SYNTHESIS

BARPI
DGPR SRT

ARIA
Médiathèque interactive de référence en accidentologie industrielle

| January 2020 |

ACCIDENTOLOGY OF INDUSTRIAL AUTOMATIONS PART 3/3:

Actuators

Ministry for the ecological transition

Ministry for the ecological transition

Sommaire

Introduction

The following is the last of our three-part series on the study of accidents involving industrial automation. This part concerns actuators. The first two parts focussed on sensors and processing, and were published in 2012 and 2014, respectively. Recent examples demonstrate that the conclusions of these studies still remain valid today. Nevertheless, for this third part, a more concise approach has been adopted in which the disruptions encountered are initially highlighted, followed by a presentation of the root causes. A series of recommendations is then proposed based on relevant accidents in the ARIA database.

As in the two previous parts, examples of accidents are presented for illustration purposes throughout the summary. Only elements of the accident relating to actuators are highlighted here. For a complete description of the accident, consult the accident summaries available on the BARPI website at https://www.aria.developpement-durable.gouv.fr/.

Study methodology/sampling

This summary is based on a sample of industrial accidents listed in the ARIA database. The level of information provided for this sample allows for a good understanding of the event (causes, circumstances, consequences). Research based on a specific input field (automatic actuator and manual actuator), then with actuator-associated keywords (synonyms, derivatives), followed by an analysis of the summary for each accident, allowed us to refine this sample. Only accidents meeting at least one of the following 3 criteria were selected for this report :

- ✓ One or more actuators were responsible for the accident;
- ✓ One or more actuators exacerbated the accident (by not operating or, more rarely, by operating);
- ✓ The absence of the actuator(s) caused or exacerbated an accident (if this absence is explicitly mentioned in the accident analysis and its installation was foreseen in the technical follow-up to the accident).

To remain consistent with the first two parts of the industrial automation study, only accidents which occurred from 01/01/1992 to 31/12/2018 were studied. The secondary sample obtained consists of 326 cases, including 28 cases outside of France.

Dam-related accidents, identified in the ARIA database since 2010, were excluded from the analysis.

The ARIA database does not list accidents and incidents that have occurred at nuclear installations (DSC/IRSN databases), or work-related accidents (EPICEA database). As such, the database's specific characteristics may under-represent certain highly automated sectors of activity (nuclear power plants, the automotive and packaging sectors, etc.), which were, therefore, not included in this study.

Moreover, as the ARIA database is an event-driven, non-statistical database (unlike the OREDA, PERD, IEEE, and EXIDA databases), data collection and accident summaries do not always yield accurate information on the criticality or technical causes for the actuator failure, its technology or its level of maintenance. 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 in operation, the relationship that exists between the BARPI and the representatives of the various sectors and the ICPE classification of the accident site (Seveso-classified sites subject to close monitoring, for example).

Part 1: Context of the study

1. Definition of the "actuator" function in industrial automation systems

Industrial automation systems perform 3 functions:

The first function is to detect an accidental situation or an operational deviation in a process. When detection occurs, information is relayed to the automated system. Several types of sensors are used in the industrial environment to detect:

- ✓ Physical parameters: temperature, pressure, density, weight, etc.;
- ✓ Spatial parameters: status, position, level, depth, interface, etc.;
- ✓ Abnormal phenomena: flame, smoke, ATEX, hazardous substances, etc.;
- ✓ Kinematic parameters: flow rate, speed, acceleration, vibration, etc.;
- ✓ Physicochemical parameters: pH, conductivity, resistivity, etc.

The entire accidentology related to these sensors is available in the summary: Accident analysis of industrial automation, part 1/3: Sensors.

The second function consists of all the technical and human components of a PLC required to send information from the sensor to the actuator: the central unit's power supply, transmission units, electronic boards, programming, man-machine interfaces, etc. The connection between the detection function and the processing function is taken into account in this second function.

The entire accidentology related to the processing function is available in the summary: Accident analysis of industrial automation, part 2/3: processing function.

The third function which is the subject of this summary is to act following the information sent by the processing function. The INERIS provides the following definition in its "Omega_10" Guide:

The "act" sub-function is performed by actuators and terminal elements. Actuators convert a signal (electric, pneumatic or hydraulic) into a physical phenomenon that can be used to control the start-up of a pump or the opening/closing of a valve. Depending on the driving energy used, reference is made to an electric, pneumatic or hydraulic actuator. They are coupled to the terminal elements, which are controlled by the actuators. This category includes the following devices: valves, rotating machinery (pumps, compressors, etc.), and audible and visual alarms.

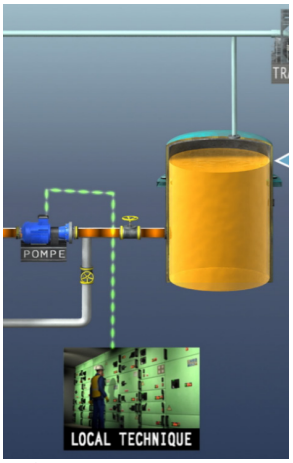


Fig. 1 : example : manual actuator remotely activates a pump - ©BARPI

Among the actuators studied, some are designed for industrial process control, while others, built into instrumented safety systems (see INERIS definition below), constitute preventive, mitigating or protective barriers.

The statistics presented and the analysis conducted on the disruptions and root causes do not take into account the distinction between these two types of actuators. Recommendations specific to instrumented safety systems are also presented in this summary.

OMEGA 10 INERIS: In safety instrumented systems (SIS), the safety function's purpose, performed partially or entirely by the SIS, is to detect hazardous phenomena and to position these elements in their final safe configuration (open/closed, stop/start). The SIS may perform the function completely (detection, processing, final action) or partially (the SIS performs the detection and processing function to include triggering of an alarm; the final action may then be carried out by a human).

The signal conveyed to the actuator, i.e. that which links the "processing" function and "action," is integrated into either the processing function, such as human-machine interfaces, or into the action function when it concerns the signal reaching the actuator (control system, carrier means (electricity, air, oil), etc.). Examples are presented in this summary.

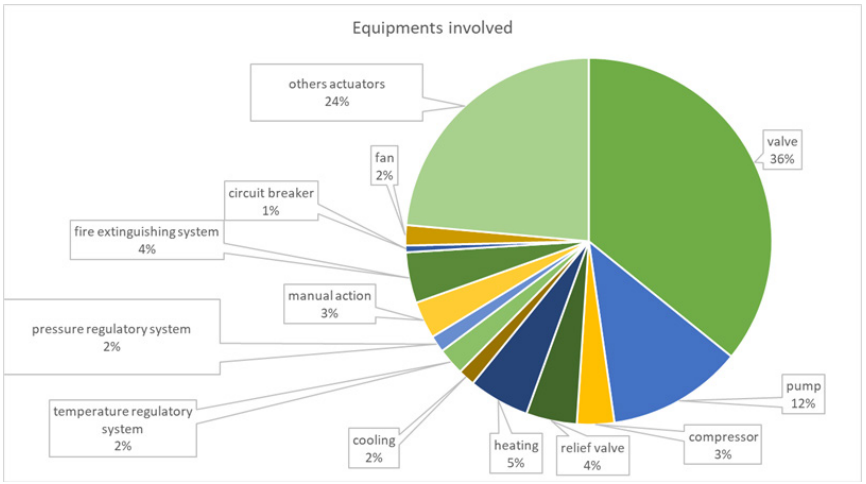
The actuator can also have one or more sensors enabling it to transmit information about their condition, position or if an action has been correctly performed or not (e.g., a valve's end of travel signal).

