Process Safety and Environmental Protection 172 (2023) 69–82

Contents lists available at ScienceDirect

Process Safety and Environmental Protection

journal homepage: www.journals.elsevier.com/process-safety-and-environmental-protection

Identification of cyber-risks for the control and safety instrumented systems: a synergic framework for the process industry

Matteo Iaiani, Alessandro Tugnoli *, Valerio Cozzani

LISES - Department of Civil, Chemical, Environmental, and Materials Engineering, Alma Mater Studiorum - University of Bologna, via Terracini n. 28, 40131 Bologna, Italy

ARTICLE INFO

Keywords:
Cybersecurity
Cyber-risk identification
Chemical and process industry
Major accident hazard
Operability
Systematic methodology

ABSTRACT

Malicious interferences to Industrial Automation and Control Systems (IACS) such as the Basic Process Control System (BPCS) and the Safety Instrumented System (SIS) of chemical and process facilities may initiate events with severe consequences such as major accident scenarios (e.g., loss of containment of hazardous substances) and production outages. Existing security vulnerability and risk assessment (SVA/SRA) methodologies, as well as the cybersecurity risk assessment approach proposed by ISA/IEC 62443 series of standards, do not provide any practical method or guideline supporting cyber-risk identification. Moreover, an evident lack of procedures addressing the concrete connection between malicious manipulations of the BPCS and SIS and the impacts on the physical process system that can be initiated, is present in the scientific literature. Given the outlined gap, in the present study, a synergic framework of tools is described and applied to a case study (offshore Oil&Gas platform for gas compression), supporting the systematic identification of the risks that can originate as a result of a malicious interference to the BPCS and SIS. The framework consists of a past incident analysis (PIA) and of two rigorous methodologies, PHAROS, focused on major accident hazards, and POROS, addressing also operability issues. The concept of cyber-attack credibility is here introduced to identify the most credible sets of manipulations based on the score of the plant knowledge level required by the attacker and that of the cyber complexity of the attack pattern, allowing to provide valuable information on how to effectively allocate resources for a more secure network architecture.

1. Introduction

Malicious interferences to Industrial Automation and Control Systems (IACS) such as the Basic Process Control System (BPCS) and the Safety Instrumented System (SIS) of chemical and process facilities, are becoming a growing concern (Center for Chemical Process Safety, 2022; Iaiani et al., 2021a). In fact, the Chemical and Process Industry (CPI) is currently undergoing a digital transition towards higher levels of automation and of interconnection with external networks (Faramondi and Setola, 2019; Khan et al., 2021; Kopbayev et al., 2022) that, while ensuring advantages thanks to the possibility to analyse a huge amount of data coming from industrial processes (e.g., reduction of total machine downtime due to predictive maintenance and remote monitoring), make CPI facilities more vulnerable to cyber-attacks (Reniers, 2011; Stouffer et al., 2008; Thomas and Day, 2015). Moreover, recently many companies have changed the way they operate as a result of the COVID-19 pandemic (e.g., a high percentage of workers operate remotely), making cybersecurity processes more stressed (Cozzani and Yang, 2022; Kaspersky and ARC Advisory Group, 2020).

Cyber-attacks are interferences to the IT (Information Technology) - OT (Operational Technology) network of the facility which may have impacts to the physical process system (see Fig. 1). The IT system includes all the hardware and software dedicated to store, retrieve, transmit, and manipulate data or information (Paulsen and Byers, 2019): the corporate network and a local network are typically within the IT system. The latter is connected to the OT system which includes all the hardware and software dedicated to detecting or causing changes in physical processes through direct monitoring and/or control of physical devices such as valves, pumps, compressors, etc. (see Fig. 1): for example, the BPCS and SIS are part of the OT system. The physical process system is, instead, the part of the architecture which is composed by the process equipment and pipework, whose operation is governed by the OT system, thus allowing attackers that are able to access the BPCS and/or SIS, to tamper with them remotely. On the

* Corresponding author.
E-mail address: a.tugnoli@unibo.it (A. Tugnoli).

https://doi.org/10.1016/j.psep.2023.01.078
Received 1 December 2022; Received in revised form 30 January 2023; Accepted 31 January 2023
Available online 2 February 2023

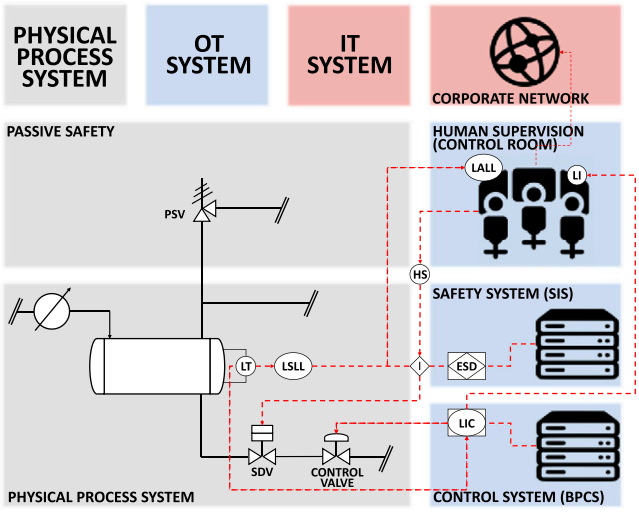

Fig. 1. Typical structure of the IT-OT network system and the physical process system in the CPI.

contrary, passive safety elements such as PSVs, are not controlled by the OT system, and thus can not be manipulated through cyber-attacks, resulting to play a key role in the prevention or mitigation of this type of attacks.

Historical evidence shows that cyber-attacks targeting CPI facilities can cause events with severe consequences on people, property, and/or the surrounding environment (Iaiani et al., 2021a; Landucci and Reniers, 2019), which, in case of lifelines and critical infrastructures (e.g., natural gas interconnectors, oil refineries), may undermine the national/local system resilience (Sun et al., 2022; Zinetullina et al., 2021). For example, in 2008 cyber criminals over-pressurized remotely the Turkish section of the BTC (Baku-Tbilisi-Ceyan) pipeline by manipulating the control and safety systems managing the pipeline. As a result, an explosion occurred, causing the release of more than 30,000 barrels of oil in an area above a water aquifer, a fire lasting more than two days, and economic losses due to the production outage of about $5 million a day (Lee et al., 2014; ARIA database, 2022). Another relevant and more recent example is the well-known ransomware attack to Colonial Pipeline that occurred on May 7th, 2021 in USA (Bing and Kelly S, 2021). In that case, attackers were able to access the CP billing system and stealing 100 GB of sensitive data (Robertson and Turton, 2021): the operators, in order to contrast the spreading of the intrusion and avoid the attacker to access the OT system, forced the pipeline to shutdown causing huge economic losses due to 6-days production outage, together with fuel shortages to refineries, airports, filling stations, etc.

In this panorama, Thomas and Day (2015) argue that cybersecurity issues can no longer be disregarded in industrial facilities processing and/or storing relevant quantities of hazardous materials, stressing the urgency of structured methodologies aimed at the evaluation of the risks that can result in the physical process system as a consequence of malicious manipulations of the OT system (see Fig. 1). Moreover, Ylönen et al. (2022) added that these methodological frameworks shall address the potential synergies with safety for a more integrated management of all the risks that a facility might face.

