An extensive method to analyze impacts of cyber-security on major hazards

François Masse

An extensive method to analyze impacts of cyber-security on major hazards

Massé F[1]

[1] Institut national de l'environnement industriel et des risques (INERIS) – Parc Technologique Alata – BP 2 – F-60550 Verneuil-en-Halatte – France

francois.masse@ineris.fr

KEYWORDS: Cyberphysical, Major Hazards, process Industry, risk analysis

ABSTRACT

Operators of industrial facilities must be able to control the risks that their installations pose to people or environment. To demonstrate this, they identify the major accident scenarios through preliminary and detailed risk analysis steps, then evaluate the performance of the risk control measures, and finally, risk acceptability in terms of likelihood and severity. The risk analysis methods used are adapted to evaluate accidental events.

Industrial control systems (ICS) include control systems, safety instrumented systems and communication systems. They tend to be increasingly interconnected with the company's information systems and to use technologies derived from IT. They are therefore more vulnerable to cyber-attacks which can potentially generate major hazards for people and the environment. A cyber-attack can be targeted or not, can be internal or external to the targeted industrial site and the means of carrying out future attacks are potentially new and unknown.

INERIS seeks to evaluate the impact of cyber-attacks on ICS in the process industry and particularly the possibility for the attacker to provoke dangerous effects for populations and environment. The approach should be focused on physical effects rather than on ICS vulnerabilities. A first approach, ATBT, consisted to link attack trees and bowtie diagrams (ESREL 2017, Computer and Security 2017). This allows to evaluate the likelihood of accidental and malicious causes of major hazards. This first approach relies on bowtie diagrams developed to assess accidental risks which are not exhaustive for attack scenarios. In this paper, we propose an approach to complete the identification of attack scenarios during the preliminary risk analysis. The aim of this methodology is to bridge the risk analysis related to cyber-attacks of IT and OT systems and risk analysis.

1 INTRODUCTION

The vulnerabilities of industrial control systems (ICS) and safety instrumented systems (SIS) constitute a threat to the safety of industrial installations. These systems may be vulnerable either to targeted malicious attacks or to different types of non-targeted attacks to which open systems on the Internet are exposed (viruses, ransomware, etc.). The convergence between industrial automation technologies (OT) and computer technologies (IT), the use of wireless networks, the interconnection between OT and IT (including office systems and Internet connections) are examples of vulnerabilities that can affect industrial control systems.

Various surveys show the exponential increase in incidents involving industrial systems. These attacks by revengeful employees, criminal organizations, etc. are common but are mainly aimed at stopping or damaging facilities, fraud or extortion. However, the methods used to carry out these attacks can be used to corrupt industrial control systems in such a way as to cause dangerous phenomena for the safety of operators, residents or the environment. These attacks are likely, in the same way as random failures, to cause major accidents. It is therefore necessary to assess and limit the impact of cybersecurity on the control of accidental risks.

The simultaneous handling of these two subjects is complex: the cultures of these two fields are different, the areas of analysis overlap partially (physical process and control command on the one hand, control command system and information systems on the other) but conflicting requirements can therefore emerge from the two analyses.
Various methodological frameworks have been proposed to address both functional safety and cybersecurity or industrial risk management and cybersecurity (SESAMO project, CORAS method). These are mainly methods focusing on the analysis of the control command system and its deviation but don't include the physical risks related to the chemical process.

2 PRESENTATION OF TWO FRAMEWORKS: INDUSTRIAL RISK AND CYBERSECURITY

2.1 Industrial Risks Management in French regulatory Context

2.1.1 Overall Framework

In the French regulatory context, any industrial installation likely to create risks or cause pollution or nuisances, for the safety and health of residents, is a Classified Installation (CI). Different regimes are defined for classified installations, depending on the importance of the risks. The installations presenting the greatest risks – according to the nomenclature of classified installations which sets thresholds according to the substances used or stored on the site and the type of activity - are subject to the authorization regime. For these installations, the operator must apply for an operating permit demonstrating that the risks are under control; the application must be accepted by the authorities before the installation is put into operation.