2. Definition of the field of study

Following the sensors and the processing function, this summary groups together accidents involving the 3rd element of an industrial controller (PLC), i.e. the actuators, as described previously. Manual and automatic actuators were studied. The following were studied :

- ✓ Fluid transfer equipment (check valve, valve, pump, compressor);
- ✓ Systems for regulating the physical parameters (pressure, temperature) of a process (heating, cooling, etc.);
- ✓ Control, prevention or protection devices, which are automatically or manually engaged at the request of a PLC (processing) when parameters are detected by one or more sensors (see Definitions in the previous paragraph).

Completely autonomous systems, not requiring a processing function, such as sprinklers, for example, were not selected for this study.



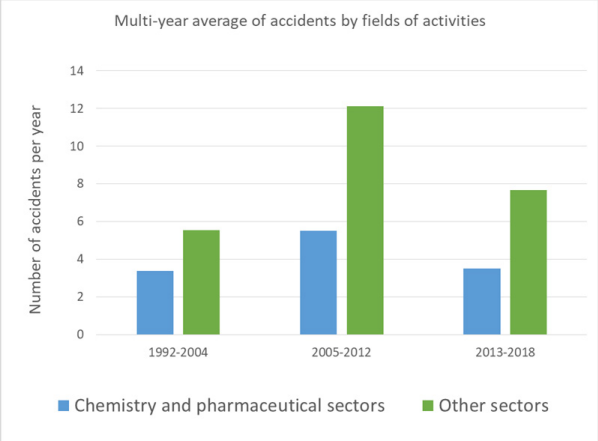
This graph shows the diversity of automatic or manual actuators that can cause incidents or accidents. Fluid transfer devices, such as valves and pumps, account for the majority of the equipment involved.

Part 2: Presentation of the accident analysis

1. Accident statistics overview

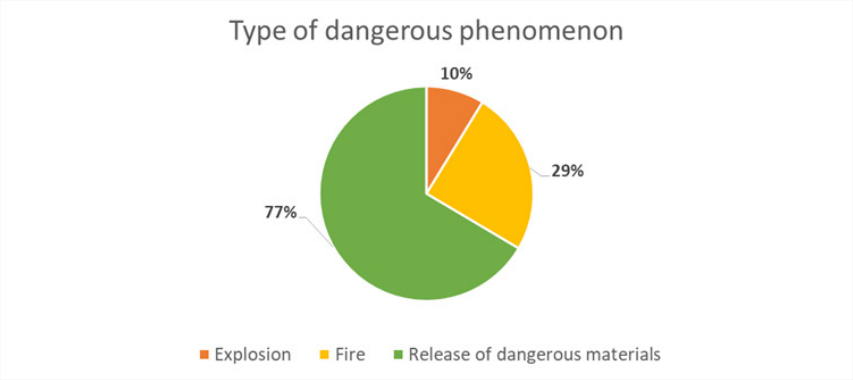
The sectors of activity with the highest number of accidents involving one or more actuators are, firstly, the chemical/pharmaceutical sector, which accounts for 1/3 of the accidents recorded from 1992 to 2018, followed by the food industry, refining and metallurgy sectors, each of which accounts for approximately 10% of the accidents.

The annual number of accidents involving one or more actuators rose sharply from 2005 onwards. The development of automatic actuators in various industries may explain the increase in the number of accidents. Their reliability has since been reinforced, which accounts for the decrease in the number of accidents since 2012.



2. Detailed accident analysis

According to the sample selected, an accident caused or exacerbated by the failure or absence of an actuator often leads to a prolonged release of hazardous substances.



Alongside the majority of the dangerous phenomena highlighted in the selection, the most frequently observed consequences are economic and environmental.

	Sample studied (326 cases)	Industrial plants - ARIA database 1992-2018 (32 571 cases)
HUMAN CONSEQUENCES	**21%**	**22%**
--> Dead	2%	5%
--> Serious injured	4%	5%
--> Total injuries	21%	21%
ECONOMICAL CONSEQUENCES	**72%**	**81%**
--> Internal or external material damage	62%	83%
--> Internal or external operating losses	36%	28%
SOCIAL CONSEQUENCES	**21%**	**23%**
--> Technical unemployment, incapacity for work	3%	10%
--> Deprivation of uses - drinking water, electricity, telephone, public transport and others	3%	3%
--> Noise nuisance	1%	0%
--> Evacuated population	5%	5%
--> Confined population	6%	2%
--> Security perimeter	15%	11%
--> Interruption of traffic	5%	3%
ENVIRONNEMENTAL CONSEQUENCES	**53%**	**33%**
--> Type of attack in the environment: air, water, groundwater, soil	58%	33%
--> Attack on wild flora or fauna, cultivated or exploited species, farm animals	7%	8%
OTHER CONSEQUENCES	3%	2%

Fig. 3 : Consequences

Accidents involving an actuator often have significant economic consequences. Property damage remains associated with the equipment responsible for the accident, which in most cases needs to be replaced. Operating losses are observed in cases where the incident or accident caused the facilities to be shut down and then restarted.

The environmental consequences, those affecting the natural environment through pollution or the release of substance into the atmosphere, surface water or underground aquatic environments and the soil, are higher than the average for accidents that occurred in a classified or similar installation between 1992 and 2018.

In the sample studied, 6 accidents, including 5 explosions, resulted in fatalities involving only employees. There were no external victims.ARIA 3536 (1992): An initial accident led to an explosion, resulting in one death. The partial automation of the unit's emergency shutdown system was implicated in this accident.

ARIA 3536 (1992): An initial accident led to an explosion, resulting in one death. The partial automation of the unit's emergency shutdown system was implicated in this accident.

Fig. 4: ARIA 3536 : view of the involved unit after the explosion - ©Exploitant

ARIA 5989 (1994): Two activities were taking place simultaneously. Due to a programming error, the PLC indicated a valve opening at the time of its reset. These circumstances led to an ammonia leak that injured three workers, one of whom later died.

ARIA 7956 (1995): A hydrogen explosion occurred, followed by a fire which resulted in the death of a technician who was operating valves. The presence of an automatic on/off valve would have prevented a product from being released into a reactor during its washing phase. The reaction of this product with the hydrogen led to the explosion.The following example involves the signal sent to the actuator:

The following example involves the signal sent to the actuator:

ARIA 7069 (1996): The reversal of the control hoses on a pneumatic valve created a position contrary to the logic programmed into the local controller. This situation led to an explosion that resulted in a fatality. Following the accident, the operator installed overview table showing the position of the valves on the powder supply systems based on limit switches and a mechanical lockout system.

ARIA 14700 (1997): An explosion was exacerbated by the lack of an automatic emergency stop system. An employee attempting to manually actuate the emergency stop died in the fire caused by the explosion.

ARIA 12280 (1998): Originally, a suspected malfunction in the control device of a furnace door led to the explosion of the furnace, resulting in a fatality.

In the last 20 years, there have been no deaths as a result of an actuator-related accident.

Part 3: Causal analysis of incidents/accidents

1. BARPI's approach to causal analysis

For the causal analysis of incidents/accidents involving one or more actuators, the methodology developed by BARPI and used in this summary is based on a simple process, which leads to the characterisation of 3 distinct blocks:

Disruptions are deviations from the expected operation that lead to a dangerous phenomenon. Such deviations can include equipment failures, inappropriate human intervention, natural disasters or technological hazards.