Regarding this issue, while the classical Security Vulnerability/Risk Assessment (SVA/SRA) methodologies (e.g., CCPS methodology (Center of Chemical Process Safety, 2003), API RP 780 methodology (American Petroleum Institute, 2013), etc.) do not provide specific support on cyber threats (Matteini et al., 2019), the ISA/IEC 62443 series of standards propose a detailed cybersecurity risk assessment (CRA) procedure (see the flowchart in Fig. 2) for IACSs. However, it lacks in providing approaches with a clear methodological framework for the evaluation of the impacts that can result from the manipulation of the BPCS and SIS (the OT system, see Fig. 1) such as the loss of containment of hazardous material and business interruption due to production outage. To this aim, the Center for Chemical Process Safety (CCPS) (Center for Chemical Process Safety, 2022) has proposed the Cyber HazOp, the Cyber-FMEA, the Threat Analysis, the Checklist, and the Bow-Tie approach as suitable qualitative and quantitative methods for cyber-risk identification and evaluation in chemical and process facilities, without providing, however, detailed information on how to perform such analyses. In the scientific literature, only few contributions make use of these methods to address the security of OT systems in facilities handling relevant quantities of hazardous materials. However, these studies present limitations concerning systematicity, reproducibility, and scope, as discussed in Section A of the Supplementary Material.

Previous works by the Authors (Iaiani et al., 2021b, 2021c) proposed systematic HazOp-like analysis procedures of the physical process system and OT system aimed at identifying all the possible combinations of manipulations with are relevant for risk assessment, i.e., that may lead to major accident scenarios and/or production outages. However, the integration of such methodologies with other components of the cyber risk assessments, in particular in terms of inclusion of lessons learned from past events and ranking of the credibility of the identified cybersecurity scenarios, was only in part analysed (Iaiani et al., 2022).

In this context, the present study in Section 2 describes a framework of synergic methods that were developed to support cyber-risk identification in existing methodologies (e.g., SVA/SRA methodologies, cyber-risk assessment proposed by ISA/IEC 62443 series of standards), allowing to fill the gap in the availability of systematic operating procedures for security assessment of the link between malicious manipulations of the BPCS and SIS and the impacts on the physical process system that can be initiated. In particular, these method address (see marked steps with star symbols in the ISA/IEC 62443 workflow shown in Fig. 2): i) the identification of potential threats; ii) the evaluation of the process-related impacts that can be generated through the manipulation of the OT system and their consequences; iii) the determination of unmitigated likelihood; and iv) the identification of possible effective countermeasures. In order to demonstrate the quality of the results that can be achieved, the developed methods are applied to an illustrative case study addressing a fixed offshore Oil&Gas platform (Section 3). The results obtained are discussed in Section 4 and conclusions are drawn in Section 5.

2. Framework for cyber-risk identification

This contribution proposes a synergic framework for the chemical and process industry aimed at supporting cyber-risk identification in existing SVA/SRA approaches, including the cyber-risk assessment method proposed by ISA/IEC 62443 series of standards (see Fig. 2). The framework is composed by a past incident analysis (PIA) through which knowledge and lessons learnt from the past events were gathered, and of two systematic methodologies, PHAROS (Process Hazard Analysis of Remote manipulations through the cOntrol System), aimed at the identification of major accident scenarios that can be caused by the remote manipulation of the BPCS and SIS, and POROS (Process Operability Analysis of Remote manipulations through the cOntrol System), which addresses mostly operability issues, allowing for the identification of the production outage scenarios that can be triggered by malicious manipulation of the OT system. A preliminary study on the synergic utilization of the above-mentioned methods is reported in Iaiani et al. (2022).

The results obtained from PIA can be used for the definition of possible (supported by historical evidence) generic cybersecurity scenarios to be used as a reference to undertake a subsequent case-specific cyber-risk identification with PHAROS and POROS methodologies, allowing to define the specific link between malicious manipulation of the BPCS and SIS of system under assessment and the major accident and production outage scenarios that can be caused.

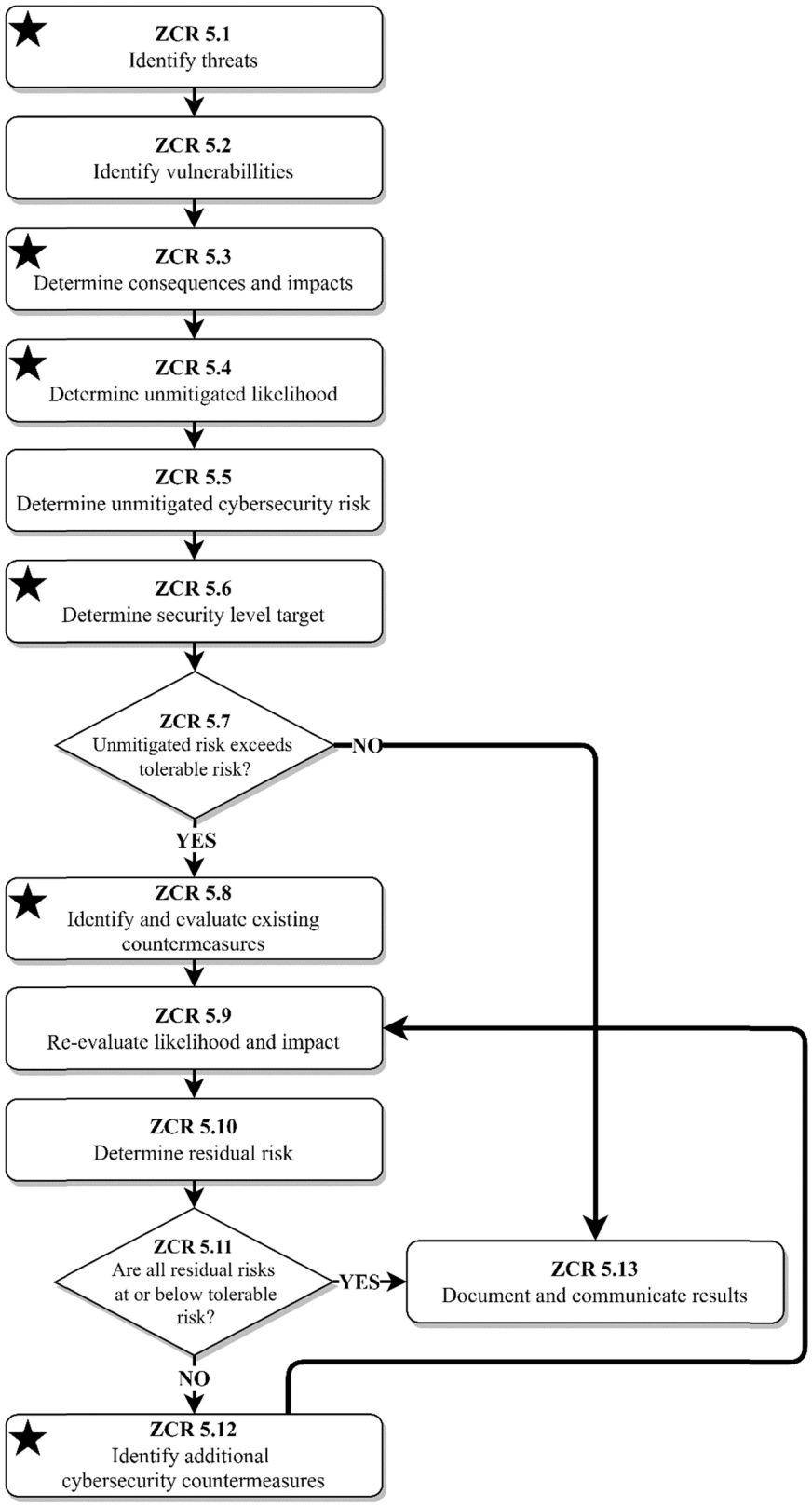

Fig. 2. Flowchart of the detailed cybersecurity risk assessment (CRA) workflow of ISA/IEC 62443 series of standards. Steps marked with star symbols are the ones to which support is provided by the proposed framework.

