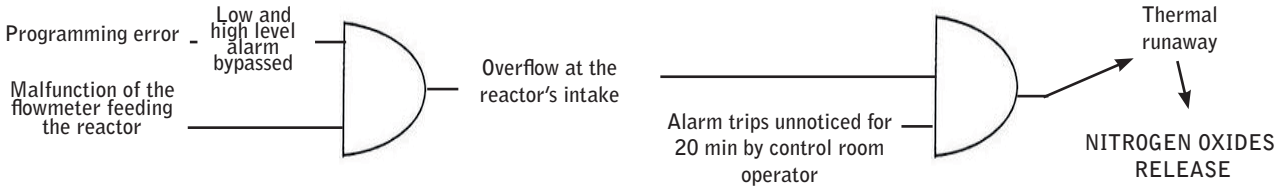
INCOMPLETE PROGRAMMING (ARIA 36437)
3rd July 2009



In a Seveso chemical plant, some 2.5 kg of ammonia were released into the atmosphere around 1:15 pm following malfunction of a gas scrubber and resulting in an odour nuisance. Someone outside the facility sounded the alarm. The component was stopped then turned back on. No staff members reported being inconvenienced and plant production was not interrupted. **The incident arose subsequent to a change in the process control system. In reality, the recommended flow rate of saltwater used in the carbonation tower gas scrubber was not carried over to the new system.** Upon start-up, the saltwater flow rate had remained at a minimum, corresponding to the workshop's nominal operating level. Given ongoing production demands, this flow rate proved to be insufficient for complete gas washing (CO_2 and NH_3), hence the release of NH_3.

OTHER RELEVANT REFERENCES Aria 11181, 16080, 23589, 25057, 25204, 36437, 42921

INAPPROPRIATE PROGRAMMING (ARIA 21994)
19th February 2002

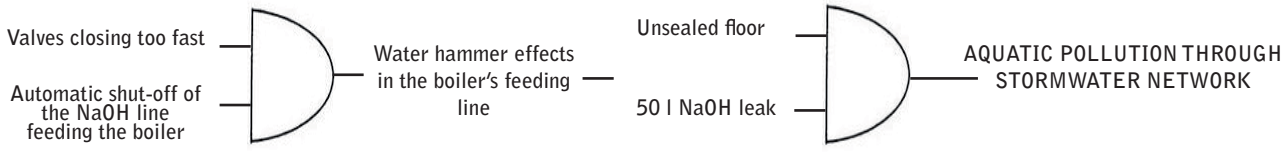


A release of nitrogen oxides (NOx) at a chemical plant resulted in a reddish cloud that hovered over the site before dissipating due to the presence of strong winds. This NOx discharge was caused by an erroneous value indicated by a flow meter placed on the nitric acid inlet line of a reactor at a glyoxylic acid manufacturing unit. Other simultaneous malfunctions were also observed. **Following a programming error, the low-level alarm bypass triggered the high-level alarm bypass as well, with the flow rate exceeding the flow meter measurement range.** Moreover, the control room operator had not noticed 3 or 4 alarms tripped during the 20 min he spent controlling installations. These multiple operating breakdowns caused a valve on the production line to open when it should have remained closed, as the quantity of nitric acid in the reactor at this point of the reaction was sufficient. Given the exothermic nature of this reaction, reactor temperature rose to a level that triggered dilution of the reaction mixture in water and a safety shutdown of the reactor, i.e. its drainage into an empty atmospheric pressure vessel designed for this purpose followed by degassing of the vessel. No injuries were reported. All plant flow meters were subsequently inspected.

OTHER RELEVANT REFERENCES

Missing or inappropriate alarm programming:	Aria 12671, 21994, 28389, 30178, 31376, 32632, 37825, 42628, 42690, 43455
Operating sequence poorly adapted to the ongoing situation:	Aria 13297, 25057, 26199, 31150, 37041, 39384
Incorrect positioning of remote operated component:	Aria 16080, 18563, 31307, 42920, 43271

HAZARDOUS PROGRAMMING (ARIA 28911)
21st September 2004



A 50-l soda (NaOH) leak occurred on the intake line of a boiler's demineralisation unit inside a glue factory. The deteriorated floor under the demineralisation columns facilitated the flow of washing water loaded with soda into a former storm drain system emptying into the nearby river. The pH rise caused calcium carbonate to precipitate, turning the river cloudy whitish over a long stretch. This discolouration disappeared 1 hour later. The factory operator responded by remodelling and sealing the unit floor, repairing pipes, **revising the automated control system to avoid a water hammer effect when closing valves**, and reducing the mismatch delay.

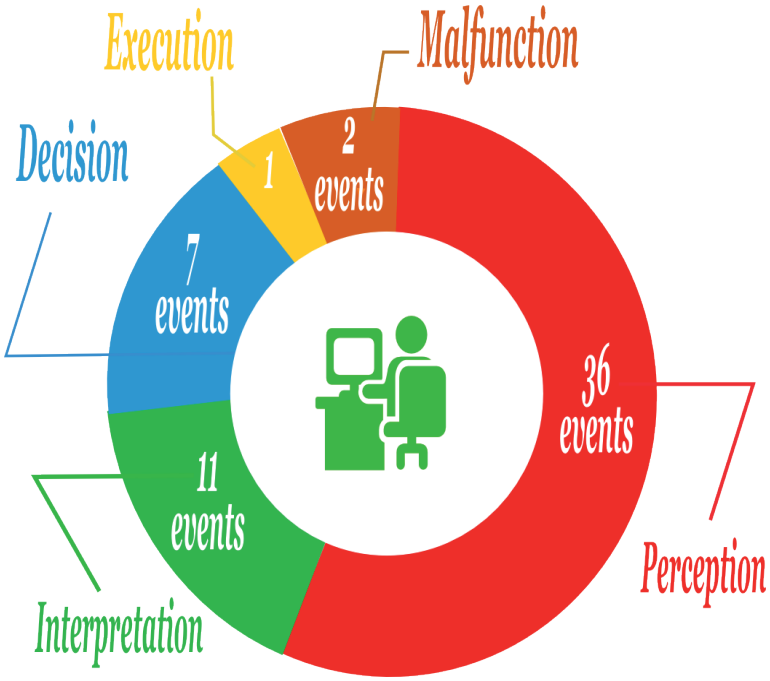
OTHER RELEVANT REFERENCES Aria 5989, 16072, 28911, 30417, 32109, 31691, 40522, 41736, 42038, 42921

3.4 Workplace and interface ergonomics

Given the control room operator's fundamental role in the processing function, ergonomics naturally become a major root cause of accidents, contributing in large part to monitoring errors (Fig. 18). While flawed ergonomics mainly pertain to perception errors due to the prevalence of parameters impossible to perceive, or control / safety alarms either inaudible or embedded in display banners, or alarm overload, etc. (see ARIA 40584, p. 22), they are also the source of interpretation and decision-making errors (see ARIA 23893, p. 38) and sometimes even execution errors (see ARIA 33334, p. 27). Moreover, the root cause of some accidents due to malfunction might be traced to a much less frequent deficiency in workplace ergonomics (see ARIA 27903, p. 38).

Poor ergonomics are manifested by monitoring errors that showcase the fundamental role of human supervision and the benefit of focusing greater attention on man-machine interface ergonomics.

Figure 18 *Direct causes stemming from flawed ergonomics*



All too often, the conception and design of industrial automated systems target the technical or economic performance of the system without paying sufficient attention to the procedures and conditions under which the control room operator will use such system. Control room operators must subsequently cope with a suboptimal situation and compensate throughout their shift for the ergonomic inadequacies in the interfaces and command functions, necessitating extra concentration and running the risk of accident occurrence should this concentration wane.

VOICE OF THE FIELD

« Since human intervention in the control process has been widely underestimated, so has the role of displays.»

« This model has been roundly criticised by control room operators: their point of view had not been taken into account in the initial version of this man-machine interface.»