The origins of such disruptions are generally less visible. These are the actual **causes**, sometimes referred to as the root causes of the accidents. The causes can be of several kinds:

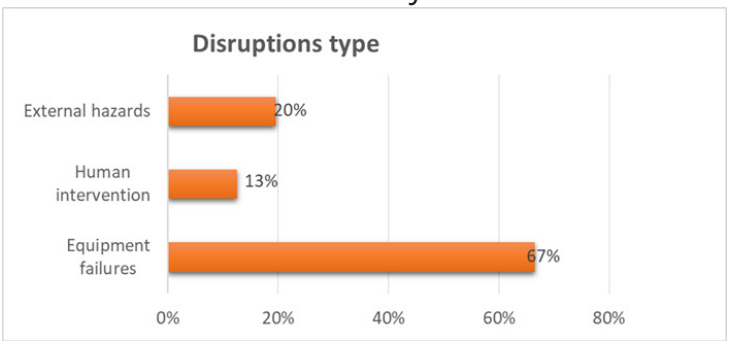
Organisational factors	Organisational factors concern the working environment and the risk management measures such as the organisation of inspections, the management of training and in-house and external skills, procedures and instructions, identification of risks, organisation of the work and supervision, communication, ergonomics, and the choice of equipment and processes, etc.
Human factors	These are factors that disrupt the physical/cognitive/mental abilities of an employee at the site and which are not the organisation's responsibility.
Unknown factors	These are elements that cause a disruption but cannot be anticipated or controlled by the organisation in place at the site. e.g., manufacturing defects.

One accident may involve several of these blocks, causes, disruptions and hazardous phenomena, due to a succession of disruptions and their causes.

As a first step, the following chapter touches upon the main disruptions resulting in accidents in which one or more actuators are involved. The root causes will be developed afterwards.

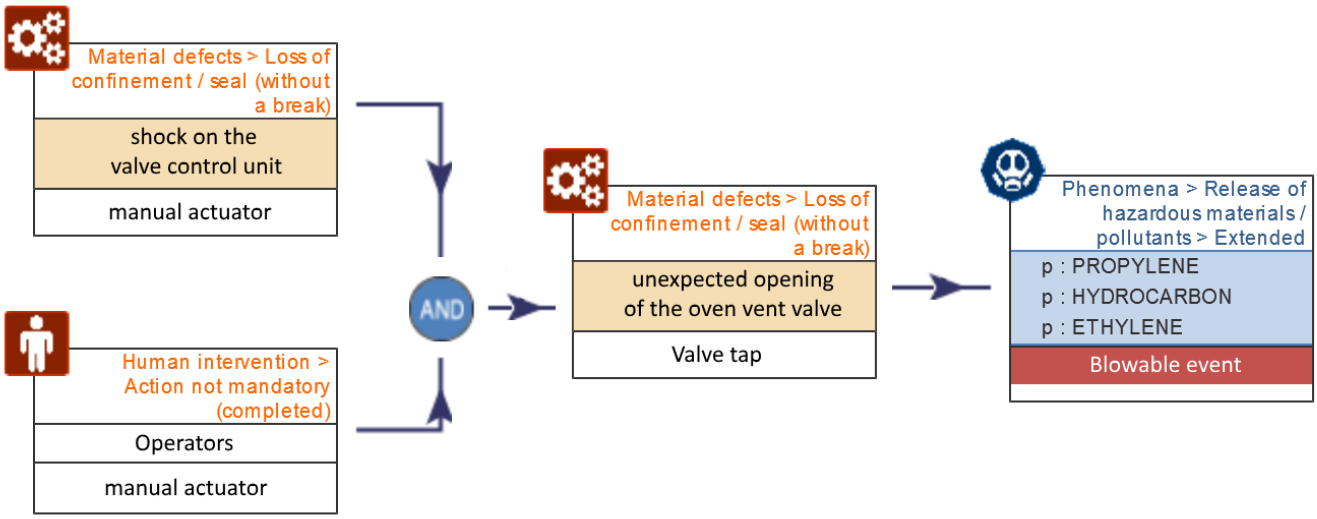
2. Analysis of disruptions

The histogram below shows the distribution of the primary causes, referred to as disruptions, in which an actuator was responsible for an accident. The percentages are expressed in relation to the total number of accidents for which information is available: out of 326 accidents, there are 287 (i.e. 88% of the cases) for which some knowledge is available (proven or supposed) about the primary cause of the event. This high percentage is explained by the fact that the accidents were selected according to their relevance for inclusion in this study.



In this histogram, the total percentage is equal to 100% because only the primary cause has been selected, i.e. the one that led directly to the hazardous phenomenon (see BARPI graph). However, this primary cause may be the result of a combination of disruptions. For example:

✓ unnecessary human intervention associated with an equipment defect



✓ a PLC malfunction associated with improper human intervention

ARIA 31023 (16/11/2005): Pollution of watercourses by phytosanitary products:

In a phytosanitary product production facility (herbicides, rat control products, etc.), 4.5 m^3 of a head lice solution containing organophosphorus substances was released into a river, polluting streams and ponds over at least 4 km. **The accident resulted from the combined failure of an automatic valve and human error** (opening of a manual valve) during a transfer operation. The hazardous product was released from a storage tank and entered an undersized containment system. Two people, including 1 employee, were sickened by the fumes emanating from the phytosanitary products; the delivery driver, sickened by the fumes, was evacuated. Hundreds of dead fish were discovered.

2.1. Equipment failures

The largest share of disruptions identified in the sample (67%) fall into the "equipment failures" category, which contains several sub-categories.

Firstly, internal faults or malfunctions specific to the actuator itself or its control system can be detailed as follows::

✓ Failures or malfunctions that are not precisely determined (which concern approximately 50% of equipment failures);
✓ Systems that are inoperative when solicited, which mainly concern valves and check valves, such as an actuator that is blocked open or closed: ARIA 32806, 39929, 46230;
✓ Inadvertent trigger, such as actuators that trigger for no particular reason: ARIA 22858, 42726, 50424, 49833;
✓ Faulty control systems: ARIA 22793;

✓ Malfunctions concerning the close limit switch signal, such as the valve closing signal, indicating that the valve is closed although it is opened: ARIA 22553, 25057;
✓ Failures for actuators in more complex systems such as cooling systems or pumps: ARIA 26475, 31935.

In the event of a fire, when internal malfunctions affect protective systems, such as automatic extinguishing systems, the actuator's failure can exacerbate an ongoing event: ARIA 32253, 49093.

ARIA 43181 (22/12/2012): Cracked gas compressor fire

An oil fire broke out on a cracked gas compressor in a steam cracking unit of a Seveso-classified petrochemical site. Operations to secure the installations resulted in hydrocarbons being directed to the unit's flare stack with the release of thick black smoke for 24 hours. The emergency services received many calls from area residents.

The site had been restarted 10 days earlier following a five-year maintenance shutdown during which the compressor line had been overhauled.

The post-accident technical analysis revealed that an impact wrench had been forgotten on the 3rd level of the compressor during the five-year maintenance shutdown. On the day of the accident, the wrench managed to enter the lower stages of the compressor and strike the impellers, causing significant vibrations which then triggered the emergency safety shutdown of the compressor. At this point, **certain safety devices associated with the compressor's safety shutdown procedure malfunctioned:** an insulation fault on the compressor caused by a fouled check valve and a poorly-closed motorised valve, its electric motor switched off following the shutdown, malfunction of the internal components ensuring the seal between the oil and gases and pressure balance during safety shutdown.


fig. 5 : compressors on chemical site - ©DRIRE

These malfunctions allowed part of the cracked gases to pass through the packing and into the oil which then caught fire.

The sample also shows disruptions related to the design of the system and its instrumentation:

✓ Actuator not in compliance with the intended model: ARIA 41870;
✓ Unsuitable actuator material: ARIA 39629;
✓ Undersized actuator: ARIA 34733, for actuators installed in a protective system, this could result in a loss of efficiency, such as in fire extinguishing systems;
✓ Excessive actuator response time: ARIA 26925, 22320, 41517;
✓ Discrepancy problem: the information available in the processing system does not correspond to the actuator's actual position. Examples for valves: ARIA 38027 and 41300. Information on the actuator's actual position may not be available in the processing system: ARIA 52784;
✓ Manufacturing defect: ARIA 51165;
✓ System degradation over time: ARIA 41516.