To demonstrate the acceptability of risks, the operator of a CI carries out a Hazard Study which identifies all hazardous phenomena and major accidents related to the installation that may have effects outside the site, assesses their intensity and severity (distance of effect and number of potentially exposed persons) and their probability of occurrence. The assessment of probability in Hazard Study was introduced in the environmental code by the law of 30 July 2003. Probabilities and severity are estimated according to scales defined in Annex 1 of the Ministerial Order of 29 September 2005. The gravity / probability pair makes it possible to locate the various accidents identified in an acceptability matrix and thus to assess the control of major accident risks for the establishment in question.
The approach used to assess risks in hazard studies follows three main steps:

- a qualitative risk analysis to identify all scenarios and select dangerous phenomena with potential effects outside the site;
- a detailed risk study to quantify these risks in probability and severity;
- risk control measures necessary to keep the risk at an acceptable level are identified and evaluated.

2.1.2 Step 1: qualitative risk analysis

For qualitative analysis, an approach such as Preliminary Hazard Analysis (PHA) or Hazard Operability Analysis (HAZOP) is generally used to identify risks in a systematic way.

Thus, HAZOP is a systematic analysis approach aimed at identifying the risks associated with a process. HAZOP is conducted by a multidisciplinary working group that identifies potential deviations from the physical parameters of the process and identifies their possible causes and consequences for the safety of people, the environment or assets. To facilitate the review, a system is divided into several parts (or nodes) for which the elementary functions can be defined. For each node, the HAZOP study team checks whether each property (PRESSURE, FLOW...) has a deviation that may have undesirable consequences. To identify these deviation, a system of questions with predefined guide words (DO NOT DO, MORE, LESS, REVERSE...) is used. For example, the working group examines the PRESSURE PLUS deviation in the "chemical reactor filling system" node, which includes piping, pumps, valves and instrumentation. It will be tried to determine the causes of this deviation (closing a valve downstream of a compressor), the consequences (bursting of the piping and loss of containment of a flammable substance) and the possible risk control measures (safety function on high pressure, limit switches on the valves, valve...).

Carrying out an HAZOP is a creative process that aims to systematically reviews the random and accidental deviation of a process. It is not intended to analyze several simultaneous deviations. It could be used to consider malicious causes of certain deviations (illegitimate control of the valve downstream of a compressor via the control command PLC, deactivation of the instrumented functions of high pressure safety and valve limit switch). However, the HAZOP format as it is used is not designed for this objective.

Once the main Hazardous Events are identified through PHA or HAZOP, their severity and probability are evaluated through a detailed risk analysis and necessary risk reduction measures are defined. The detailed analysis can be supported and synthetized through method like Bow-Tie diagram.

2.2 Cybersecurity of industrial systems in the French context

In France, regulatory requirements have been applicable to Vital Importance Operators (OIVs) since the last quarter of 2016 through specific decrees based on guides developed by Working Groups on Cybersecurity of

Industrial Installations led by ANSSI (Agence Nationale de Sécurité des Systèmes d'Information) which have published 2 documents: "Classification method and main measures" and "detailed measures". These guides define a three-step approach, similar to the approach of the hazard study, that can be applied to any industrial system, OIV or not:

- identification of critical information systems based on a qualitative approach;
- detailed risk analysis for these information systems;
- definition of the security measures applicable to these systems.

These steps are covered by most of risk management methods for information system security.

ANSSI guides focus on assessing the likelihood of attacks. This is the estimate of the likelihood of a threat scenario or risk occurring. It is estimated according to the technologies and functionalities of the systems, their connectivity, the management of the stakeholders and the level of potential attackers. For the assessment of severity, the guide simply presents severity scales for human and environmental impacts and for impacts following the cessation of the service provided (economic impacts). The means of accurately assessing the impacts of an attack and situating them on these scales are not presented in the guide.
The EBIOS method, mainly in use in France, is an example of cyber risk analysis method that can be used to identify and evaluate critical information systems.

2.3 A general risk analysis framework

We are seeking to define a methodology for analyzing major risks for people and environment that integrates cyber-attacks as initiating events. This methodology has to makes it possible to:

1. Identify risks: list physical risks to people and environment as comprehensively as possible and rate them in terms of severity
2. Analyze risks: identify attack scenarios leading to the identified risks and rate them in probability or likelihood
3. Assess risks: conclude on the acceptability of the risk, by evaluating the different risk reduction measures and placing the scenarios on a multifactorial acceptability matrix and set requirements for additional or improved risks reduction measures.