Testimonials of specialists in the field of industrial ergonomics [16, 17]

A study conducted in 1991 on the ergonomics of 5 control rooms at French industrial sites covering 3 sectors of activity (food processing, paper production, mining extraction) revealed the recurrence of several deficiencies [16]:

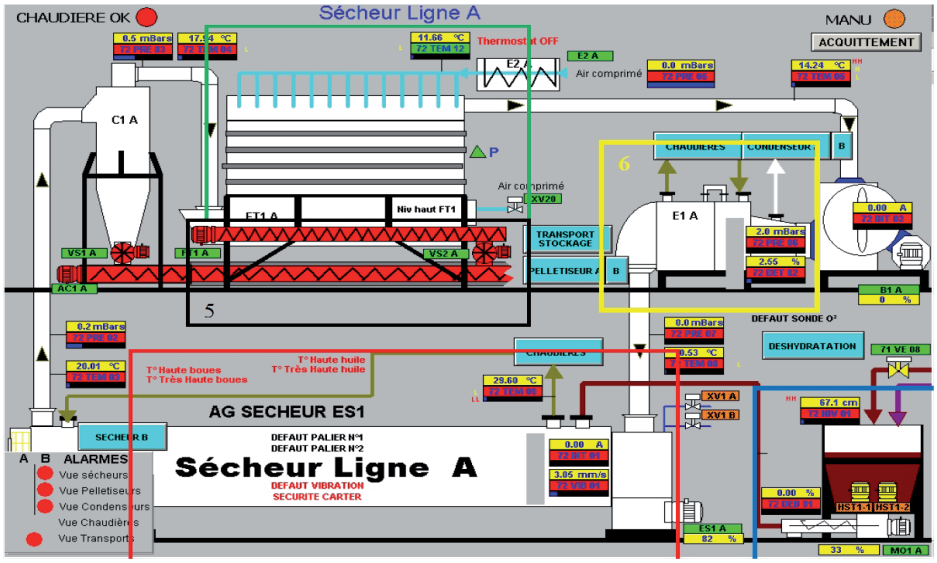
- interfaces designed for normal operations, yet ineffective under abnormal conditions (e.g. no basic view of component malfunctions, delayed access to critical information);
- screens saturated by block diagrams, overload of information displayed, including some images that are obsolete or useless for the ongoing phase;
- little or no block diagram animation on displays (e.g. tank filling, valve opening);
- limited feedback informing control room operators about the result of their actions;
- no display of the status of component controlled manually despite its importance in the process;
- a graphic representation of component inconsistent with its relative size or location inside the unit, an illogical use of colours compared to process and component states.

VOICE OF THE FIELD

«Overlooked during the procurement process and acknowledged late in the distributed control system (DCS) installation, the design of imaging displays is often mishandled by suppliers, who are solely driven by the start-up deadline in order to avoid late penalties.»

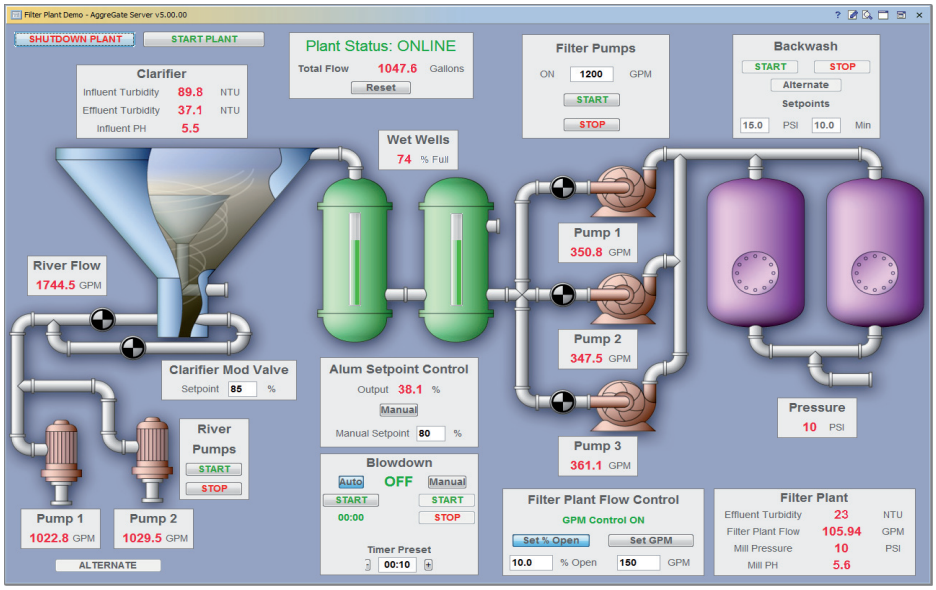
Testimonial of an industrial ergonomics specialist [16]

Control rooms evolution between 1970 and 2010

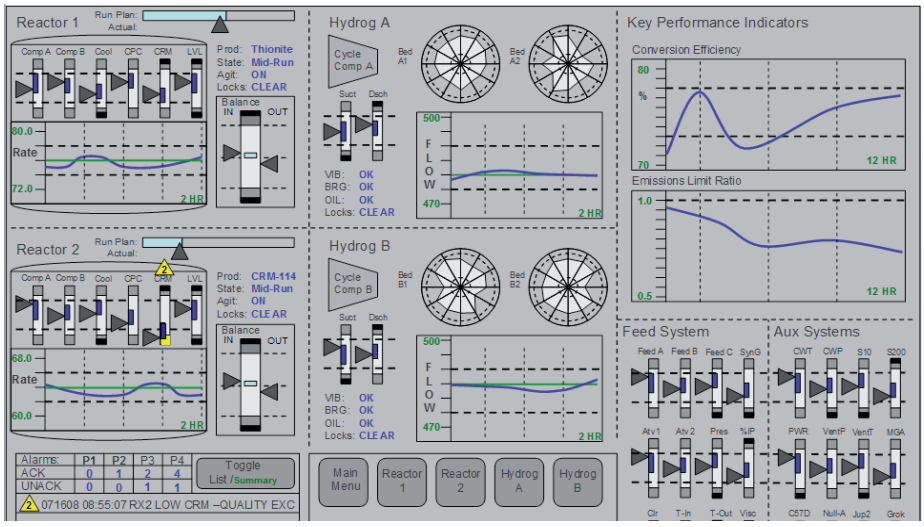


Examples illustrating the importance of control interface ergonomics

An overloaded interface, illegible state data, unit operations are difficult to understand and bright colours cause eye strain for control room operators. This harsh interface results in an operator's failure to detect an accidental situation (see ARIA 42156).

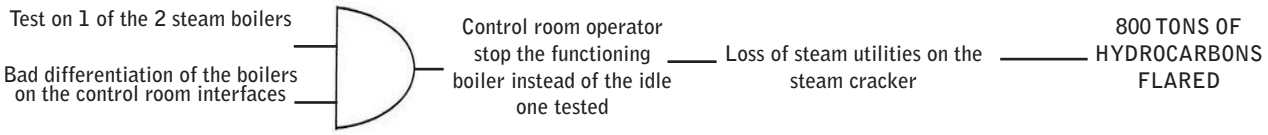


A more streamlined interface, unit operations are easier to understand and state changes are clearly indicated (colour and On/Off), yet recognition of display values can still be improved (detection of operational drift).



Good interface ergonomics: values are shown in their normal operating range along with a time history, which facilitates the detection of abnormal situations; bright colours are reserved for graphic alarms, which are assigned priority, and only data relative to the most important equipments and ongoing phases are permanently displayed (extracted from « *The high performance HMI handbook* »).