Disruptions such as leaks or loss of containment (ARIA 48845, 42415, 41870) or, conversely, clogging and/or fouling (ARIA 6343, 51505) of the automation systems, which cannot then fulfil their function, are highlighted in the sample. For this type of disruption, the root causes are related to a lack of inspection or maintenance faults (see next chapter).

2.2. Human interventions

Fig. 6: human in front of commands panel

Material defects are not the only disruptions that appear in the accident sample studied. They can sometimes be combined with human interventions that have led operators to either initiate an action that is not necessary or fail to perform or to carry out correctly a required action (misperception, misinterpretation, execution or decision-making error, etc.).

Human interventions on systems that include an actuator can result in erroneous actions during the various phases of an installation's life cycle:

2.2.1. During the design phase

During the automated system's design phase (equipment selection, programming, etc.), a human error or a wrong choice can then lead to a failure on the action to be performed by the actuator when it is engaged:

- ✓ Actuator programming error: ARIA 43695 , 17253;
- ✓ System dimensioning error: ARIA 18411;
- ✓ Incorrect actuator programming choice, fail-safe or non-fail-safe: ARIA 38055, 36390, 42921, 42920, 47536.

This means that the possibility of the actuator entering fail-safe mode and the associated risks in the event of a failure must be investigated.

The **fail-safe mode**, for actuators built into a safety instrumented system (SIS), means that, in the event of an actuator failure or loss of power or signal processing error, the actuator is programmed to assume the position in which its safety function is performed. Examples: if a valve is used to confine a system in the event of a leak, its fail-safe position will be 'closed'; on the other hand, if a valve is used to drain a system, its fail-safe position will be 'open'. This is why decision-making or interpretation errors can occur with regard to the fail-safe position that is chosen.

2.2.2. During the construction / assembly phase

Other human interventions resulting in system failures occur when the actuator is installed in its control system (assembly, connection, alignment):

- ✓ Fluid connection error (electricity): ARIA 10165;
- ✓ Actuator positioning error in the installation's system: ARIA 19596;
- ✓ Failure to check alignment ARIA 50755;
- ✓ Reversal of control hoses (pneumatic) and no limit of travel signal: ARIA 7069;
- ✓ Faulty actuator installation: ARIA 45061, 49845;
- ✓ Incorrect valve/check-valve setting ARIA 12671.
- ✓ Tightening error: ARIA 49161.

Fig. 7: ARIA 44070: locking valve opened by error - ©Exploitant

A complete summary covering alignment errors (system positioning) is available on the BARPI website. Certain accidents may concern actuators; the purpose here is not to repeat the conclusions of this summary.

2.2.3. In the operation phase

Certain automated systems also require manual action on the actuator following an alarm, for example. In this case, the accident may be related to:

- ✓ An alarm acknowledged without further action: ARIA 53080;
- ✓ An error on the equipment to be operated: action performed on the wrong tank (ARIA 13228), the wrong valve was closed or opened, for example;
- ✓ An error concerning the operation to be performed: ARIA 47277, 50055;
- ✓ Opening instead of closing and/or vice versa: ARIA 35863;
- ✓ Valve left open: ARIA 10165, 47813;

ARIA 8325 (15/02/1996): Spillage of diesel fuel and pollution of two rivers

In a transport company, a lorry driver left his vehicle unattended while filling the tank with the nozzle latched. The system designed to automatically shut off the flow of fuel when the tank is full had malfunctioned, and several hundreds of litres of diesel fuel spilt onto the ground, making its way to the ERIE and LEYSSE rivers. The company's director was required to regularise its administrative situation and bring its flammable liquid distribution installation into line with current standards.

2.2.4. In the maintenance, inspection and/or work phase

In the sample studied, it is noted that incorrect human intervention takes place more particularly during maintenance, inspection and/or work phases.

ARIA 43695 (04/18/2013) : Boiler plant incident at a pharmaceutical plant

A natural gas-fired boiler at a lower-tier Seveso pharmaceutical plant overheated at around 11:50 a.m. after being restarted. A subcontractor's technician in charge of operating the boiler plant restarted thermal oxidation of VOCs via the human-machine interface and sent the VOCs to the combustion chamber at around 11:30 a.m. Several minutes later, the LEL alarm sounded. The boiler went into bypass mode and then automatically into safe mode. The technician noticed the beginnings of a fire on the VOC supply pipe located in the area of the main fan on the first floor.

The fire was caused by excess fuel laden with VOCs due to **a design error in the VOC facility's software program** which made it possible to switch to incineration regardless of the LEL of the mixture. The VOC facility had been restarted following preventive maintenance performed by a subcontractor. However, the existing safety system, which was controlled by explosivity thresholds and deviated VOC streams if the thresholds were reached, only operated in incineration mode. The operator modified the VOC facility's software program. **A valve position error (withdrawal and control) due to different controls between automatic and manual mode** caused all the heavily VOC-laden condensates to be reinjected. The operator supplemented the procedure for controlling the fractionating column and the PLC change management process (automatic/manual) with additional information.

These unfortunate actions are encountered either during the intervention itself or when systems are shut down or restarted. These phases are critical transitory moments in the operations of an industrial installation.

Changes made to the system's usual operating mode: shunt, by-pass, switch to manual mode, different technicians than usual (subcontractor or internal maintenance technician). All these situations

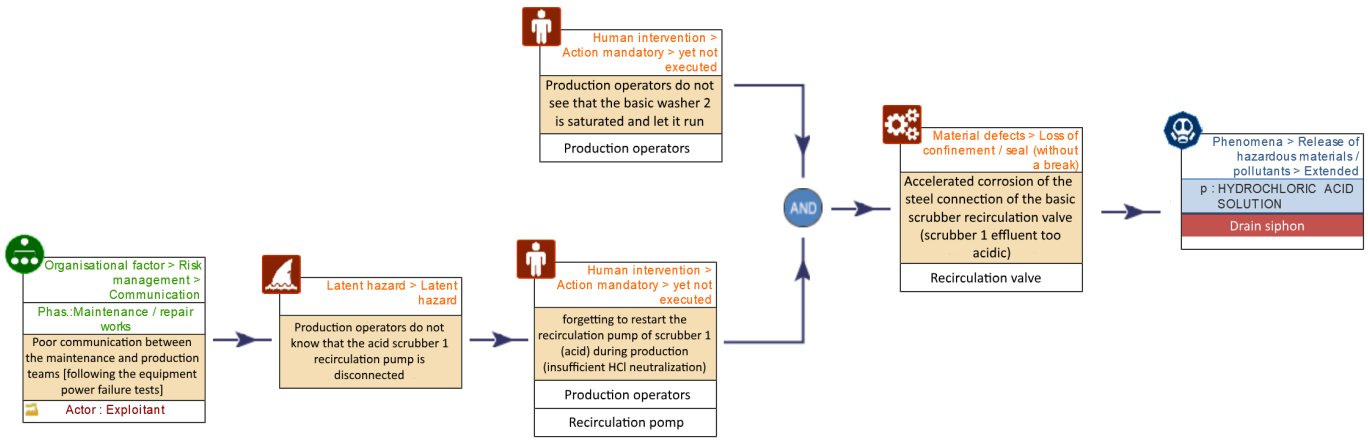
may have led to actuator-induced accidents.

Shunt or by-pass: automated systems may have been taken out of service to allow an intervention to be performed on system equipment or on another installation near the shunted system to prevent its unintentional tripping (e.g., in stop/start phases). In these situations, the actuators were by-passed, although compensatory measures were in place during the intervention. When the intervention was completed, the by-pass had not been removed when the entire system was put back into operation: ARIA 9967, 25239.

Switch to manual mode: The transient stop/restart phases are sometimes subject to changes in the process' operation including, in particular, the switchover of certain actuators, typically in automatic mode, to manual mode: ARIA 11181, 50604, 44896, 35882, 34624, 43736, 45692. Errors are then committed by technicians who are not familiar with this mode of operation. For example, a valve was opened when the order was not required at that specific time: ARIA 44793. In this operating configuration of an installationinsufficient risk analysis before maintenance work may also lead to human errors: ARIA 32484.