This methodology has to apply to industrial processes and their control systems and be, as far as possible, consistent with the general risk analysis framework used for classified installations. Unlike risk analyses conducted for industrial systems, which use experience data as well as past accident analyses to predict the possible causes and frequencies of future accidents, cyberattack risk analyses require considering operating procedures that have never been observed. Indeed, several difficulties arise in the development of the method:

- the type of attackers and their motivations are variable;
- the means of attack are not known: it is not known in advance which systems are most likely to be attacked and the attack procedures are evolving in time;
- the attackers will seek - to the extent of their competence - to bypass existing security;
- evaluating the probability of an attack doesn't really make sense;
- the complexity of the system makes it difficult to analyze exhaustive attack scenarios.

INERIS has therefor developed an analysis methodology focused on targets: knowing the potential effect that can be achieved by attackers, the systems involved (actuators, sensors, controllers) and the physical behaviors of these systems that the attacker will seek to obtain to achieve these objectives will be identified, without evaluating at this step the means of attack used, vulnerabilities exploited and likelihood of the attack. The detailed analysis of the cyber-physical scenarios. The detailed analysis of the scenarios will then focus on their severity, probability for accidental causes and likelihood for cyber causes. To this end, the scenarios will be analyzed by the accident risk analysis teams on the one hand and the cyber risk analysis teams on the other.

Such an analysis requires skills on physical processes and associated risks and also specific skills on cybersecurity control that are not generally integrated into the working groups carrying out HAZOP or PHA. The methodological framework will therefore involve different working groups in the different phases of analysis:

- the working group in charge of evaluating the physical risks of the process, which is also responsible for HAZOP or PHA analyses;
- the working group in charge of the analysis of cybersecurity of the industrial control system.

The Figure 1 below shows the interactions between physical and cyber risk analysis processes. Different information must be exchanged between the two working groups:
(1) The Working Group on Physical Hazards will identify scenarios and low-level elements of the CIM pyramid which may cause damage to people or the environment. These output data will be provided to the working group

responsible for evaluating the cybersecurity of the industrial system and will be integrated into their analyses as undesirable events. This working group will then identify the attack scenarios, the different IT and OT systems involved, the existing or necessary security measures and the level of residual risk (likelihood of the attack). This working group will therefore apply the cyber risk analysis method generally used by the organization to major risk scenarios for people and the environment (e.g. EBIOS method).
(2) The likelihood of the attack will then be integrated into a bow tie model integrating random and malicious causes.
(3) Finally, the requirements on risk control measures and safety measures to achieve an acceptable level of risk will be specified and implemented.

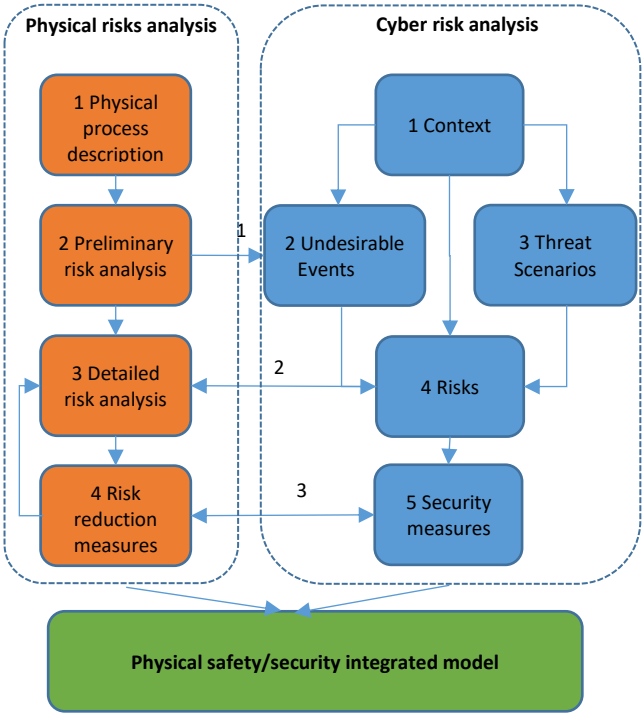

***Figure 1**. Interactions between accidental and cyber risk analysis.*

The cyber risk analysis process is like the EBIOS method presented above with a focus on the undesirable events resulting from the physical risk analysis. It is therefore not presented in more detail in this article.
The consideration of cybersecurity events in the various stages of physical risk analysis is presented below.