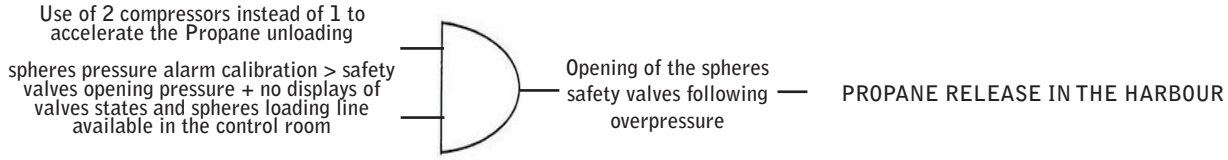
CONFUSING INTERFACES (ARIA 23893)
9th November 2002



Inside a petrochemical unit, a steam supply problem encountered at the site's steam production plant caused activation of the cracked gas compressor. The steam cracker was immediately shut down and the gases routed to the flare, resulting in the flaring of 800 tonnes of a hydrocarbon mix between Saturday evening and Sunday end of the afternoon. The unit's supply was being provided by 2 boilers, one serving as a backup to the other. During the incident, one of the boilers was taken off-line for maintenance, leaving just a single boiler running. The idle boiler had undergone numerous safety tests, one of which called for closing the intake valve. **The test operator mistakenly closed the fuel intake valve on the operating boiler from the control panel, causing a significant and sudden drop in steam supply to the units.** With the steam cracker shutting down immediately, the installations were degassed and the flare network used as a backup for hydrocarbon ignition. T**o mitigate this type of error, the site operator improved boiler differentiation appearing on the control room's graphic interface**s.

OTHER RELEVANT REFERENCES Aria 10131, 25216, 35432, 33516, 36722, 41207, 42156

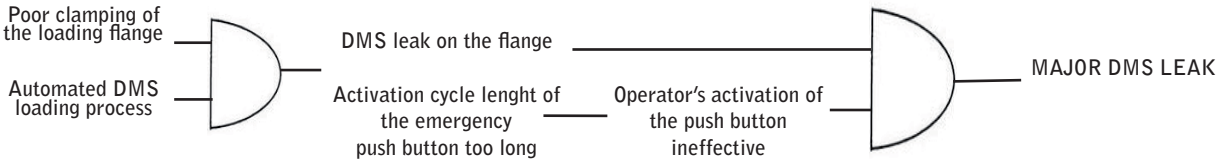
MISSING CONTROL PARAMETER (ARIA 42690)
11th August 2012



At 6:55 am, a propane ship unloaded its cargo into 2 mounded spherical storage tanks at a Seveso plant. At 8:50 that evening, the liquid phase had been completely unloaded and the vessel's pumps were turned off. Unloading of the gaseous phase via the ship's compressors began a few minutes later. At 9:35 pm, the 2 relief valves on one of the tanks opened at their calibration level (10.9 bar) for 30 seconds. The on-duty pump operator stopped the transfer and connected the 2 spheres in order to lower the pressure, steadying it at 9.8 bar. The plant manager and ship captain jointly decided to halt the unloading operation and monitor pressure of both tanks every 30 minutes. According to the site operator, the sphere's pressure rise from 9.2 to 10.9 bar in 35 min was due to the simultaneous use of both propane ship compressors to accelerate unloading. The installation inspection revealed that pressure alarm thresholds on the sphere had been set at a higher value than the valve calibration pressure. **Subsequent to the incident, the pre-alarm levels (visual and sound) and sphere alarm were calibrated at 10.4 and 10.7 bar, respectively, i.e. below the valve tripping values. The effective closure of the sphere filling valve and opening of the spraying valve were both prominently displayed on the control room displays.**

OTHER RELEVANT REFERENCES Aria 2900, 13850, 14619, 19533, 23231, 33333, 37139, 34597, 40993, 42746

WORKPLACE ERGONOMICS (ARIA 39900)
28th January 2009



Dimethyl sulphate (DMS) began leaking around 11 am at a chemical plant as the product was being loaded. The connection between the DMS container and the loading station consisted of disassembling the solid flanges, replacing the joint by a new part and reconnecting the container flanges to the unit's pipe flanges. After initiating DMS loading in the control room, the field operator climbed down to inspect the container and, at that point, identified a leak on the flange connecting the container to the loading pipeline. He sounded the siren and the emergency light before pressing the emergency stop button. The next day, the plant operator concluded that the leak had been caused by poor clamping of the loading flange while the container was connected to the loading station. Moreover, **the safety automated system was not activated because the pushbutton had not been held down long enough for its cycle length (1/10th of a second). All emergency stop pushbuttons were replaced by locking buttons throughout the site.**

OTHER RELEVANT REFERENCES Aria 3536, 27903, 33334, 42077

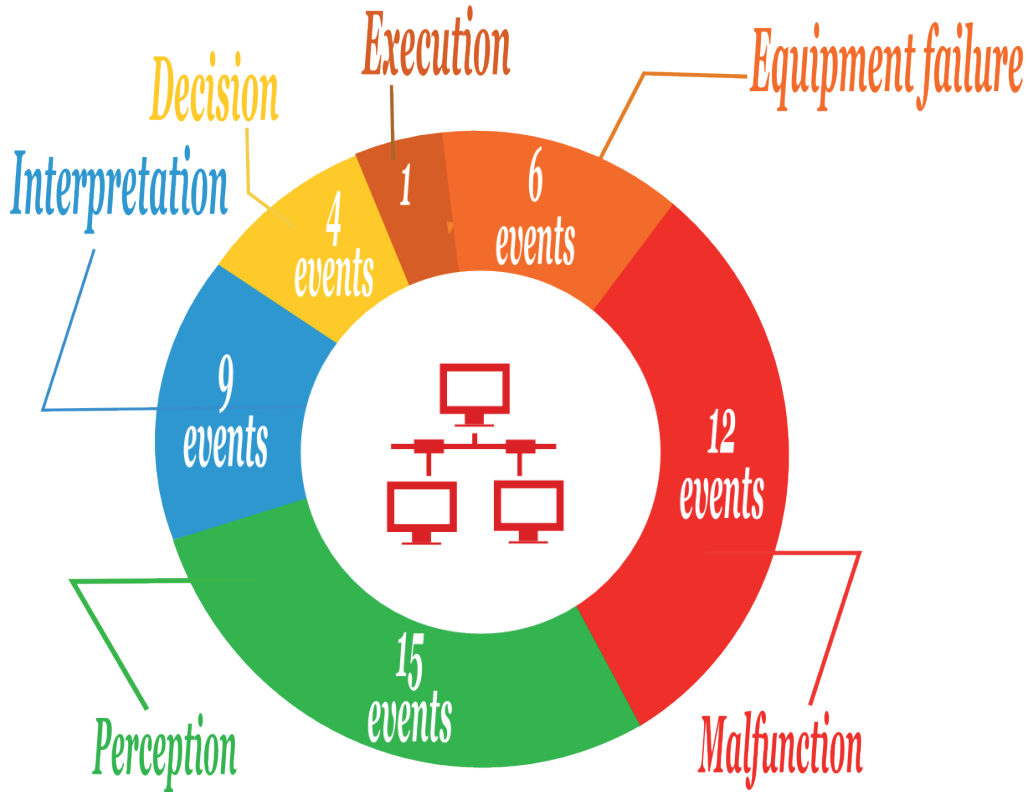
3.5 System design

System design flaws remain one of the main root causes associated with processing accidents (Fig. 14, p. 28); such flaws pertain equally to the installation of new automated systems as to the modification of existing ones (see ARIA 38676, p. 41). Automating a process, especially when it is complex or versatile (as is the case in the fine chemistry and pharmacy sectors), presumes a detailed study has been conducted of the various operating scenarios, in encompassing the most likely and most serious failures or malfunctions. Even though the methodologies applicable to these kinds of studies have been available for a long time (e.g. AMDEC, HAZOP, LOPA), the processing-related accidents under study herein all too often point to atypical situations, such as transient phases, successive restarts or emergency shutdowns, tending to be ignored during the design phase. More specifically, it is quite commonplace for the safety shutdown sequences of an automated process to transform a minor technical incident into a serious accident (see ARIA 32109, p. 22).

System design flaws remain a significant root cause of processing accidents, as regards both component failures and monitoring errors. On the other hand, these flaws are more difficult to detect and prevent once the automated system has become operational.

As opposed to design problems found in accidents involving sensors [1], system design flaws are reflected, first and foremost, by malfunctions and monitoring errors but only rarely by component failure (see Fig. 19 and ARIA 31691, p. 41). This observation indicates that design flaws are root causes that remain difficult to detect once the system is running; moreover, such flaws often only appear once the abnormal situation has been initiated. It is thus critical to perform early prevention via a strict specification and design process.