Unlike in previous works (Iaiani et al., 2021a, 2021b, 2021c) in which these three tools were described and applied independently, in the present study they are presented in a synergic way, showing how the results of PIA can be better investigated and defined in terms of required sets of manipulations of the BPCS and SIS through PHAROS and POROS methodologies. Moreover, the novel concepts of the required plant knowledge level of the attacker and of cyber complexity of the identified combination of manipulations, are here introduced in the two

methodologies in order to semi-quantitatively estimate the credibility of each possible set of manipulations being performed by an attacker. This provides important information in the context of the effective allocation of resources for a more secure and resilient OT system against cyber-attacks aimed at interfering with normal operations.

2.1. Past incident analysis (PIA)

A total of 82 cybersecurity-related incidents were collected and analysed. Each entry in the database is compliant with two inclusion criteria:

1. the incident shall originate from an accidental or intentional interference to the IT-OT network system of the affected facility;
2. the incident shall involve a facility of interest (chemical and process industry and similar sectors).

The structured analysis of the developed database was performed using Exploratory Data Analysis (EDA) (Tukey, 1977). Application of EDA allowed to develop knowledge and lessons learnt from the past incidents, obtaining valuable information to support application of existing methodologies addressing cybersecurity issues (see Fig. 3). In fact, most of the SVA/SRA methods specifically propose PIA as a possible approach for this purpose (American Petroleum Institute, 2013; Center of Chemical Process Safety, 2003): however, given the limited data and the extremely variable nature of the systems that can be compromised by cyber-attacks, approaches based on systems specific information are needed. For this reason, the results obtained from PIA can be used as basis for the definition of generic cybersecurity-related scenarios to be employed by authorities and practitioners as a reference to undertake a subsequent case-specific cyber-risk assessment.

Fig. 3 graphically summarizes the results obtained from EDA application and their potential use in the context of cyber-risk identification (CRA). The results concern the types of attackers and possible attack paths within the IT-OT network, the potential impacts of cyber-attacks, and the effective cybersecurity countermeasures in preventing a cyber-attack. Support is provided, e.g., to the steps ZCR 5.1 “identify threats”, ZCR 5.3 “determine consequences and impacts”, ZCR 5.8 “identify and evaluate existing countermeasures”, and ZCR 5.12 “identify additional cybersecurity countermeasures” of the CRA proposed by the ISA/IEC 62443 series of standards. Further details are reported elsewhere (Iaiani et al., 2021b).

2.2. PHAROS and POROS methodologies

The outputs of the PHAROS and POROS methodologies consist in the identification of the list of possible security events that may be caused by the malicious manipulation of the BPCS and SIS (major event scenarios in case of PHAROS, production outage scenarios in case of POROS), the sets of the BPCS and SIS components that need to be manipulated, the related sets of manipulations, as well as the inherent/passive (IPS) and active/procedural (APS) safeguards in place that may block the cyber-attack (see Fig. 4).

Therefore, PHAROS and POROS methodologies support the case-specific identification of the cyber-risks as required by the CRA procedure proposed by the ISA/IEC 62443 series of standards. In particular, support is provided to steps ZCR 5.3 “determine consequences and impacts”, ZCR 5.4 “determine unmitigated likelihood”, ZCR 5.6 “determine security level target”, and ZCR 5.12 “identify additional cybersecurity countermeasures” (see Figs. 2 and 4). Also the methods developed Hashimoto et al. (2013), Gertman et al. (2006), Cusimano and Rostick (2018), as well as that proposed by the German DIN VDE V 0831-104 (2015) (see Section A of the Supplementary Material) can benefit from the outputs of PHAROS and POROS methodologies.

Fig. 5**-a** shows the flowchart of PHAROS methodology, while Fig. 5**-b** the one of POROS methodology. They consist in 9 main steps each, which are meant to be applied by a team that includes a team leader, a secretary, a project engineer, a process design engineer, an instrumentation and control engineer, and a safety engineer. Due to the initial assumption to consider that the attacker has gained full access to the OT system (see Fig. 1) of the targeted facility, only generic IT skills are required in the team.

For the sake of conciseness, the reader is referred to Section B of the Supplementary Material for the detailed description of each of the 9 steps, while the key elements in PHAROS and POROS application, together with some examples, are shown in Table 1. In the following, the new concept of credibility of an attack action, not present in the original methodologies (Iaiani et al., 2021b, 2021c), is introduced.

As shown in Fig. 5, in both methodologies, in Step 1 the input information is collected, in Step 2 the nodes of concern are identified, in Step 3 the remotely manipulable components (RMC) and the relative manipulative elements (ME) of the BPCS and SIS are allocated to selected nodes, in Step 4 the remote manipulations (RM) on MEs and the corresponding local consequences (LC) on RMCs are identified, in Step 5 the security events (SE) of concern are associated to each node, in Step 6 the mechanisms of action (MA) through which such SEs can be initiated are investigated, in Step 7 the specific combination of local

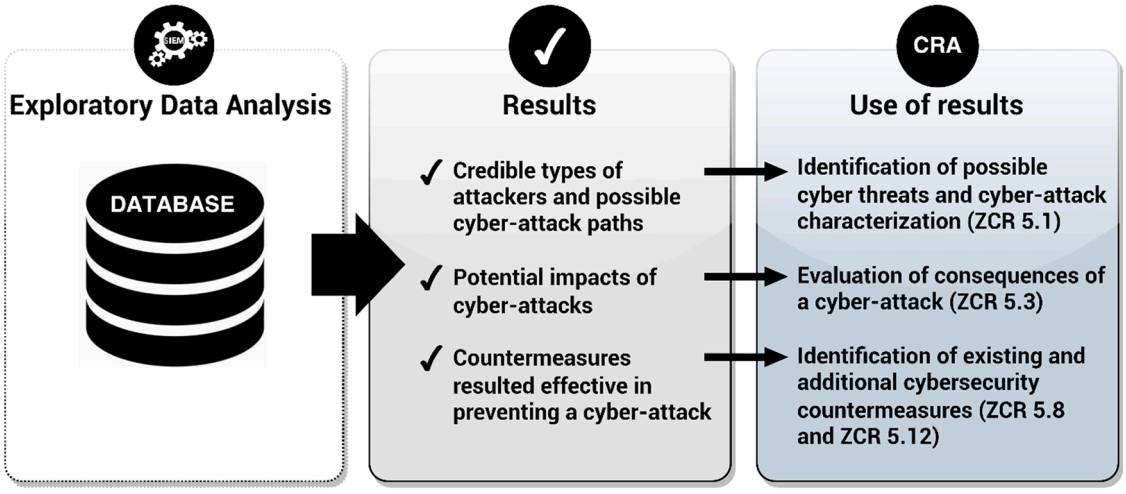

Fig. 3. Results obtained from the past incident analysis and their use in the context of cybersecurity risk assessment (CRA). The steps of the CRA proposed by ISA/IEC 62443 to which support is provided are reported in brackets.