3 IMPLEMENTATIONS OF THE METHOD FOR SCENARIOS IDENTIFICATION

This section presents the method developed for preliminary cyber risk analysis. The objective of this preliminary analysis is to identify cyber risk scenarios that will be evaluated during the detailed analysis.

3.1 Motivation, challenges and objectives of the method

The integration of cyber-attacks as major accident initiating events in risk analyses is not obvious: indeed, multiple attack paths on very different systems can be at the origin of the feared scenarios. In addition, an attack scenario can rely on the corruption of several systems simultaneously.

The realization of an inductive analysis, like a FMECA, starting from the different possible types of corruption of each equipment of the industrial control system and identifying their consequences as well as the consequences of the combination of concomitant corruptions of several devices is unrealistic: the programmable devices can be numerous, the modes of corruption varied (unavailability (following a detected anomaly, corruption or data destruction), modification of thresholds, corruption of orders, modification of variables or measured values, modification of sequences of operations, modification of application software).
A deductive approach, based on undesirable events to identify possible malicious causes, is therefore preferred. The aim is to enrich the creative process, as organized by the PHA and HAZOP methods, by adding the search for malicious causes. To do this, the working group performing the accidental analysis will need a description of the different level 0 and 1 control command systems of the CIM pyramid in interaction with the studied process. When

searching for the causes of the various deviations (for HAZOP) or the various feared events (for PHA), it will be necessary to identify data corruption, changes in instructions or control logic or untimely actions by actuators that could lead to these events.

In the context of Hazard Studies of chemical processes, Undesirable Events are defined as the uncontrolled loss of containment of a product (generally liquid or gas). The loss of containment itself can be the source of dangerous phenomena in some cases (explosion, fire, dispersion of toxic substances), in other cases secondary events (e.g. ignition of an explosive gas cloud) may be necessary.

3.2 Typology of hostile actions and first identification of scenarios

We therefore seek to identify for each product present on the site the possible conditions of a loss of containment that could cause a dangerous phenomenon that could affect people or the environment. The conditions for achieving containment losses are of different kinds:

- A: modification of physical parameters (pressure, temperature, flow rate...) by controlling valves, compressors, heating and cooling systems;
- B: dispersion of dangerous substance by overflowing a capacity or opening of emptying devices;
- C: contact of products reacting in a dangerous way;
- D: shutdown of a continuously operating system that maintain the process in a safe state (ventilation, suction, inerting);
- E: modification of the operating sequences (quantities of substances, duration of the different phases, order of operations)

A first identification of these scenarios is made by exploiting the existing PHA made for accidental events. In this PHA it is possible to identify basic events that can be provoked by cyber-attacks and Safety Instrumented functions that can be compromised.

This first identification of scenarios is not sufficient: PHA, as HAZOP, deals with scenarios due to the deviation of a single parameter or the failure of a single equipment or function. The cyber-attacks scenarios should include scenarios due to the modification of several parameters and the simultaneous corruption of several equipment. This is the purpose of the cyber-PHA.
In this approach, following the description of the context and of the dangerous substance on the process, some possible physical attack scenario will be identified. The identification of the scenario will be realized in working group and will be guided by the typology of sources of loss of containment listed above plus to other possible types of attacks:

- F: shutdown or reset of one or several PLC during each phase of operation (with consequences on the position of each actuators);
- G: Modification or disabling of a Safety Instrumented Function (SIF).

3.3 The Cyber-PHA methodology

The cyber-PHA model follows a systematic approach to identify which phenomena are critical, whether there are means to cause these phenomena and whether there are means to detect them or security barriers that will avoid the consequences. The proposed approach is as follows:

3.3.1 Preliminary phase

In this preliminary phase, the description of the installation used for the conventional PHA will be completed by a description of the industrial control system. The industrial process is divided in nodes and for each node, the following elements are described:

01- Identification of the different phase of operation;
02- Identification of the dangerous substances involved in this node;
03- Identification of the physical parameters
04- Identification of low level control command control equipment (sensors, PLCs and actuators) acting on this node.