Figure 19 *Direct causes stemming from system design flaws*



Accidents also arise after modifications, especially when an automated system replaces a manual one or coexists alongside with it, even when interactions between the two systems «outside of normal operations» have not been well identified (ARIA 21466, p. 41). A poor design also creates common mode failures in the event of malfunction: when automation is responsible for supervising both the process and safety systems, when malfunction of the redundant system spreads to the main system, or when an electricity outage neutralises the backup system by preventing it from placing the process in safe operating mode or from stopping/detecting accident occurrence (see ARIA 38676, p. 41). System failure becomes even more serious if control room operators lose the capacity to accurately appraise the actual state of the process or implement the site's safety systems (see ARIA 38485, p. 14), forcing them to act «in the dark» (see ARIA 12671, p. 43).

« Computers are not responsible for introducing new types of errors. They simply introduce more and easier opportunities to repeat the old ones.»

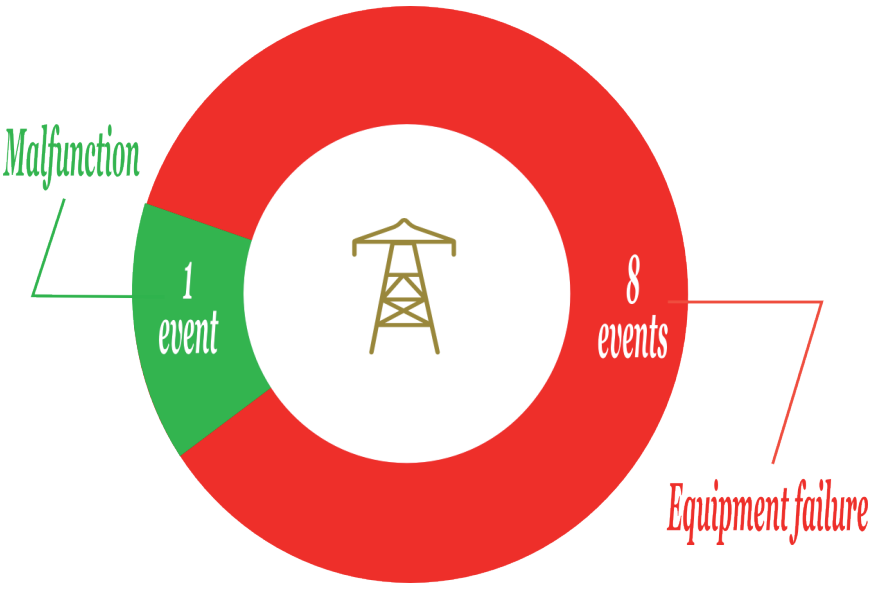
Trevor KLETZ - English chemical engineer and expert in industrial safety - «Wise after the event»

3.6 Loss of external utility

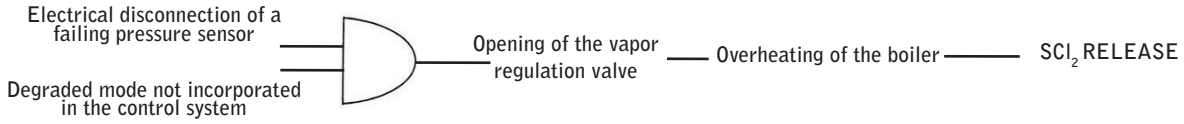
The loss of utility supplied by the electrical network appears to be a rather marginal root cause with respect to the processing function, more likely to cause outright system failure than malfunctions (Fig. 14, p. 28, and Fig. 20). Since automated system have often been identified as strategic component for the purposes of production and safety, backup or redundant power supply is typically planned in order to maintain functional control for the time it takes to place process equipment in safe operating mode. The few catalogued accidents for purposes of this study pertain to rarer phenomena, e.g. domino effects following the failure of other component (see ARIA 28416, p. 43).

The loss of utility is a rather rare root cause, which no doubt indicates the high level of protection offered to automated systems.

Figure 20 *Direct causes stemming from a loss of electrical utility*



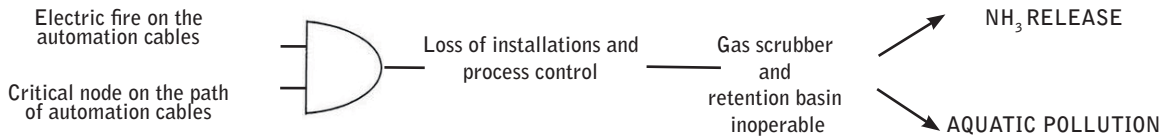
DESIGN FLAW (ARIA 31691)
26th April 2006



Inside a chemical plant, a sulphur dichloride (SCl_2) leak on a pipeline supplying the boiler tube of a distillation column hydrolysed, thereby generating a strong emission of hydrogen chloride (HCl). 50 ppm of HCl were recorded inside the building. Operating losses were valued at Euros 270,000 (the downstream unit stayed idle for 18 days). A pressure sensor was undergoing maintenance; it had been diagnosed as defective after indicating a reading of 108 mbar of pressure at the boiler tube output, thus triggering closure of the valves controlling SCl_2 supply and regulating the vapour heating the boiler tube. **Since the sensor was not «fail safe», its electrical disconnection caused the vapour regulation valve to open, thus heating the boiler tube, whose temperature rose from 24° to 120°C in 30 min, and causing the emission of SCl_2.**
Several measures were adopted as part of the feedback provided: monitoring and intervention procedures in a degraded operating mode, modification of the sectional valve / pressure sensor assembly, introduction of a positive safety loop independent of the regulation, thereby prohibiting any automatic restart once the high pressure threshold had been reached. **This accident demonstrates that a process control system can in no way be equated with a safety system. More specifically, industrial automation satisfy a rationale and criteria that are not all known by response teams and that do not necessarily incorporate degraded modes and lockouts situations.**

OTHER RELEVANT REFERENCES Aria 18563, 27060, 28389, 32640, 40986

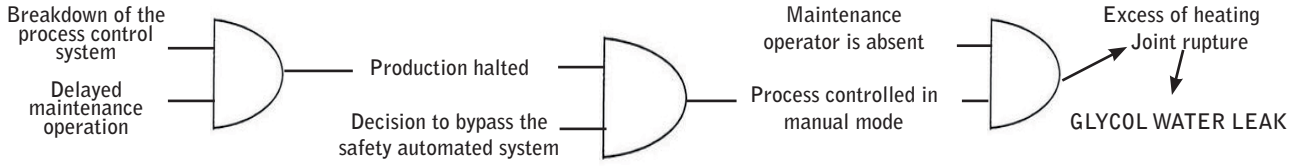
COMMON MODE FAILURE (ARIA 38676)
24th July 2010



At a facility producing carbonate and sodium bicarbonate, fire broke out at 7 am in an electrical cabinet containing transmission cables for the liquid part of the process. The blaze caused a complete loss of control for 2 hours and a shutdown of the process responsible for releasing 2 to 8 kg of gaseous ammonia (NH_3) into the atmosphere, subsequent to the sudden stoppage of the gas scrubber. In addition, ammonium hydroxide was released into the plant's accidental pollution retention basin following discharge of a brine tank; this water made its way into the nearby river given that retention basin controls and monitoring installations had become unresponsive. This discharge wound up causing the death of some 400 kg of fish. According to the facility operator, the heating of electrical cables, traced to worn insulation, had triggered the incident. **The control system, composed of control stations, a connecting bus and an automated system programmed to monitor the process, had been designed with a critical point in the form of a «node» at the time of creating the site's 1st control system (26 years prior), through which all automated system cables were routed. Whereas all electrical component supply lines had been backed up, the automated system cables ran through a single cable tray in the electrical cabinet.**