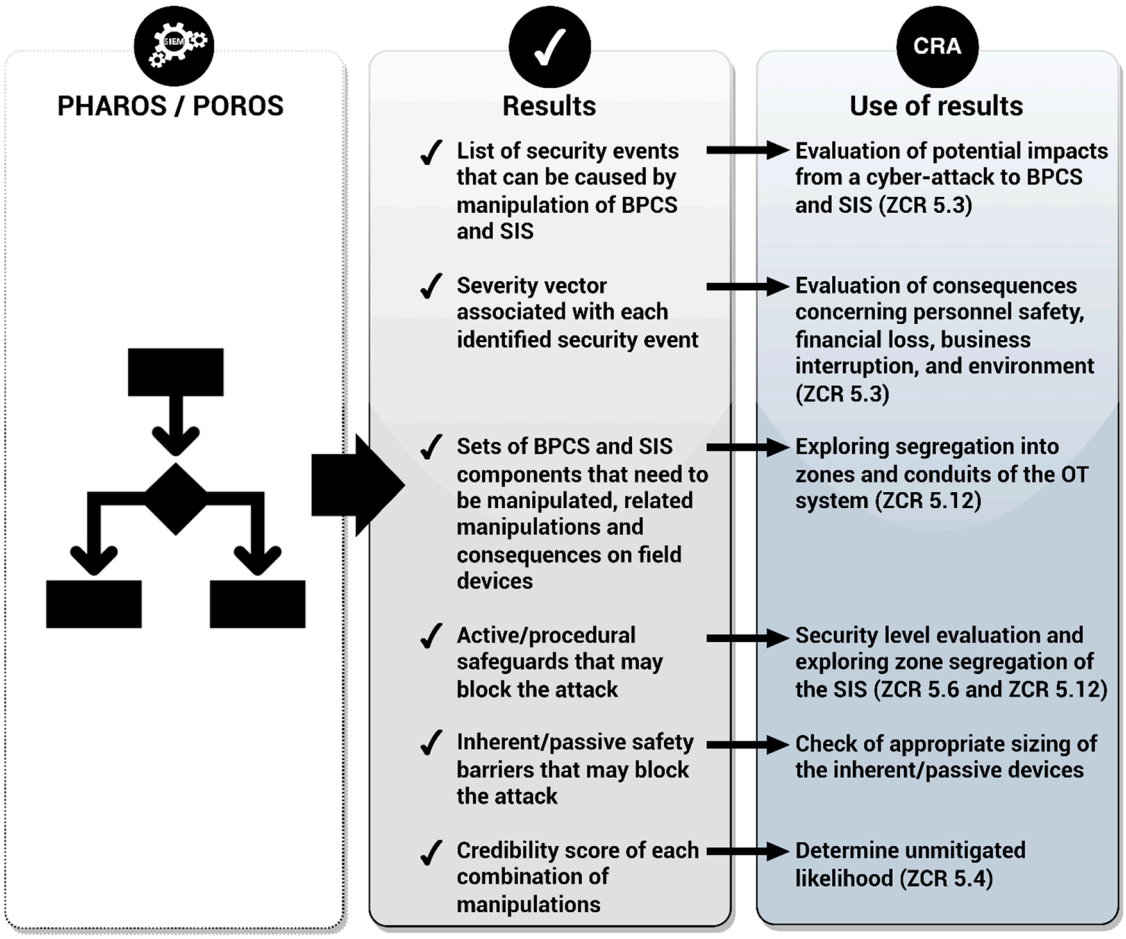

Fig. 4. Results that can be obtained from the application of PHAROS and POROS methodologies in the context of cybersecurity risk assessment (CRA). The steps of the CRA proposed by ISA/IEC 62443 to which support is provided are reported in brackets.

consequences on RMCs that are required to perform each MA are identified, in Step 8 the inherent/passive (IPS) and active procedural (APS) safeguards potentially effective in preventing or mitigating the SE are identified. Therefore, as output of Step 8 of both the methodologies, a list of CM+APS attack actions is obtained, that, if performed by an attacker, can trigger a specific security event in the physical process system. As several attack actions are generally possible for each SE, a further step is introduced (Step 9 in Fig. 5), requiring the estimation of a credibility score for each identified CM+APS attack action. The credibility of an attack action is a semi-quantitative score of the probability of the CM+APS attack action being successfully carried out by a generic attacker who gained access to the OT system of the facility. The credibility score of the SE is the greater among the credibility scores of the CM+APS attack actions through which it can be initiated.

The concept of CM+APS attack action credibility provides a basis for ranking the CM+APS attack actions, allowing a more effective allocation of resources for risk mitigation with respect to the most credible sets of manipulations and security events for the specific threat scenario of concern.

The credibility rank associated to each CM+APS attack action is estimated combining a score on two dimensions: the "plant knowledge level" required by the attacker and the "cyber complexity" of the CM+APS attack action. These dimensions fall within the scope of current analysis and are both identified as key contributors to the characterization of threats by the SRA methodology proposed by the API RP 780 standard (American Petroleum Institute, 2013).

The "plant knowledge level" is the degree of technical knowledge of the process plant under consideration (or of similar plants) which is required by the attacker in order to perform a given CM+APS attack action. This may span from need of complete knowledge about the plant (e.g., plant specific features need to be known) to no plant knowledge at all (e.g., no process plant competences required). A qualitative ranking based on three levels is proposed in Table 2.

The "cyber-complexity" of a CM+APS attack action scores how complex is the required attack action in terms of number of RMCs that have to be manipulated, the number of zones of the OT system that have to be accessed, and whether or not the actions to be performed require a specific sequence and timing. Four levels are proposed, each defined in Table 3. The concept of "zone" originates in the ISA/IEC 62443 series of standards (International Society of Automation and International Electrotechnical Commission, 2018): a "zone" is defined as the grouping of cyber assets that share the same cybersecurity requirements (e.g., BPCS and SIS are typically two different zones within the OT system). The reader is referred to the standard to more detailed information on zones.

Overall, the credibility score for a CM+APS attack action is calculated with the aid of the matrix reported in Fig. 6. As it can be observed from the figure, the credibility score increases as the level of "plant knowledge level" required by the attacker and the level of "cyber-complexity" of the actions to be carried out decrease. In fact, the lower the technical knowledge required by the attacker and the lower the complexity to perform a CM+APS attack action, the more the CM+APS attack action is likely to be performed by an attacker who successfully gained access to the OT system of the facility analysed. For example, the highest credibility score for a CM+APS attack action (i.e., score of 16) is obtained in case of low required "plant knowledge level" (score of 4) and low "cyber-complexity" of the attack action (score of 4) as any attacker,