Subcontracting: In the maintenance and/or work phases, some accidents involve subcontractors who have performed repairs on actuators: ARIA 16080, 22573, 44996, 48569, 50109. These accidents also point to a lack of verification/acceptance of the work by the site's operator following maintenance work (see the following chapter on the root causes).

ARIA 45692 - Hydrochloric acid leakage in a chemical plant



BARPI has compiled a complete summary of subcontracting-related accidents, some of which may involve actuators. The conclusions of this summary are available on the BARPI website at the following link: Subcontracting and risk control.

2.3. External hazards

This paragraph presents the disruptions that are external to the equipment itself or the installation as a whole.

2.3.1. External hazards of natural origin

Such hazards are mainly weather-related: lightning (ARIA 52087) or freezing up of the actuator (ARIA 38027) can render them inoperative.

An event was caused by a major earthquake that hit Japan in 2011: ARIA 40256.

2.3.2. Hazards of man-made origin

The actuator is involved in a man-made event. Examples:

- ✓ A pump caught in a fire was unable to function: ARIA 14700;
- ✓ Hammering on a valve: ARIA 42163;
- ✓ Impact on a valve: ARIA 52194;
- ✓ A fire in an electrical power supply unit of the PLC controlling the actuator: ARIA 50793.

Malicious actions can also cause an actuator to malfunction: ARIA 7435.

Fig. 8: ARIA 50793 : intervention in a slaughterhouse for fire of an electrical box leading to an ammonia leak ©Synergi

2.3.3. Loss of utilities

Some of the events in the accident sample studied were caused by a loss of utilities. Where actuators are concerned, this can result in the loss of the electrical, air or hydraulic power supply depending on the type of actuator:

Fig. 9: ARIA 54499 : fire in electrical cables supplying an ammonia pipe isolating solenoid valve - ©DREAL

- ✓ Loss of electrical power supply (ARIA 42235): general electrical failure (ARIA 35841, 49984), faulty electrical installation (ARIA 36110, 48580), connection fault (ARIA 36198, 49965), thunderstorm-induced power failure (ARIA 36770, 40197), internal short-circuit (ARIA 32132, 40506), Ethernet connection fault (ARIA 43639);
- ✓ Loss of air supply: rupture of compressed air line controlling an automatic valve (ARIA 7131), leak of compressed air supplying a pressurised transfer system (ARIA 19969), valve fails to open upon lack of air (ARIA 49735);
- ✓ Power supply failure on hydraulic pressure-operated components: ARIA 7440 and 22683.This is why it is important to study the actuators' fail-safe position and the risks associated with the loss of utilities or signal.

This is why it is important to study the actuators' fail-safe position and the risks associated with the loss of utilities or signal.

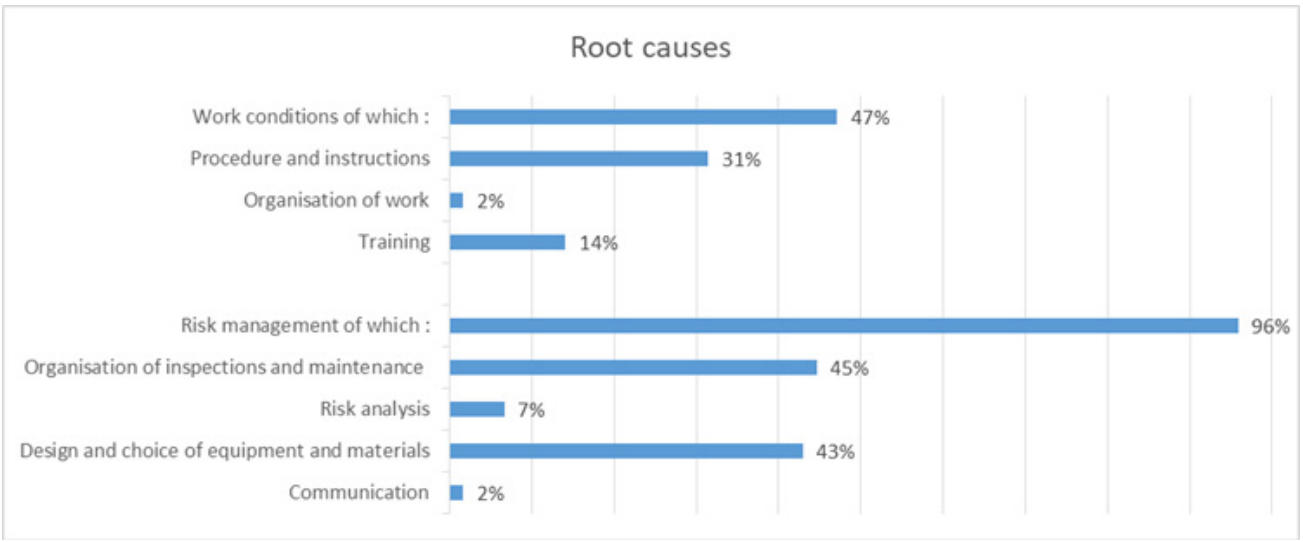
Once these various disruptions have been brought to light, it is important to identify the root causes of accidents or incidents involving one or more actuators. There are many reasons for researching the causes:

- ✓ To prevent new accidents from reoccurring at the same site;
- ✓ To allow all those involved to benefit from the lessons learnt from the accident by sharing the feedback;
- ✓ To efficiently identify malfunctions at the site and correct them with appropriate measures and not only with measures focused on the symptoms (disruptions);
- ✓ To share a more realistic vision of the safety organisation at an industrial site with the authorities. For SEVESO sites, the Safety Management System (SMS) includes chapters dealing with the organisation of sites in terms of safety;
- ✓ On the other hand, on sites subject to operating authorisation, prefectural orders do not always address these organisational factors. Only a few chapters deal with training or procedures and instructions.

Particularly for the topic considered here, certain accidents are caused by a series of malfunctions. In such cases, it is essential to search for the root causes in order to trace possible common modes and to remove any root cause that could potentially lead to accidents.

3. Analysis of root causes

The accidents studied were selected according to their relevance to the subject under study. For the most part, they are instructive in terms of organisational factors. As seen previously, many of the disruptions affecting the actuators are of hardware origin. But the analysis must not stop there, otherwise all accidents could be avoided if the only issue was equipment reliability. In addition to these disruptions, the root malfunctions referred to as 'causes' or 'root causes', must be identified to ensure that they will not be repeated. These causes, which may be multiple or common depending on the accident, will be the basis for implementing appropriate actions to combat the primary failures in a sustainable manner, whether of hardware or human origin or external to the system, as described in the previous chapter.



The main root causes identified can be grouped into the following 3 categories:

- ✓ The design and choice of equipment and materials (43%);
- ✓ The organisation of inspections and maintenance operations (45%);
- ✓ The procedures, instructions and training of technicians (45%).

The percentage is higher than 100% because several root causes were identified in some cases.

The root causes that next emerge in the sample point to the need for change management and risk analysis. For the sample in question, when an in-depth analysis of the accident is conducted, a series of root causes is revealed which often involve the organisation of the work or communication.

3.1. Design and choice of equipment and materials (43%)

Firstly, the problems identified in the accidents studied were related to the actuators' design or to the original choice of equipment and materials for the actuators that were not questioned during operation:

- ✓ An internal design fault of the actuator itself; leading to, e.g., non-compliant actuator or unsuitable actuator material;
- ✓ Absence of an automatic actuator: non-automated pump or valve, non-automated global safety system, therefore manual action was required but was not or was improperly performed (refer to human interventions in the operation phase): ARIA 53080;
- ✓ System completely absent: ARIA 47536, 51178;
- ✓ The function performed by the actuator is not relevant in case of process deviation: ARIA 52379;
- ✓ Unsuitable design of process control operation: ARIA 49983, 41517, 40522;

✓ Actuator trip threshold problem for built-in pressure or temperature type control systems: ARIA 47781;
✓ Lack of redundant control: ARIA 40092;
✓ Lack of operational feedback (good and/or bad) in the control room: ARIA 32484.