OTHER RELEVANT REFERENCES Aria 3536, 11665, 36660, 36767, 41305, 42557

COEXISTENCE OF MANUAL AND AUTOMATED SYSTEM (ARIA 21466)
12th September 2000



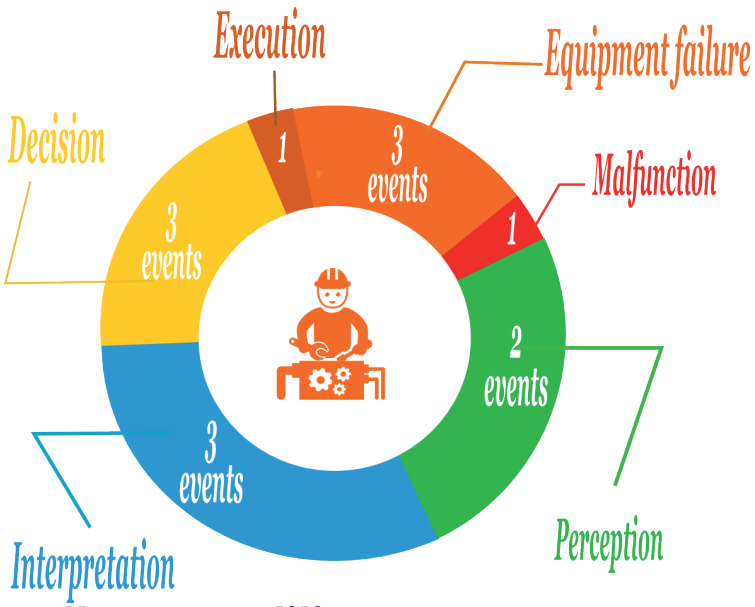
A leak of over-pressurised and overheated glycol water occurred at a chemical plant after the rupture of a pipe joint. At 2 am, a control room operator recorded a drop in coolant temperature (150°C), preventing vacuum drying operations from continuing. On-call staff diagnosed a loss of communication link between the plant's utilities automated system and the plant's process automated system. A specialist in such systems confirmed the defect of a card on the utilities automated system, whose replacement had been postponed until the next morning. **Once the specialist left the premises and confident of his diagnosis, the on-call maintenance operator decided to restart the unit. He short-circuited all of the safety mechanisms for hot fluid monitored by the process system, and replicated the corresponding settings in manual mode.** Called by another workshop an hour later, the operator abandoned the post for 30 min. Upon his return, the hot fluid had exceeded 180°C, and a noise resembling a detonation shook the plant. After joint rupture, the glycol water vaporised on the premises, which were closed immediately thereafter.

OTHER RELEVANT REFERENCES Aria 21316, 25156, 40522

3.7 Working conditions

Unsuitable working conditions are most readily observed by monitoring errors (Fig. 21), arising from situations in which a control room operator is faced with a complex event to manage within an environment that alters the capacities of perception, interpretation and decision-making, e.g. during a start-up phase or when an abnormal situation causes a series of process-related anomalies (see ARIA 12671, p. 43).

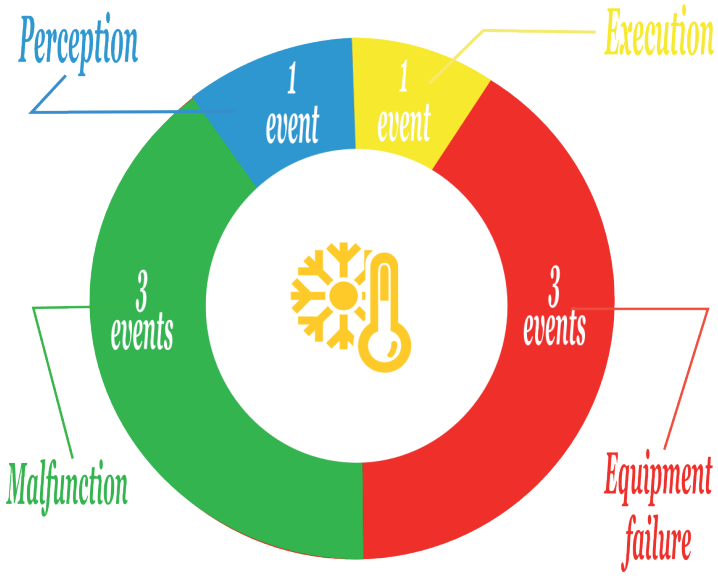
Figure 21 *Direct causes stemming from poor working conditions*



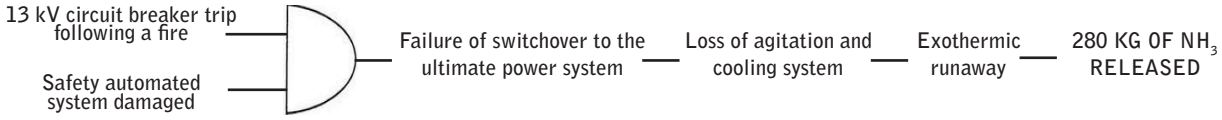
3.8 Hostile weather conditions

Hostile weather has been the source of a few accidents, mainly by causing the processing function to fail or malfunction (Fig. 22). In most cases, thundershower phenomena have triggered electrical or electromagnetic disturbances affecting the automated system hardware components (see ARIA 32624, p. 43).

Figure 22 *Direct causes stemming from hostile weather conditions*



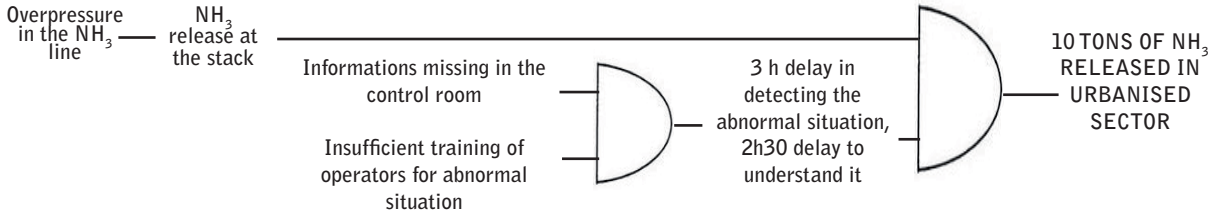
LOSS OF EXTERNAL UTILITY (ARIA 28416)
25th October 2004



In a Seveso chemical plant, a fire broke out at 12:59 pm in a substation supplying a hydrazine hydrate unit. An electrical fault on a cooling water pump caused a generalised short circuit on an electrical tower. The fire alarm was triggered at 1.00 pm. The fire spread to the other towers of the panel through the subfloor. The 400 V circuit breaker located upstream was blocked and did not function. The fault current passed through the 13,000 / 400 V transformer, there was overpressure and an oil leak followed by a primary side homopolar fault causing **the 13 kV circuit breaker to trip. The absence of voltage caused the diesel generator set to stop but the switchover to the emergency system failed as the automatism was damaged by the fire.** The smoke spread to the UPS room whose door remained opened. The UPS stopped when a high temperature (> 40 °C) was reached causing the loss of control and command on the process. The component switched over to safety mode. **Due to the lack of power supply, the cooling system, agitation and the internal and external emergency plan siren were no longer functional**. Since the ongoing reaction was exothermic, the reactor temperature and pressure increased. Several measures are taken such as designing an emergency cooling circuit, improving circuit breaker maintenance, sectoring UPS system, electric boards, generator sets, etc.

OTHER RELEVANT REFERENCES Aria 8885, 26199, 38676, 41460, 42235

WORKING CONDITIONS (ARIA 12671)
27th March 1998

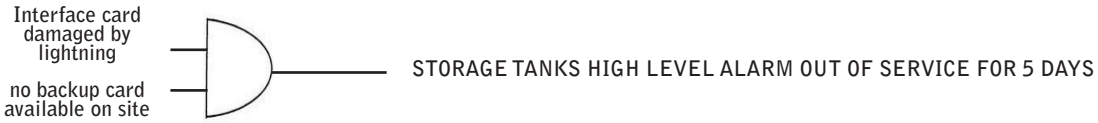


On a tubular exchanger, a disc broke over ¼ of its cross-section at 4:50 am during a pressure surge in the liquid ammonia (NH_3) circuit connecting NH_3 storage cells to a urea workshop operating under stable conditions. NH_3 was partially led to a 100-m high degassing stack. Given stable weather conditions, a foul-smelling cloud drifted towards the city. **The release occurred unbeknownst to control room operators, who had incorrectly interpreted several alarms that had tripped**. Once the diagnosis rendered, the device was isolated at 6:25 am. **The plant operator only became aware of the severity of the event at 8 am; two and a half hours were then needed to fully determine the origin and likely causes**. The 10 tonnes of NH_3 release was due to a succession of physical, organisational and human malfunctions:
- Lack of anomaly detection and automatic safety systems: **information made available to control room operators was inadequate;**
- **Poor diagnosis / decision-making process** lacking adequate verifications despite several precursors;
- Incomplete safety recommendations, insufficient monitoring procedures and inspection plans.