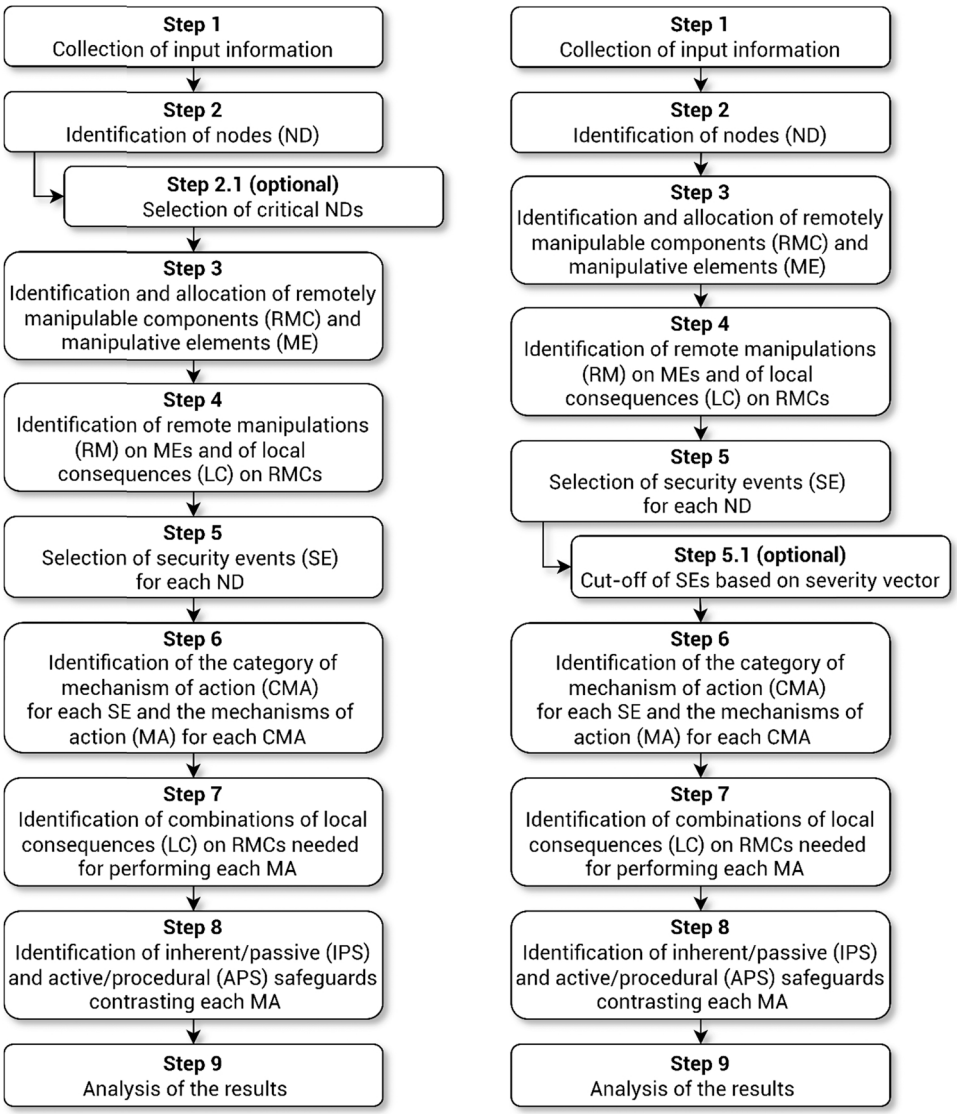

Fig. 5. a) Flowchart of PHAROS methodology; b) Flowchart of POROS methodology.

independently of his/her competencies on the plant, can easily complete such attack action.

Once all the steps have been carried out, the results can be summarized, for each assessed ND, in a worksheet as the one shown in Fig. 7. The first four rows of the worksheet summarize the node ID, the security events (SE) of concern selected for the ND, the categories of mechanisms of action (CMA), and the mechanisms of action (MA) that can be used by attackers to trigger the corresponding SE. The first column reports the remotely manipulable components (RMC) allocated to the ND. The columns in the centre list the local consequences (LCs) for each relevant RMC (each of these columns constitutes a combination (CM) to carry out the corresponding MA). The CM IDs are reported in the fifth row. The five bottom rows of the worksheet identify the active/procedural safeguards (APS), the inherent/passive safeguards (IPS), the score for required plant knowledge level of the attacker, the score of the cyber complexity of each CM+APS attack action, and the credibility score.

3. Illustrative case study

3.1. Set-up of the case study

An offshore Oil&Gas platform for gas compression is considered in the illustrative case study.

Fig. 8 shows the simplified block diagram of the process, while Fig. 9 shows the simplified P&ID of the section within the scope of the analysis (node ND_1 and node ND_2 in the following). The inlet stream from the sealine is separated by the Slug Catcher SC100. The liquid phase is sent to the liquid treatment section (out of the scope of current study), while the gas phase is sent to a two-stage compression with intermediate cooling by seawater (exchangers HE100 and HE101). The compressors CR100 and CR101 are driven by a gas turbine TR100. The KO drums KD100 and KD101 avoid the presence of liquid in the suction lines of the compressors.

The OT system managing the operations of the platform is composed by two zones as defined in Section 2.2.2: one consists of all the BPCS-related assets, while the other consists in all the SIS-related assets.

3.2. Results of the case study

3.2.1. Generic scenarios from past incident analysis

Combining the knowledge developed from the application of Exploratory Data Analysis (EDA) regarding the type of attacker, system affected, and impacts of cyber-attacks for a facility as the one considered in the case study, i.e., an offshore Oil&Gas platform for gas compression which fall under the “petrochemical” industrial sector class considered in PIA (the reader is referred to the reference source Iaiani et al. (Iaiani

Table 1
Definition of key elements in PHAROS and POROS application.

Element	Acronym	Definition	Examples
RMC	Remotely Manipulable Component	The physical objects in the plant whose operation is regulated by the BPCS and the SIS	Automatic control and shutoff valves, pumps, compressors, etc.
ME	Manipulative Element	The elements of the BPCS and the SIS that regulate RMCs	PID and PLC controllers and their logics
RM	Remote Manipulation	Manipulation action carried out remotely by attackers on MEs	Setpoint change, signal shutdown, etc.
LC	Local Consequence	Physical change on a RMC as a consequence of the manipulation of the ME by which the RMC is regulated	Valve closed/opened, pump/compressor with increased/decreased rotational speed, etc.
SE	Security Event	Undesired event that affects the operability and/or the physical integrity of the system under investigation	PHAROS: Loss of containment (LOC) or loss of physical integrity (LPI) involving a hazardous substance; POROS: LOC, LPI, stop of plant operations, operation out of specification, equipment damage, etc.
CMA	Category of Mechanism of Action	The general mechanism (based on a hypothetical facility) that can trigger a SE	Pressure exceeding safety limits
MA	Mechanism of Action	The specific mechanism (based on the features of the facility analysed), belonging to a CMA, that can trigger a SE	Increase the internal pressure of a vessel by closing the valve/s in the gas outlet stream
CM	CoMbination of local consequences	Set of LCs required to carry out a given MA	See examples of LCs
IPS	Inherent/Passive Safeguard	Devices/Elements that provide their safety action independently of the IT-OT network system under attack	Pressure Safety Valves (PSV), rupture disks, vent systems, emergency hatches, etc.
APS	Active/Procedural Safeguard	Automated or human-mediated actions which involve response by the same IT-OT network system under attack	Active safeguards: logics that perform automatic response actions on the physical process system; Procedural safeguards: monitoring systems, remote controls allowing to perform corrective actions on the physical process system, and any other human-mediated action
CM+APS	Attack action	Set of LCs required to carry out a given MA + set of APSs that have to be overcome by the attackers	See examples of CMs and APSs

et al., 2021c) for the detailed results), it was possible to define the following five generic cybersecurity scenarios:

1. accidental attacker infecting the IT system and compromising sensitive data;
2. intentional internal attacker infecting the OT system and inducing a LSD (local shutdown) or a PSD (process shutdown);
3. intentional external attacker infecting the OT system and inducing a LSD (local shutdown) or a PSD (process shutdown);
4. intentional internal attacker infecting the OT system and inducing a LOC (loss of containment) from equipment unit.
5. intentional external attacker infecting the OT system and inducing a LOC (loss of containment) from equipment unit.

Table 2
Definition of the ranking adopted for the required "plant knowledge level" of the attacker.

Plant knowledge level required	Definition	Examples of attacks	Examples of applicable CM+APS attack actions	Score
High (H)	The attacker needs complete technical knowledge on the process plant, i.e., complete access to plant documentation (PFD, P&ID, control philosophy, cause/effect matrix, etc.)	The attacker is able to carry out precise, non-random mechanisms (MAs) to initiate adverse events, taking into account plant specific features	• All CM+APSs identified by PHAROS/POROS application and not belonging to the categories below [Low and Medium knowledge]	1
Medium (M)	The attacker needs only general technical knowledge on the process plant and/or on similar plants	The attacker is able to carry out only common mechanisms (MAs) to initiate adverse events, ignoring plant specific features (e.g., mechanisms to cause overpressure reported in standard API 521)	• CM+APSs that do not depend on plant specific features (e.g., a specific design of pipework, a specific operating procedure) and do not belong to the category below [Low knowledge]	2
Low (L)	The attacker has not technical knowledge on the process plant or on similar plants	The attacker is able to carry out only "random" actions on the plant remote manipulable components (RMCs)	• CM+APSs consisting in the random manipulation of a single RMC • CM+APSs achievable by manipulating all the RMCs of a unit the same way	4

An accidental attack is an attack that is not directed towards a specific target, but that infects any vulnerable host. On the contrary, an intentional attack is carried out against a specific target and it is designated to exploit specific weaknesses of the target system: internal means that the attacker is an insider (e.g., employee, contractor, business partner, vendor, etc.) who normally has authorized access to the assets of the company, while external means that the attacker is from the outside the company management and normally has no authorized access.