3.3.2 Cyber Physical Scenarios identification

The cyber physical scenarios will be conducted on each node considering their different phase of operations. The different types of scenarios will be reviewed:

- A: Scenarios related to the variation of physical parameters, for each substance:
    - o A1- identification of critical physical parameters;

    - o A2- identification of the existence of control means to exceed these parameters;
- B: Scenarios related to the dispersal or spreading of dangerous substance, for each substance:
    - o B1- Identification of risks related to malicious spreading;
    - o B2- identification of the means (actuators) to carry out this spreading;
- C: Risk related of incompatible mixtures:
    - o C1- Realization of an incompatibility matrix to identify potentially dangerous mixtures;
    - o C2- identification of the means (actuators) to make substance into contact;
- D: Risks related to the corruption of systems maintaining the installation in a safe state:
    - o D1- Identification of these systems (pressure regulation, inerting, temperature regulation);
    - o D2- Analysis of consequence of their disabling or modification of setting points;
- E: Risks related to the modification of the sequence of operations:
    - o E1- Identification of the normal operations sequences;
    - o E2- Analysis of consequence of sequence modification;

F: Risks related to the shutdown or reset of a logic controller:
- o F1- Identification of logic controller acting on the node;
- o F2- Analysis of consequence of reset or shutdown of the controller during each phase of operation;

F: Risks related to the shutdown or reset of a logic controller:
- o F1- Identification of logic controller acting on the node;
- o F2- Analysis of consequence of reset or shutdown of the controller during each phase of operation;

G: Risks related to the disabling or modification of safety instrumented function (SIF):
- o G1- Identification of SIF acting on the node and condition of activation;
- o G2- Analysis of consequence of disabling or modification considering the frequency of their solicitations;
- o G3- Analysis of the consequences of spurious operation of SIF.

Theses seven types of physical attacks can be combined. For each node, the working group will define the possible dangerous events, the combination of illegitimate action that can provoke them and the instrumentation and control systems involved in this attack.
For each attack scenario, the detection means and safety barriers and their vulnerability to cyber-attacks will be identified. Some of the measures identified may be not programmable (e.g. valve) and not targeted by cyberattacks. The working group will also evaluate the possibility to provoke several similar dangerous events simultaneously, for example, fire of several hydrocarbon storage
This will give a description of cyber-physical scenarios which will be studied in detail in the detailed risk study carried on by the cyber risk analysis in one hand and the accidental risk analysis on the other hand. The detailed risk analysis will the be merged in an ATBT model as describe in [2].

4 CONCLUSION

The proposed methodology enables integrate cyber security into physical risk analyses and to complete scenarios leading to dangerous effects for people or the environment. Following the identification of the scenarios, a detailed study of the likelihood (malicious attacks), probability (accidental events) and severity can be carried out for each of them. This approach helps to identify critical systems for which protection, monitoring and maintenance procedures are necessary, to set up attack detection systems, or to implement non-programmable security barriers that act on both the physical effects of attacks and accidental phenomena.

5 REFERENCES

1. Abdo H., Flaus J.M., Masse F., *Towards a better industrial risk analysis: A new approach that combines cyber security within safety.* In Safety and Reliability Theory and Applications: Proceedings of ESREL (Portoroz, Slovenia), pages 179–187, 2017.
2. Abdo H., Flaus J.M., Masse F.,*A safety/security risk analysis approach of Industrial Control Systems: A cyber bowtie - combining new version of attack tree with bowtie analysis*, In Computers & Security, Volume 72, 2018, Pages 175-195, ISSN 0167-4048.
3. Kriaa S., Pietre-Cambacedes L., Bouissou M., Halgand Y., *A survey of approaches combining safety and security for industrial control systems*, In Reliability Engineering & System Safety, Volume 139, 2015
4. Masse F., Abdo H., Flaus J.M., Vers une approche intégrant les exigences de cybersécurité à la maîtrise des risques d'accidents majeurs pour les ICPE). In 12ème Congrès International Pluridisciplinaire en Qualité, Sûreté de fonctionnement et Développement durable, Bourges, France 2017