This poor diagnosis would explain the delay required to isolate the deficient circuit and the potential impact of this release. Long periods elapsed between the onset of the accident, the alarm and activation of the internal emergency plan, source identification, causes and circumstances of the discharge, and then a definitive quantification.

OTHER RELEVANT REFERENCES Aria 8885, 26199, 38676, 41460, 42235

HOSTILE WEATHER (ARIA 32624)
26th July 2006



A thunderstorm struck in the vicinity of a flammable liquid storage facility protected by an early streamer emission lightning rod. The indirect effects of the lightning damaged one of the 4 computer interface cards. This particular card had interfaced with the bus network responsible for relaying high-level safety alarms from the storage tanks. The facility operator detected the malfunction via the depot supervisor, who had indicated the communication breakdown. **The operator did not possess a backup card and was unable to perform a quick replacement.** He decided to inform the entire operating staff and requested extra vigilance when monitoring the performance sheets. Operations continued in this manner for 5 days before the interface card could actually be replaced. The damaged card had not been protected against indirect lightning effects. Following this accident, the operator kept on hand an additional card as a backup and implemented the recommendations issued in the study on indirect lightning effects conducted in April 2006. These recommendations focused on the protection, mainly by lightning rod, of the supervisor's computer, alarm relay units, sensors, utility rooms, fire pumps serving 3 depots, and the electric generating sets for 2 sites.

OTHER RELEVANT REFERENCES Storm: Aria 8885, 20835, 32016, 38617 / Heavy rain : 32579, 36496, 35167

1

This synthesis has confirmed the positive role of industrial automation in ensuring installation safety and accident prevention. While the processing function of an automated system is involved in fewer accidents than the sensor function, its performance flaws remain a key accident factor in highly automated sectors of activity that make use of hazardous materials and component.

2

Organisational and human factors are fundamental to assessing accident risks associated with the processing function, in noting better hardware reliability and less exposure to hostile process environments than for sensors and actuators, plus the key role played by control room operators.

3

The predominance of monitoring errors compared to component failures among the direct causes identified underscores the importance of placing the control room operator, and not the machine, at the centre of automated system specification and the associated risk analysis. More specifically, interfaces ergonomics must allow the operators to easily grasp the process state, access feedback on the impacts of his actions and quickly perceive the truly critical alarms, so as to guarantee his effectiveness in abnormal or degraded situations when his input becomes essential and determinant.

4

Moreover, the training and certification of control room operators must be regularly monitored and kept up-to-date, at the risk of losing familiarity with a process that may gradually transform into an «invisible black box».

The following pages tie the 5 primary root causes of processing function-related accidents, as identified in this summary (see Chapter 3), to a series of prevention-oriented recommendations.

- **For each origin of these root causes, the relative importance of the two major categories of direct causes, namely component failures ( ) and monitoring errors (, Chapter 2), has been scored on a scale from 0 to 5:**

  direct cause never or only rarely encountered (0)

  direct cause systematically encountered (5)

- **Each recommendation has been rated on the basis of its implementation complexity, extent of likely internal resource allocation and estimated cost should a subcontractor be required. This classification was established according to the following scale:**

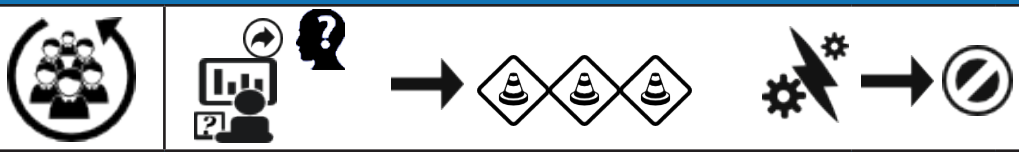
  : *negligible to low*

  : *low to moderate*

  : *moderate to high*

  : *high to very high*

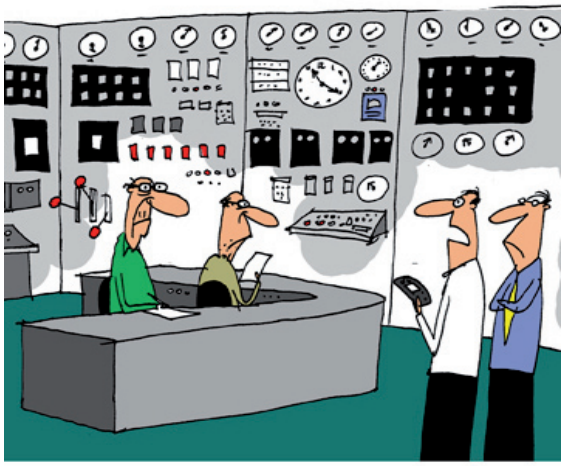
WORKPLACE COMPETENCIES AND ORGANISATION



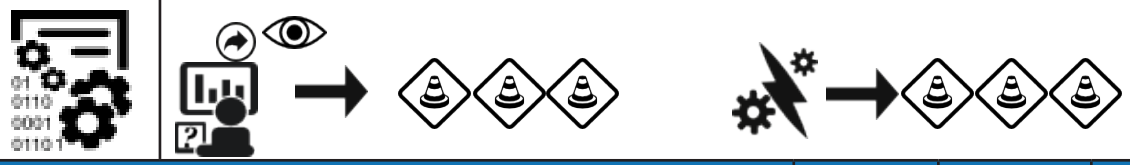
Recommendations	Complexity	Internal ressources	Cost
Define the skill and knowledge prerequisites for each control room operator position (basic instruction, professional experience, familiarity with processes and risks related to the activity, analytical capabilities).			
Establish and implement a control room training curriculum, leading to certification, with regular refresher courses and periodic verifications of experience and process control mastery.			to
Balance workloads among control room operators. Encourage shift rotation and multi-skilling on the part of operators in order to stimulate their vigilance and overall understanding of the process being monitored.			
Clearly stipulate authorised or prohibited actions based on the level of qualification attained by the control room operator: bypassing of safety component or system, acknowledgment of priority alarms, situations in which management must be consulted before making a decision			
Insist on the fact that a decision intended to improve safety will never be penalised, even if it turns out after the fact to have been useless and the cause of production losses or extra workload for the team.			
Schedule regular training practices for control room operators involving degraded and atypical situations, if possible on a dedicated simulator faithfully reproducing the automated system operations (e.g. time lags) and interfaces.			to
During initial or refresher training, enhance operators' understanding of the process state: key parameters, normal and abnormal operating ranges, parameters adjustment to return the process to its control zone.			
During initial or refresher training, enhance understanding of the effect of automated safety systems: activation conditions, effects on the process, timelines and situations in which their efficiency will be improved or downgraded...			
Encourage control room operators to adopt an inquisitive attitude and converse among one another on abnormal situations to compare opinions.			
Verify that any internal human resource issue (e.g. time off, sick leave, on-the-job training) does not require the control room operator to perform unfamiliar tasks with the potential to distract, even momentarily, from his supervisory activities; moreover, verify that the control room is always sufficiently staffed to handle abnormal or degraded situation.			
Verify that the control and safety procedures implemented: • encompass all of the unit's various operating modes (including degraded modes, emergency/shutdown situations), the set of risks identified and the various possible control room working configurations (reduced staff, temp workers, personnel-in-training, etc.); • clearly define the roles of responsibilities of all personnel; • lay out the «contours» for guiding the control room operator to the right decision, without being excessively authoritarian yet maintaining mandatory «milestones» (see [20]); • correspond to control room operators' working practices in having staff contribute to writing the procedures; • were adequately tested and are understandable by control staff (appropriate vocabulary, effective illustrations, no ambiguity, etc.); • are regularly updated in the event of: 1) request for relevant modification submitted by a control room operator or group of operators; 2) technical or organisational unit change, even a minor one, like adding a parameter or an alarm (management of change process); and 3) use of internal or external feedback from incident or accident; • are easily and quickly accessible from any work areas in the control room; • undergo testing to ensure familiarity and good understanding among control room operators within the scope of their initial / refresher training.			