It is important to underline that none of the incidents collected in the database involved an Oil&Gas platform. However, there is historical evidence of cyber-attacks targeting plants with equipment similar to those present in offshore Oil&Gas platforms (e.g., gas/liquid separators, heat exchangers, compressors, pipework, etc.) and processing and/or storing similar substances (e.g., crude oil, natural gas, etc.). Therefore, the same impacts are expected to be caused by cyber-attacks to plants like the one considered in the case study. For example, pipelines

Table 3
Definition of the ranking adopted for the "cyber complexity" of the CM+APS attack action.

Cyber complexity	Definition	Examples of attacks	Score
High (H)	The CM+APS requires the remote manipulation, with specific sequence and timing, of RMCs whose corresponding MEs are grouped in two or more "zones" of the OT system.	CM+APS requires closing a valve in zone A and, only when temperature is high enough, to start a pump in zone B (specific sequence)	1
Medium (M)	The CM+APS requires the remote manipulation, with no specific sequence, of RMCs whose corresponding MEs are grouped in two or more "zones" of the OT system.	CM+APS requires manipulating a valve in zone A and a pump in zone B (no specific sequence)	2
Low (L)	The CM+APS requires the remotely manipulation, with no specific sequence, of several RMCs of different type, whose corresponding MEs are grouped in the same "zone" of the OT system.	CM+APS requires manipulating a valve and a pump in the same zone A (no specific sequence)	3
Very low (VL)	The CM+APS requires the remotely manipulation of a single RMC or the remotely manipulation, with no specific sequence, of several RMCs of the same type, whose corresponding MEs are grouped in the same "zone" of the OT system.	CM+APS requires stopping a pump in zone A	4

Credibility score of a CM+APS attack action		Plant knowledge level		
		L	M	H
Cyber complexity	VL	16	8	4
	L	12	6	3
	M	8	4	2
	H	4	2	1

Fig. 6. 4 × 3 matrix for the estimation of the credibility score for a CM+APS attack action, based on "cyber complexity" and "plant knowledge level".

transporting oil and gas, as well as refineries, have been strongly affected by cyber-attacks in the last two decades (Iaiani et al., 2021c). In addition to the two events described in the introduction Section (BTC pipeline explosion in 2008 and Colonial Pipeline ransomware attack in 2021), in another case, occurred in 2012 in Saudi Arabia, attackers infected the network system of a Saudi Aramco oil plant with Shamoon worm aiming at stopping oil and gas production in the Country. Even if they did not succeed in their primary objective, approximately 30,000 computers were affected and lot of sensitive data was stolen. Moreover, in 2003 in the United Kingdom, attackers infected with MUMU worm the OT system of a petrochemical plant owing to a weak admin password in an HMI workstation. The fiscal metering system became infected and production was stopped for an unspecified number of days.

With reference to the generic cybersecurity scenarios listed above, it can be noted that only accidental cyber-attacks are considered as causes of IT-related impacts. This is due to the fact that, in chemical and process plants, the presence of high quantities of hazardous materials poses risks that are much higher than those posed by IT assets, and thus complex and target-specific attacks are considered having as primary objective the generation of OT-related impacts, as more severe consequences can be caused. Moreover, as typically accessing the OT system requires bypassing more layers of protection (e.g., firewalls) than accessing the IT system, even if there is historical evidence of accidental cyber-attacks able to affect the OT system, they are not considered as possible causes of OT-related impacts. Therefore, only intentional attacks, performed by both insiders and outsiders, are associated to LSD/PSD and LOC/LPI impact scenarios.

Among all the possible threats, insiders are considered a very critical category of attackers as they usually have extensive knowledge of both the process and the plant, and they can carry out the attacks having direct access to the assets of the facility (no scanning and gaining access phases are needed as for external attackers (Iaiani et al., 2021c)).

Overall, the results obtained through PIA do not provide sufficient detail to identify the specific attack actions (e.g., the manipulations that the attackers have to carry out in order to generate the desired security events) which strongly depend on the features of the IT-OT network infrastructure of the analysed platform. Therefore, in order to integrate the information on the impacts present in the generic cybersecurity scenarios listed above and derived from PIA, PHAROS or POROS is applied.

3.2.2. *Case-specific cyber-risk identification using POROS methodology*

Depending on the scope of the analysis which may be on major accident scenarios or that may also include operability issues, PHAROS or POROS is chosen. Clearly enough, given the systematicity of the two analyses, the sets of combinations initiating major events obtained by applying POROS coincide exactly with those that would be obtained by applying PHAROS to the same plant.

In the context of the present case study, POROS methodology was applied, allowing to identify the specific attack actions (CM+APS) that can initiate both PSD/LSD and LOC/LPI impacts scenarios. This way, it was possible to integrate, with case-specific knowledge, the generic cybersecurity scenarios derived from PIA that imply an infection of the OT system (i.e., scenarios from 2 to 5, see Section 3.2.1). In the following, the main results obtained from the application of POROS are reported.

Once the needed information was collected (Step 1, see Fig. 5), the remotely manipulable components (RMCs) of the plant and the corresponding manipulative elements (MEs) were identified and allocated in the two nodes considered in the case study (ND_1 and ND_2 identified in Step 2, see Fig. 5), following the guiding rules reported in the description of Step 3 of the methodology. The results are summarized in Table 4: RMCs include emergency shut-off valves (blowdown valve and shutdown valves), control valves and a motor-driven gas turbine. The shut-off valves are controlled by MEs which are part of the SIS (e.g., PLCs), while the control valves are controlled by MEs belonging to the BPCS (e.g., PID controllers). The gas turbine is controlled by both BPCS and SIS, which are two different zones in the OT system of the facility analyzed.

As for the remote manipulations (RMs) to the MEs and the local consequences (LCs) on RMCs (Step 4, see Fig. 5), "signal shutdown" and "function reprogramming" were considered for all the MEs of the SIS and for the single ME of the BPCS acting on the gas turbine, while "signal shutdown" and "setpoint change" were applied for all the remaining MEs of the BPCS. The identification of the LCs on the RMCs allocated to the two nodes of interest required to consider the fail-safe nature of all the automatic valves, the control action of the PID controllers (direct or

ND_ID		RESULTS FROM PHAROS/POROS APPLICATION					
Security events (SEs)		SE.x, SE.y		SE.z		Additional SEs	
Categories of mechanisms of action (CMAs)		CMA.α		CMA.β		CMA.δ	
Mechanisms of action (MAs)		MA.α1	MA.α*	MA.β1	MA.β*	MA.δ1	MA.δ*
Combinations (CMs)		CM.1	...	...	...	...	CM.*
Remotely manipulable components (RMCs)	RMC.1	LC	...	...	...	...	LC
	...	...	...	...	...	...	...
	...	...	...	...	...	...	...
	RMC.*	LC	...	...	...	...	LC
Active/Procedural safeguards (APSs)		APSs	...	...	...	...	APSs
Inherent/Passive safeguards (IPSs)		IPSs	...	...	...	...	IPSs
Required plant knowledge level		H/M/L	...	...	...	...	H/M/L
Cyber complexity		H/M/L/VL	...	...	...	...	H/M/L/VL
Credibility		...	...	...	...	...	...