Fig. 10: Redondant system - ©pxhere

3.2. Organisation of inspections and maintenance (45%)

Secondly, for all the actuators that were unable to fulfil their function due to a failure, loss of integrity or clogging, the root causes are most often related to faulty maintenance and/or inspection:

✓ Lack of inspection: ARIA 49735, 36385, 33626, 50755;
✓ Lack of a preventive maintenance program: ARIA 42275, 51721;
✓ Insufficient maintenance: ARIA 48833, 21967;
✓ Inspection planned but not performed: ARIA 6343, 51505;
✓ Insufficient inspections: ARIA 46555, 50235;
✓ Lack of preliminary equipment testing: ARIA 17740;
✓ Inappropriate testing: ARIA 49752, 50339;
✓ The entire fail-safe channel had not been tested: ARIA 30920;
✓ No monitoring of anomalies in place: ARIA 7069;
✓ No checks performed following the intervention on the equipment by a subcontractor: ARIA 36198.

ARIA 45744 (22/09/2014): Projection of ammonia during a maintenance operation on an etching bath

The accident occurred in a printed circuit board manufacturing facility. **The pumps supplying the etching baths unexpectedly started although a maintenance operation was in progress.** The two technicians conducting the visual inspection on the injection nozzles were sprayed with ammonia and ammonium chloride.

The machine had not been entirely shut down before this weekly maintenance operation and had been in standby or heating mode. This mode allows the PLC to regularly restart the pumps to homogenize the bath. The operator modified the intervention procedure by specifying that the machine must be stopped using the isolating switch before opening the etching module.

As far as the subcontracting operations are concerned, human errors were highlighted in the previous paragraph. Throughout the rest of this document, a few recommendations will be made specifically concerning the actions of subcontractors on the actuators and the importance of monitoring them. The complete analysis of the accidentology related to subcontracting operations is available on the BARPI website: Subcontracting and risk control.

3.3. Procedures, instructions and training (45%)

Alongside the actions to be performed daily by the technicians in charge of controlling the process, or even the maintenance and inspection of the equipment, the associated procedures and training must also be carried out. These elements are sometimes lacking, or not sufficiently explicit, to allow the technicians to take appropriate action:

- ✓ Lack of instructions or procedures: ARIA 33487, 19596;
- ✓ Inappropriate instructions or procedures: ARIA 12671, 27564, 39629;
- ✓ Lack of clarity in existing instructions and procedures: ARIA 3536;
- ✓ Disregard for instructions or procedures: ARIA 48639, 18563;
- ✓ Technicians' lack of knowledge about the operation of the automatic system: ARIA 2684;
- ✓ Training: ARIA 23010.

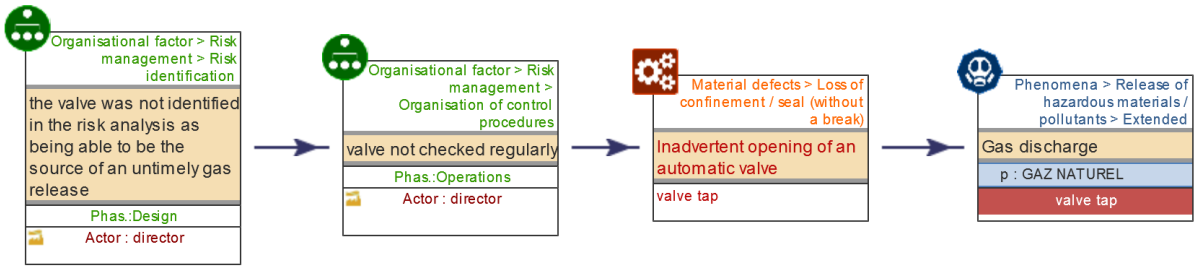
3.4. Change management

Accidents that have been caused or exacerbated by the actuation or non-actuation of an actuator can sometimes be the result of system malfunctions. The organisation must be able to ensure that the equipment is capable of fulfilling its function, particularly when it is considered as a safety barrier. For SEVESO high threshold establishments, the SMS is a means to track these changes:

- ✓ Modifications not taken into account by the technicians or not integrated into the operating or safety system: ARIA 16080 (modification also performed by a subcontractor), ARIA 36599;
- ✓ Modifications resulting in a temporary installation: ARIA 30691;
- ✓ Change management without preliminary risk analysis: ARIA 35863.

3.5. Risk analysis

The root causes stemming from the risk analysis itself tend to come after an initially identified root cause. For example, the release of a hazardous material is due to a physical disruption, associated with a control failure, due to a lack of risk identification during the analysis



Among the sample studied, various accidents illustrate this situation, including, in particular:

- ✓ Equipment that was not included in the risk analysis: ARIA 52784;
- ✓ Initiating elements not studied in the risk analysis ARIA 38601;
- ✓ A scenario not considered by the manufacturer: ARIA 50490;
- ✓ A scenario not considered by the operator in its hazard study: 35215, 36110, 39898;
- ✓ Shortcomings in risk analysis: ARIA 21967, 25057, 32484.

Transitory phases must be taken into account in risk analyses: such phases must be given particular attention, notably changes involving how installations are operated during these phases: switching to manual mode although the installation is normally in automatic mode (see the chapter on human interventions during these critical phases).

3.6. Organisation of work, division of labour, communication

As with risk analysis, the organisation of work and/or communication intervene in accidents, most often at the 2nd root cause level.

To trace back to these causes, an in-depth accident analysis must be conducted to challenge the common building blocks of an existing organisation, such as:

- ✓ The definition of everyone's roles and responsibilities, in terms of maintenance operations for example: ARIA 31238;
- ✓ Communication of instructions during shift changes: ARIA 42644, 35863, 46230.

Once all the causes have been identified, actions must be undertaken to correct them.

Part 4: Recommendations

After analysing the accident sample and identifying the disruptions and the origin of the root causes, recommendations can be made to prevent them from reoccurring. Firstly, technical measures can be taken to address material failures primarily and to prevent erroneous human interventions. As explained above, these technical measures cannot provide in-depth system improvement. For this reason, a set of measures will be proposed to deal with organisational and human factors. An example of a relatively old accident is presented below, which shows a range of technical measures along with essential organisational changes.

ARIA 3536 (04/22/1992) : Explosion on an H2O2 unit

An explosion perceived tens of km around and an ensuing fire destroyed 1,000 of the 4,000 m^2 of a hydrogen peroxide unit (H2O2) located near a series of hydrogen and chlorine tanks.

This accident was due to a defect in the electrical supply card in one of the unit's control system (digital command control) cabinets. The situation was exacerbated by: **partial automation of the unit's emergency shutdown function**, non-independent control / security features, **insufficient controls over the proper sequencing of installation security** combined with several manual steps failing to be carried out by technicians to assist with the nighttime shutdown.

Several technical and organisational improvements were introduced at the site: **enhancement of the command/control system** (safety system designed for an emergency shutdown independent of the operating control device), new control room, **improved workstation comfort/ergonomics**, redefined scope of site intervention, **more efficient information dissemination / training, publication of adapted safety instructions**, and completion of **safety reports** dedicated to the manufacturing, transfer and storage of H2O2.

1. Technical measures

The first recommendation that repeatedly emerges from the analysis of the sample is to study the pertinence of installing automatic actuators where there are none or where manual action was required instead.