CONTROL AND MAINTENANCE

Recommendations	Complexity	Internal ressources	Cost
Adopt a preventive maintenance policy (contents and frequency) for each critical system component based on experience, manufacturer recommendations and the available reliability-driven databases (e.g. *Oreda, Eireda, PDS*).			
Specify the type and periodicity of tests to be conducted on the various automated system components: functional and visual verification, verification of environmental conditions, etc.			
Display in the control room (either manually or automatically) an updated operating status of the main automated system components, to ensure control room operators are informed: active, unavailable, out of order, bypassed, etc.			to
Establish the set of automated system maintenance procedures by identifying critical components, maximum repair times to be imposed (applying the notion of *Mean Time To Repair*) and compensatory measures to implement during downtime. Ensure traceability of these procedures and on-site accessibility to both control and maintenance teams.			
Develop indicators to detect possible maintenance discrepancies: average repair time, supply schedules, availability of inventory and tools, component failure rate, etc.			
Verify that the lines of communication between control and maintenance teams are open and regularly used (monitoring log, meetings, etc.).			
Ensure the quick availability of spare automated system components, in particular those that often require replacement (e.g. input/output cards, relays). Update documentation on a regular basis.			to
If the risk of obsolescence is a possibility (e.g. discontinuation of parts by the manufacturer), assess the benefit of changing to a more recent generation of automated system or, as an alternative, ensure the capacity to quickly procure spare components no longer distributed by the manufacturer (1st and 2nd emergency inventories either on-site or off-site, cannibalisation techniques, rebuilding of parts upon request, etc.).			to
Be sure to always have on call (in the vicinity), whether internally or externally, a competent and quickly mobilised workforce in order to handle on-site maintenance of the various automated system components and engage in regular exchanges with control room operators.			



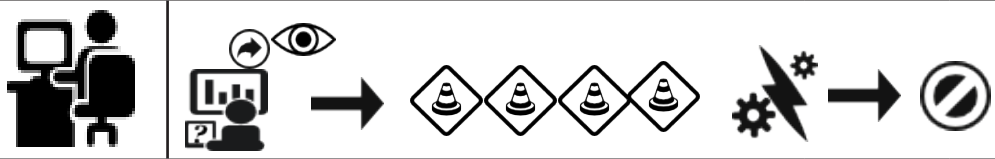
"We put all this high-tech control equipment in 30 years ago. I still don't understand why we can't get the information we need out of the system."
(Automation.com, ARR)

PROGRAMMING			
			
Recommendations	**Complexity**	**Internal ressources**	**Cost**
During the automated system specification process, involve supervisors and control room operators so as to verify that all expected functions and operating modes used in the unit have been included in the specification documents.			
Verify that the subcontractor assigned to program the system has effectively understood the unit's operating principles and instrumented safety chains; conduct regular assessments during each step and testing with the subcontractor before placing the automated system into service.			
In the new automated system installation schedule, allow time for testing and trial phases, avoid premature service start-up should it be felt that the system is not quite ready.			
During testing scheduled prior to service start-up, include the atypical process operating phases (start up, extended downtime, emergency shutdown) as well as the main anticipated degraded modes (breakdown or lockout of some components, loss of utility, etc.).			
If the unit can be controlled both manually and automatically (e.g. the case of retrofits), evaluate «possible edge effects» between these two control modes and programme the automated system to prevent or mitigate such effects.			to
Verify that the site's management of change procedures also account for the adjustments required in automated system programming (hardware modifications made to the process, e.g. equipment change, addition of new functionalities or monitoring parameters).			
Ensure that a computerised support always remains on hand to adjust the programming, in order to overcome difficulties encountered by the control room team and incorporate the necessary upgrades identified over time.			

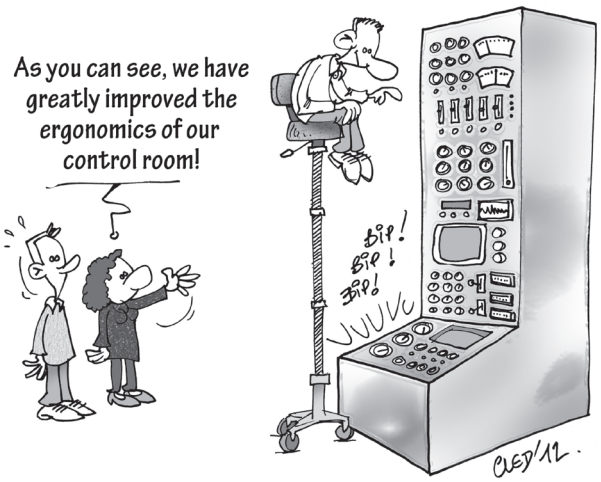
"OK... let's get the programmer back in here and de-hum-bug the process."

(Automation.com, ARR)

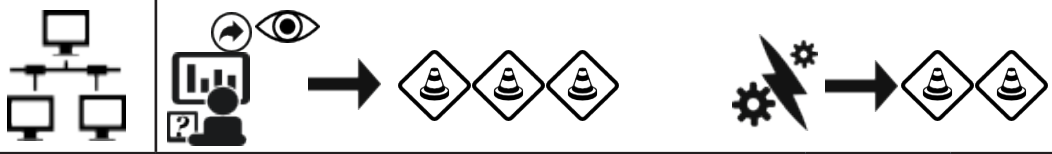
ERGONOMICS



Recommendations	Complexity	Internal ressources	Cost
Control interfaces must be designed to streamline the control room operator's perception, understanding and vigilance. For this purpose, it is advised to pay close attention (see EEMUA Standard 201, [16, 20]) to: • animation of control displays (filling, opening, etc.); • consistency of graphical component depictions with their actual size or location within the unit; • use of colours to reduce eye strain and provide a good level of contrast, and matching of colours with their standards or stereotypes (e.g. red for high priority, yellow for medium priority, etc.); • availability of feedback given to control room operators regarding the results of their actions; • priority display of critical parameters along with their normal operating range and a timeline; • display of priority alarms: easy and quick perception, without interference from other displays etc. • display of a common block diagram to simplify overall perception of the unit status, plus a series of more specific diagrams to visualise the status of certain process parts or component in detail; • user-friendly manipulation of alarm banners (no complex navigation between several screens); • terms and symbols on display, as these must be intuitive, standard and homogeneous with those used by control room operators and in current procedures; • the size of characters and symbols displayed, which must be easily read from the control room operators' workstations.			 to 
Practice prototyping the control interfaces and collect the opinions of control room operators to provide an interface best suited to their «field» practices.			
Incorporate workplace and software ergonomic features from the control room into current management of change procedures.			
Account for control room workplace ergonomics in ensuring that operators' working conditions are as well adapted as possible: keyboards and screens, furnishings, work postures, environmental factors and their variability over time (light, noise, etc.), moving around inside the control room, verbal and visual exchanges between operators on duty, lines of communication with operations staff (see ISO 11064 Standard and [20]).			 to 