Fig. 7. Worksheet proposed for the summary of the results obtained from PHAROS/POROS application for a selected node (ND).

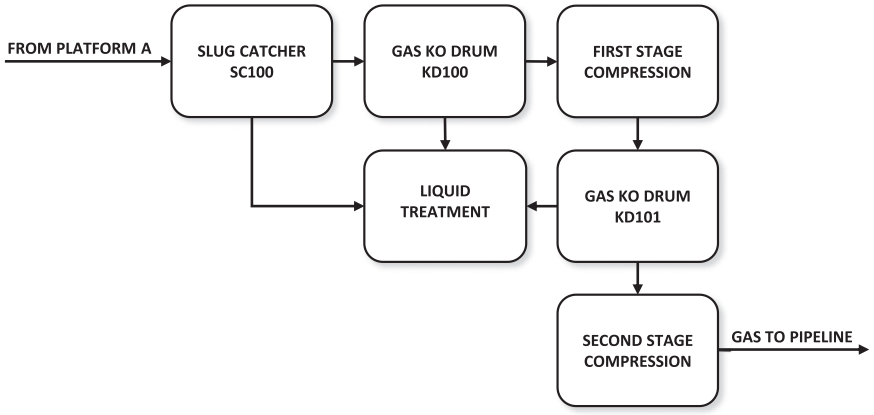

Fig. 8. Simplified block diagram of the offshore Oil&Gas platform considered in the illustrative case study.

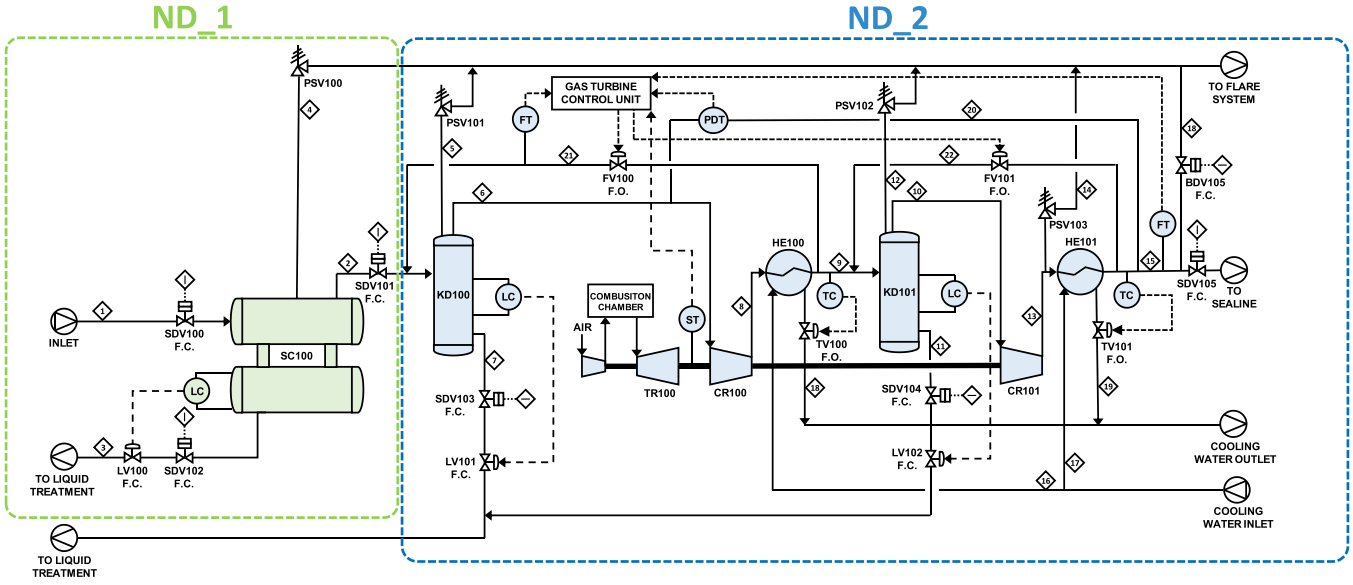

Fig. 9. Simplified P&ID of the nodes ND_1 ("Slug Catcher") and ND_2 ("Two-phase compression").

Table 4
Remotely manipulable components (RMCs) allocated to nodes ND_1 and ND_2 and zone of the corresponding manipulative elements (MEs) in the OT system. FC: fail close; FO: fail open.

RMC	RMC type	Allocated to	ME zone
SDV100	RMC1: shut-off valve (FC)	ND_1	SIS
SDV101	RMC1: shut-off valve (FC)	ND_1 and ND_2	SIS
SDV102	RMC1: shut-off valve (FC)	ND_1	SIS
SDV103	RMC1: shut-off valve (FC)	ND_2	SIS
SDV104	RMC1: shut-off valve (FC)	ND_2	SIS
SDV105	RMC1: shut-off valve (FC)	ND_2	SIS
BDV105	RMC1: shut-off valve (FO)	ND_2	SIS
LV100	RMC2: control valve (FC)	ND_1	BPCS
LV101	RMC2: control valve (FC)	ND_2	BPCS
LV102	RMC2: control valve (FC)	ND_2	BPCS
TV100	RMC2: control valve (FC)	ND_2	BPCS
TV101	RMC2: control valve (FC)	ND_2	BPCS
FV100	RMC2: control valve (FC)	ND_2	BPCS
FV101	RMC2: control valve (FC)	ND_2	BPCS
GAS TURBINE (TR100 + CR100 + CR101)	RMC4: gas turbine launched by electric motor	ND_2	BPCS and SIS

reverse), the logics of the PLCs and the safety instrumented functions (SIFs) of the SIS. For instance, as a consequence of a signal shutdown to the PLC by which the valve is controlled (i.e., its ME), the shutdown valve SDV100 stops the flow as it fails in the closed position.

For both the nodes, the security events (SEs) considered (Step 5, see Fig. 5) and further detailed in terms of set of manipulations of the BPCS and SIS, are "activation of ESD/PSD/LSD logic" (coded SE03 according to the codes reported in the guiding lists present in the reference source of POROS methodology (Iaiani et al., 2021c) and "loss of containment (LOC) and loss of physical integrity (LPI)" (coded SE06). These SEs are the two identified through PIA (see Section 3.2.1). Considering an average value of production of 1′420′000 $/day, a severity vector of [2, 1,1,1] was estimated for SE03: economic losses from downtime are between $100 K and $1MM (recovery follows normal start-up procedures, with expected downtime of less than 6 h), which scores a severity level 2 for EC according to the scale proposed by Iaiani et al. (2021c); no appreciable loss of reputation is expected due to the limited outcomes of the event on third parties (severity level 1 for IV); no damage to environment (severity level 1 for EN); no damage to people (severity level 1 for HV) as plant integrity is maintained in the SE. In the same way, a severity vector of [4,2,1,1] was estimated for SE06: recovery requires repair and replacement of equipment (estimated losses of more than $10MM, i.e., severity level 4 for EC); the scenarios following the loss of containment (e.g., jet fire) would be notified to the population in the nearby areas and may affect regional reputation (severity level 2 for IV); negligible damages to environment are expected from natural gas release (severity level 1 for EN); damage to people is considered unlikely as the platform is normally unmanned (severity level 1 for HV).

Though severity of SE03 is clearly low (each component of the severity vector scores a severity level lower than 3), no cut-off according to Step 5.1 (see Fig. 5) was carried out in the current case study in order to provide a more complete presentation of potential results.