A high degree of vigilance must be implemented in system transformation. Transformations cannot be performed without a prior assessment of the technical aspects (design, location, access, modification during a technical shutdown, etc.) and the suitability of the actuator to be installed (response time, responsive action, etc.). For such modifications, the appropriate expert must be involved:

- ✓ The users of the previous and the future system, who are knowledgeable about the process into which the future actuator will be installed;
- ✓ The manufacturers, who have extensive knowledge of the various technologies employed and who will be able to provide the best response as required;
- ✓ Maintenance technicians to check the maintainability of the system over time.

Within the scope of the modifications made to automatic systems, a preliminary study must be conducted to determine the impact of these changes on process control, safety, maintenance, etc. To do this, risk analyses must be conducted or updated if they currently exist.

Depending on the modifications considered, the organisational provisions associated with the control and/or safety system will have to be updated: procedures, training, by-pass conditions, etc. (See the following paragraph).

Fig. 11: electrical safety chain for transmission of the fault signal (ARIA 54305) - ©Exploitant

Based on the sample studied, simple hardware modifications to better meet the desired function include:

√ Modification of the materials used for the actuator: ARIA 39629;
√ Addition of two automatic on/off valves: ARIA 7956;
√ Simplification of systems: ARIA 16080;
√ Changing of the fail-safe position: ARIA 36390;

In light of these examples, we can see that if modifications were made to a correct system involved in an accident, then the modifications also need to be made on similar systems at the same site or even at other workshops and sites. Applying these measures on equivalent systems appears to be essential to prevent an accident happening again in the same unit or on the same site. The sharing of feedback with other sites helps develop collective safety.

Redundancy can also be used to improve the actuator's function:

√ Installation of a second complete safety channel, independent of the first: ARIA 2684, 30920, 40379;
√ Redundancy to supply power to the actuator to prevent the loss of utilities: ARIA 35841.
√ The installation of additional alarms is also a means of detecting actuator failures to improve the reliability of automatic systems:
√ Position indicators or end of travel sensors: ARIA 7069, 20941, 32798, 38485;
√ Alarm reporting to signal actuator operation: ARIA 46555 (pump);
√ Alarms on electrical systems to prevent the loss of utilities: ARIA 36110, 50121;
√ Discrepancy alarm: ARIA 52784;
√ Installation of a device showing the position of the actuator: ARIA 39362.

In general, the alarms then require manual action. Therefore, "information processing" by the technicians is required before action is taken. It is essential to pay particular attention to the **management of alarm priorities**, in particular, by means of instructions or procedures, or by the ergonomics and organisation of the control rooms, and the distribution of roles and responsibilities of the technicians.

The reliability of actuator position sensors must also be checked. In this respect, the conclusions of part 1/3 of the summary concerning sensors (accident analysis of industrial automation), should be noted: Accident analysis of industrial automation, part 1/3: Sensors.

2. Organisational provisions

Organisational provisions are paramount to avoid the biases associated with over-automated systems: man must remain in control of the system and is sometimes the ultimate means for regaining control when things go wrong. To do this, the right tools must be available, combined with a good knowledge of the field and regular refresher courses, which are also aimed at experts, and a certain autonomy in the actions that can be performed. The more complex the system is, the more time it will take to analyse a situation and provide the appropriate response.

The ergonomics of the control rooms and the definition of responsibilities are means to clarify the actions to be taken following possible failures of the actuators installed in automated systems.

As mentioned previously, **system design** has proven to be a root cause that can often lead to actuator failures. The means to correct this are, for example:

✓ Investigate, at the manufacturer's level, the compliance and efficiency of these safety devices (reliability of the pneumatic valve): ARIA 23010;
✓ Conduct tests, check whether the actuator fulfils its function in its operational context: testing of the entire safety channel (sensor, PLC, actuator) and in real conditions: ARIA 23589;

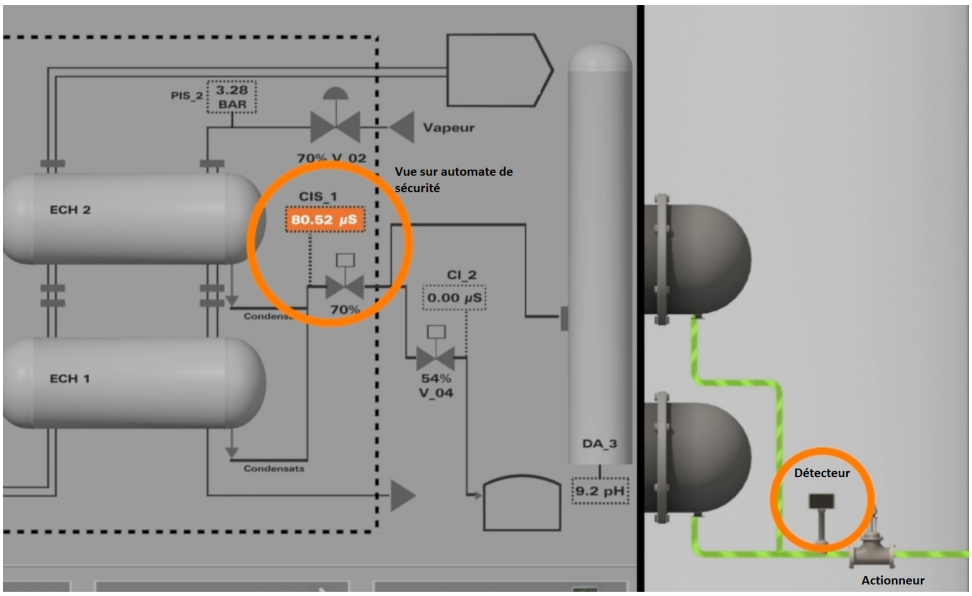


Fig. 12: overview of a safety chain: sensor, PLC, actuator - ©BARPI

✓ Modify process control: ARIA 49983;
✓ Modify PLC programming: ARIA 40522, 47536;
✓ Modify the control between actuator and sensor: ARIA 50490;
✓ Check equipment response time: analysing the entire chain makes it possible to check whether or not the equipment's reactivity is in line with the function to be fulfilled: ARIA 41517;
✓ Integrate the fail-safe position into the design and check that the actuator acts correctly in fail-safe (e.g., ARIA 36390) unless its triggering could generate a new risk and/or lead to significant operating and/or property losses; if the device does not enter the fail-safe condition, the loss of power and circuit integrity must be detected and reported, and compensatory actions must be foreseen;
✓ Verify that the concept is well-proven;
✓ Check the safety level of actuators identified as safety barriers (QUALISIL certification for Seveso facilities, for example).

Concerning the organisation of **inspections and maintenance**, the second set of root causes previously identified, improvements can be based on:

- ✓ Reinforced periodic testing and preventive maintenance: ARIA 23629, 26475, 33626, 35533, 48384, 49845;
- ✓ An increase in the frequency and number of control points: ARIA 21960, 37226, 42921;
- ✓ The qualification or reconfiguration of equipment before initiating a new batch: ARIA 7069;
- ✓ Control of subcontractors: ARIA 25248, 50339;
- ✓ Ensuring that safety barriers out of services are correctly managed: ARIA 42163.

Similarly, procedures, instructions and training must be improved at all hierarchical levels and involve subcontractors, e.g.,

- ✓ Implementation of checklists, programs to raise the awareness of technicians, supervision and on-call management personnel: ARIA 15397;
- ✓ Raising the awareness of external subcontractors: ARIA 50339;
- ✓ Refresher training for drivers: ARIA 49921;
- ✓ Implementation of action to raise staff awareness of the risks inherent to the activities of an installation: ARIA 34116;
- ✓ Review of the training provided to experienced and newly hired employees and drafting of emergency procedures to be followed in the event of a critical alarm: ARIA 48639;
- ✓ Raising the awareness of technicians concerning the risk and the necessary vigilance required: ARIA 34205;

To address the management of transitional phases, staff training is to be improved concerning the temporary removal of safety devices from service: ARIA 32484.