SYSTEM DESIGN



Recommendations	Complexity	Internal ressources	Cost
Analyse and sort the various components of the automated control chain by their criticality relative to safety: sensors, actuators, calculators, cards and communication networks, control interfaces, software applications, etc.			
For those components classified as critical: • define the behaviour required in the event of hardware failure, loss of utility or automated system malfunction (e.g. fail safe, backup power supply); • favour standard and long-life cycle component in order to minimise the risk of failure and facilitate maintenance; • select components that are easily testable and, if possible, designed with the capacity for self-diagnosis (sensors, calculators, etc.); • emphasise a choice of components that can be maintained without (completely) stopping the unit and compromising safety.			
Analyse both the service and environmental conditions applicable to these components in order to define constraints imposed without functional failure: temperature, humidity, dust, corrosive atmosphere, vibrations, mechanical shocks, electrostatic discharges, etc.			to
During the choice of automated system components and architecture, base the selection strategy on a reputed risk analysis methodology, in minimising the risks of common mode failures and promoting the identification of redundancies deemed necessary for critical components (Hazop, concept of intrinsic safety, etc.).			
For the design of an automated safety chain, reconcile the accounting of selected components with expectations in terms of autonomy, reliability and response time (overall «SIL» level reached by the complete chain).			to
If the unit can be controlled both manually and automatically, identify «possible edge effects» between these 2 control modes and incorporate them into the choice of operating configuration.			to
Implement an alarm management methodology that entails: • identifying existing alarms in both normal and degraded situations, measuring alarm flows; • interviewing control room operators on existing alarms: relevance, flow volumes, priority in the display, alarm processing practices in both normal and degraded situations, bypass protocol on alarms considered to be «nuisances», processing times deemed sufficient?; • assessing the actual utility and priority of each alarm with respect to the ongoing situation; • evaluating the relevance of alarm thresholds in order to minimise the risks of oscillation and bothersome alarms; • reporting redundancies between alarms (several alarms indicating the same problem or tripping repeatedly for the same reason); • determining the target alarm rates in both normal and degraded modes that are compatible with operators' processing capacities (see ISA 18.2 or EEMUA 191 Standards); • differentiating alarms by type and priority (tone, modulation, vibrations, etc.); • facilitating acknowledgment of alarms from the control station (minimum movement, quick access to the block diagram); • selecting alarms to be displayed for compliance with the target alarm rate, and indicating their priority level (at most 3 levels); • defining an alarm management strategy for both future on-site automated projects and alarm modifications.			to

- [1] DGPR/BARPI . « Sensors, compliant with safety? ». Accident analysis of industrial automation, part 1/3, June 2012. Available at : ***http://www.aria.developpement-durable.gouv.fr/analyses-and-feedback/by-theme/sensors-accidents-analysis/?lang=en***
- [2] BAINBRIDGE, L. « Ironies of automation ». Automatica, 19, pp. 775-779, 1983.
- [3] (in French) DGPR/BARPI. « Inventaire 2013 des accidents technologiques ». Available at : ***http://www.aria.developpement-durable.gouv.fr/inventaire-2013/***
- [4] ***(in French)*** Dossiers de sécurité fonctionnelle. « Instrumentation : des équipements à surveiller de près ». Mesure, n° 813, March 2009.
- [5] HEALTH AND SAFETY EXECUTIVE. « Human factors aspects of remote operations in process plants ». Contract research report, 432 / 2002, ISBN 0 7176 2355 6.
- [6] ***(in French)*** COLLMELLERE, C. « Quand les concepteurs anticipent l'organisation pour la maîtrise des risques : deux projets de modifications d'installations sur deux sites classés Seveso 2 ». Thèse de doctorat de sociologie, Université technologique de Compiègne, 566 p., 2008.
- [7] MOULTON, B. ; FORREST, Y. « Accidents will happen : safety critical knowledge and automated control systems ». New Technology, Work and Employment 20:2, ISSN 0268-1072.
- [8] ***(in French)*** BARIL, R. « Les transformations du travail des opérateurs de raffinerie de pétrole : le passage des cadrans aux écrans ». Pistes, vol n° 1, November 1999.
- [9] CHARETTE, R. N. « Automated to death ». IEEE Spectrum, December 2009. Available at : ***http://spectrum.ieee.org/computing/software/automated-to-death***.
- [10] ***(in French)*** Repères. « Alarmes et diagnostics : des composants essentiels ». Jautomatise, n° 77, pp. 44-47, July-August 2011.
- [11] « Alarm management best pratices: are you following them ? ». Automation world, 8th Ferbruary 2012. Available at: ***http://www.automationworld.com/operations/alarm-management-best-practices-are-you-following-them***.
- [12] STAUFFER, T. et al. « Managing alarm using rationalization ». Control engineering, 3rd March 2011. Available at : ***http://www.controleng.com/single-article/managing-alarms-using-rationalization/13efb381a8d417b6f7d16b3140799f29.html***.
- [13] PARASURAMAN, R. ; RILEY, V. « Humans and Automation : Use, Misuse, Disuse, Abuse ». Human factors, 39, pp. 230-253, 1997.
- [14] ***(in French)*** LEVARAY, J.P. « Putain d'usine ». Editions de l'insomniaque, 94 p., 2002, ISBN 2 9087 4445 7.
- [15] RALEIGH, P. « Operating procedure key to process safety ». Process engineering, 16th July 2012. Available at : ***http://processengineering.theengineer.co.uk/operating-procedure-key-to-process-safety/1013172.article***.
- [16] ***(in French)*** FANCHINI, H. « Imagerie de conduite industrielle : le choix des images, le poids des maux ». Le travail humain, tome 54, n° 3, 1991.
- [17] ***(in French)*** Repères. « L'opérateur : le maillon faible ? ». Jautomatise n° 53, pp. 52-57, July-August 2007.
- [18] ***(in French)*** DANIELLOU, F., SIMARD, M., BOISSIERES, I. « Facteurs humains et organisationnels de la sécurité industrielle, un état de l'art ». Numéro 2012-02 des *Cahiers de la sécurité industrielle*, ICSI, Toulouse, 2010, ISSN 2100-3874
- [19] SWAIN, A.D., GUTTMANN, H.E. « Handbook of Human Reliability Analysis with Emphasis on Nuclear Power Plant Applications ». NUREG/CR-1278, USNRC,1983.
- [20] ***(in French)*** DANIELLOU, F. « L'opérateur, la vanne, l'écran. L'ergonomie des salles de contrôle ». Edition de l'ANACT, Collection outils et méthodes, April1986, ISBN 2-03540-34-9.

TECHNOLOGICAL ACCIDENTS ONLINE

Safety and transparency are two legitimate requirements of our society. Therefore, since June 2001, the website www.aria.developpement-durable.gouv.fr hosted by the French Ministry of Ecology, Sustainable Development and Energy has been offering to both professionals and the general public lessons drawn from analyses of technological accidents. The main sections of the website are available in both French and English.

Under the general sections, the interested user can, for example, inquire for the governmental action programmes, access large excerpts of the ARIA database, discover the presentation of the European scale of industrial accidents, become familiar with the ''dangerous substances index'' used to complete the ''communication on the spot'' in case of accident or incident.

The accident description, which serves as the raw input for any method of feedback, represents a significant share of the site's resources : when known, event sequencing, consequences, origins, circumstances, proven or presumed causes, actions taken and lessons learnt are compiled.

Over 250 detailed and illustrated technical reports present accidents selected for their particular interest. Numerous analyses, sorted by technical topic or activities, are also available. The section dedicated to technical recommendations develops various topics : fine chemistry, pyrotechnics, surface treatment, silos, tyre depots, hot work permits, waste treatment, material handling, etc. A multicriteria search engine enables getting information about accidents occurring in France or abroad.

The website **www.aria.developpement-durable.gouv.fr** is continually growing. Currently, more than 40 000 accidents are online, and new theme-based analyses will be regularly added.

This synthesis constitutes the second part of an in-depth study on the accident of industrial automation within the ARIA database. In focusing on the «processing function», this study has presented the main lessons drawn from a detailed analysis of 325 accidents found in the base.

These lessons and recommendations are intended to build awareness among safety professionals working at industrial facilities. The synthesis has revealed that flaws in the processing function of an industrial automated system, responsible for initiating or exacerbating an accident, are for the most part directly ascribable to human errors tied to organisational root causes.
(June 2014)

See also :

Accident analysis of industrial automation, part 1/3 :
« Sensors, compliant with safety ? »

Accident analysis of industrial automation, part 1/3 :
« valves and actuators » (to be published)

The summaries of catalogued events are all available at the site:
www.aria.developpement-durable.gouv.fr

BARPI - Bureau for analysis of industrial risks and pollution
5 place Jules Ferry
69006 Lyon - FRANCE
Phone : + 33 426 286 200

Department for technological risks
General Directorate for Risk Prevention
Ministry of Ecology, Sustainable Development and Energy

Liberté • Égalité • Fraternité
RÉPUBLIQUE FRANÇAISE
Ministère de l'Écologie, du Développement durable et de l'Énergie