ARIA 42163 (05/14/2012) : Accidental release of phosgene on a chemical platform

Around 11:30, external sensors detected a COCl2 concentration build-up. By 11:52, a pressure sensor on the vapour circuit was reading in the tens of bar, triggering shutdown of the unit by closing shutoff valves on both the enclosure confining the unit and the condensate drainage circuit. **The quick sequence of these closure steps caused a water hammer that broke a drainage valve at the base of the exchanger**; the remaining COCl2 spilled into the enclosure, lowering vacuum pressure and closing the exchanger bypass valves. Only successful implementation of the 2nd safety barrier (pressure sensor and its safety chain, in addition to integrated enclosure confinement) avoided the discharge of a large quantity of toxic gas outside the site boundary (with dwellings as close as 260 m).

Procedures were formalised or consolidated, namely:

- ✓ instructions in case of activation of the unit's technical safety barriers: conductivity meter, pressure sensor, etc.;
- ✓ Bypass of the unit's technical barriers: awareness-building for both technical staff and managers, definition of each team member's roles and responsibilities, clarification and restriction of authorised bypass conditions;
- ✓ Conditions applicable to unit technician certification regarding both process safety and equipment inspection;
- ✓ Formalisation of information/feedback loops among operations teams and the online analyser maintenance department

As the pillars of industrial risk control, risk analyses are often updated or expanded following accidents involving one or more actuators, such as:

- ✓ Updating of hazard studies (site subject to authorisation) following an incident: ARIA 42415;
- ✓ Performance of a hazard and operability study (HAZOP) for complex systems: ARIA 34305, 48639;
- ✓ Pre-emptive identification of electrical supply malfunctions of various safety features, in addition to planning the supply of safety-related priority functions: ARIA 13689;
- ✓ Considerations on controlling the automatic opening of valves to assess the risks of uncontrolled opening: ARIA 50424;
- ✓ Risk analysis according to various operating conditions: ARIA 28649.

Risk analysis must take transitional phases into account. Also, certain technical biases (e.g., lack of knowledge of the installations) and/or economic biases (e.g., scoping of the risk analysis according to the amount of time that the technicians have to devote to it) should be avoided. As mentioned above, everyone involved must participate in the risk analysis process.

For the sites concerned, this may result in a modification of the safety management system to take into account the lessons learnt from the incident: ARIA 35841.

Finally, in very general terms, certain accidents involving one or more actuators have made it possible to highlight actions to improve the organisation of work or communication:

- ✓ Improved communication between line managers and shift managers to provide the next shift with a comprehensive review of the problems encountered: ARIA 46230;
- ✓ Establishment of an additional and direct link between the operations office and the arriving ships by purchasing ATEX-compliant mobile telephones: ARIA 34205;
- ✓ Establishment of an instructions transmission sheet and a logbook: ARIA 42644...

Although not exclusive to actuators but still relevant, new risks must also be into taken into account, such as:

- ✓ Preventive monitoring of the ageing of installations: ARIA 36722, 41516;
- ✓ Cybersecurity: in response to the emergence of remote programming and control (e.g., ARIA 51131), the right questions need to be asked. Some thinking has been done regarding sensors and PLCs, which is also applicable to actuators. See the report on Cybersecurity in industry;
- ✓ Malicious intent targeting utilities;
- ✓ The development of new actuator technologies.

Lessons learnt (conclusion)

Following the analysis of the 326 accidents considered in the study, certain lessons can be drawn to avoid accidents meeting at least one of the following 3 criteria:

- ✓ One or more actuators were responsible for the accident;
- ✓ One or more actuators exacerbated the accident (by not operating or, more rarely, by operating);
- ✓ The absence of one or more actuators caused or exacerbated an accident (if this absence is explicitly mentioned in the accident analysis and its installation was foreseen in the technical follow-up to the accident).

For the first two points, hardware disruptions can be avoided by paying closer attention to the design of systems, their suitability for the process (location, material used, etc.) and their maintainability over time. All departments within an organisation must be mobilized to ensure the reliability of industrial automation processes.

For the third point, the study found that some accidents could have been prevented if an automatic actuator had been installed in the appropriate location. If they perform their function correctly, automatic actuators can correct a system deviation. When such a deviation can result in damage, such systems can ensure that installations remain safe. Their installation and use must, therefore, be studied as soon as possible while maintaining the technicians' understanding and control of the installations. The requirements for systems performing a safety-related function must be in keeping with the equipment that they are designed to protect. The certifications of human and technical barriers may be considered essential if they are a key element of the hazard studies used to develop population protection plans and/or land-use regulations.

Also, in order to take in-depth action on the causes of accidents, managerial organisations must be committed to providing the means required and to establishing the priorities of action. The mere modification of equipment or human behaviour is not enough. The management of organisational and human factors as a whole must be based on a safety-focused organisation, taking priority over economic constraints. The accidents studied also highlight the economic losses associated with events in which one or more actuators are involved. We should be thinking outside the box when it comes to processes as a whole, especially in a context where automation is increasingly prevalent and designed to reduce human constraints. We must bear in mind that man remains an ultimate barrier, and sometimes, a means to correct problems. The necessary skill sets must evolve with technology. Knowledge of the operational environment and its risks must remain at the top of decision-makers' concerns.

Reporting and sharing of feedback are also the core elements of prevention-related actions. The dissemination and exchange of good practices is an important factor in improving industrial safety. The new technologies must be mastered collectively so as not to lose sight of human accountability in their design, operation, maintenance, dismantling, etc.

The three aspects studied in the context of industrial automation accidentology have allowed us to highlight a certain number of recommendations for each of the functions, taken separately. It would appear logical that these systems should be studied as a whole to ensure that they operate in the best possible conditions.

The summaries of all events presented here are available on the following website:

www.aria.developpement-durable.gouv.fr

To submit a comment or suggestion, to report an accident or to obtain permission to use this data for publication purposes:

barpi@developpement-durable.gouv.fr

BARPI (Bureau for Analysis of Industrial Risks and Pollutions)

5 place Jules Ferry
69006 Lyon
France

Telephone: (+33) (0)4 26 28 62 00

Department for Technological Risks
General Department of Risk Prevention
Ministry for an Ecological Transition

Tour Sequoia
92055 La Défense Cedex
France

Telephone: (+33) (0)1 40 81 21 22

MINISTÈRE
DE LA TRANSITION
ÉCOLOGIQUE

Liberté
Égalité
Fraternité

TECHNOLOGICAL ACCIDENT SUMMARIES ONLINE

Safety and transparency are two legitimate demands being imposed by society. In response, since June 2001, the Ministry for an Ecological Transition has made www.aria.developpement-durable.gouv.fr available to professionals and the general public, presenting the many lessons drawn from analyses of technological accidents. The main headings of the website are presented in both French and English. Users may, for example, obtain information on governmental actions, consult large excerpts from the ARIA database, find out about industrial accidents at the European level, and check the index of hazardous substances to round out the information provided in news bulletins and announcements in the wake of accidents or incidents.

The description of accidents, as the raw material of any feedback-driven approach, makes up a significant portion of the site's resources: the stages and consequences of an event, its origins, circumstances, identified or assumed causes, actions taken and lessons learnt.

Some 100 detailed and illustrated technical datasheets present a selection of accidents offering pertinent lessons. Many analyses by accident typology or industrial sector are also available. The heading devoted to technical recommendations is divided into various topics, e.g.: fine chemicals, pyrotechnics, surface treatments, silos, tyre warehouses, fire permits, waste processing, and material handling.

A multi-criteria search engine can be used to find information on accidents that occurred in France or abroad.

The site www.aria.developpement-durable.gouv.fr is continually expanded.

There are currently about 50,000 accident reports available online, and new thematic analyses are regularly added.