For both the nodes, the credible mechanisms of action (MAs) through which an attacker can initiate any of the selected SEs, were identified (Step 6, see Fig. 5): the identification was based on the applicable categories of mechanisms of action (CMAs) provided in the reference source of the methodology (Iaiani et al., 2021c), and tailoring them considering the equipment units present in the system under assessment. The results are summarized in Table 5. For example, the generation of a false signal, whether it is of very high level (MA1, MA4, and MA5), temperature (MA3), pressure (MA6), which activates a ESD/PSD/LSD logic is the mechanism of action through which SE03 can be generated in both the nodes. In the same way, inducing excessive pressure by closing the gas outlet from heat exchanger HE101 (MA7), by increasing the rotation speed of the GAS TURBINE (MA8), or a combination of the two MAs (MA9), or, alternatively, inducing start and stop cycles of the GAS TURBINE (MA10), or inducing liquid fraction in compressor CR100 suction by overfilling the knockout drum KD100 (MA11), were found as the mechanisms of action through which SE06 can be initiated in node ND_2. However, it is important to underline, that MA11 requires actions on the nearby node ND_1 to be obtained. In fact, in order to overfill KD100 it is necessary having liquid in the gas stream entering it: this can be obtained by overfilling the slug catcher SC100 which belongs to ND_1. Therefore, a new SE was added to the ones considered for ND_1, named "SE01: product out of specification (liquid fraction in the gas outlet)".

Moreover, another important thing to underline, is that no suitable MA was identified for SE06 in ND_1: in fact, the specific features of the equipment present in this node and the processed fluids do not allow the occurrence of the SE (e.g., no change of temperature is possible, pressure from upstream lines is always lower than design pressure).

Clearly enough, as already stated, given the systematicity of PHAROS and POROS methodologies, combinations CM2, CM3, and CM8 to CM15 (see Table 5) would have been identified also by PHAROS application to the system analyzed as they refer to mechanisms of action that are aimed at initiating major accident scenarios such as LOC of hazardous substances and LPI which are within the scope of the methodology.

A total of 15 combinations (CMs) were identified in Step 7 (see Fig. 5) to carry out the identified MAs. Table 6 reports the ones identified for ND_1 (i.e., CM1 – CM3), while Table 7 and Table 8 the ones identified for ND_2 (i.e., CM4 – CM15). The tables also report the active/procedural safeguards (APSs) and inherent/passive safeguards (IPSs), identified in the application of Step 8 (see Fig. 5), that can block each CM. As an example, CM3 (see Table 6) consist in manipulating the ME of the SIS which acts on SDV102 so that the valve closes: the PSD logic activated by LSHH on SC100, the high and very high level alarms (LAH and LAHH) on SC100 plus the hand-switch (HS) for manual ESD/PSD/LSD, and the position light ZLL for SDV102 plus the HS for its manual reset, are the APSs contrasting this CM. Instead, no IPS is present. Alternatively, in order to perform the same MA (i.e., MA2), a different way is to manipulate the ME of the BPCS which acts on the level control valve LV100 so that the valve closes partially or totally (see CM2 in Table 6): with the exception of the SDV102 position light ZLL, all the APSs reported for CM3, are potentially effective also against CM2.

Virtual RMCs have been added to the ones allocated to the two nodes in order to fictitiously represent those RMCs that are manipulated as a consequence of a false signal to the SIS that initiates a ESD/PSD/LSD of the system analysed (see CM1 in Table 6 and CM4 to CM7 in Table 7).

As the last step of the methodology (Step 9, see Fig. 5), the credibility score for the required "plant knowledge level" and that for the "cyber complexity" were evaluated for each CM+APS attack action, according to the credibility ranking scales reported and defined in Table 2 and Table 3 respectively. It is important to underline that, for the purposes of this illustrative example, the assessment of the scores was performed considering only active safeguards (i.e., ESD/PSD/LSD logics). As procedural safeguards require human-mediated actions and the probability of human errors may be high during emergency situations (Mannan, 2012). This choice is expected to provide reasonable results in most

Table 5
Security events (SE), associated severity vectors, mechanisms of action (MAs), number of combinations (CMs) identified for ND_1 and ND_2, and credibility score of the related CM+APS attack action.

Node	SE	Severity vector [EC,IV,EN,HV]	MA	Identified CMs	CM+APS credibility score
ND_1	SE03: activation of ESD/PSD/LSD logic	[2,1,1,1]	MA1: generating a false signal of very high level in SC100	CM1	8
	SE06: loss of containment (LOC) and loss of physical integrity (LPI)	[4,2,1,1]	No MA identified		
	(added) SE01: product out of specification (liquid fraction in the gas outlet)	[1,1,1,1]	MA2: overfilling of SC100 by closing the liquid outlet	CM2 CM3	4 6
ND_2	SE03: activation of ESD/PSD/LSD logic	[2,1,1,1]	MA3: generating a false signal of very high temperature in the gas discharge manifold	CM4	8
			MA4: generating a false signal of very high level in KD100	CM5	8
			MA5: generating a false signal of very high level in KD101	CM6	8
			MA6: generating a false signal of very high pressure in CR100 suction	CM7	8
	SE06: loss of containment (LOC) and loss of physical integrity (LPI)	[4,2,1,1]	MA7: inducing excessive pressure by closing the gas outlet from HE101	CM8	6
			MA8: inducing excessive pressure by increasing the rotation speed of the GAS TURBINE	CM9	4
			MA9: inducing excessive pressure by closing the gas outlet from HE101 + increasing rotation speed of the GAS TURBINE	CM10	2
			MA10: inducing start and stop cycles or speed variation cycles of the GAS TURBINE	CM11	8
			MA11: inducing liquid fraction in CR100 suction by overfilling KD100 (requires actions on ND_1)	CM12 CM13 CM14 CM15	2 3 2 2

Table 6
CM+APS attack actions identified for node ND_1 and related credibility scores.

ND_1				
Combinations (CM)		CM1	CM2	CM3
Relevant remotely manipulable components (RMC)	SDV102	-	-	Totally closed
	LV100	-	Partially/Totally closed	-
	Virtual RMCs	Manipulated as a consequence of false signal initiating ESD/PSD/LSD	-	
Active/Procedural safeguards (APS)		-	• PSD logic activated by LSHH on SC100 • LAH/LAHH on SC100 + manual ESD/PSD/LSD	• PSD logic activated by LSHH on SC100 • LAH/LAHH on SC100 + manual ESD/PSD/LSD • Position light ZLL for SDV102 + SDV102 manual reset
Inherent/Passive safeguards (IPS)		-	-	-
Plant knowledge level		M	M	M
Cyber complexity		VL	M	L
Total credibility score		8	4	6

Table 8
CM+APS attack actions identified for node ND_2 and related credibility scores (CM12 +APS_{CM12} to CM15 +APS_{CM15}).

ND_2 (CM12 +APS_{CM12} to CM15 +APS_{CM15})					
Combinations (CM)		CM12	CM13	CM14	CM15
Relevant remotely manipulable components (RMC)	SDV103	Totally closed	Totally closed	-	-
	LV101	-	-	Partially/Totally closed	Partially/Totally
	RMCs in ND_1	Manipulated (see CM2 in Table 6)	Manipulated (see CM3 in Table 6)	Manipulated (see CM2 in Table 5)	Manipulated (see CM3 in Table 5)
Active/Procedural safeguards (APS)		• PSD logic activated by LSHH on SC100 • LSD logic activated by LSHH on KD100 • LAHs/LAHHs on SC100 and KD100 + manual ESD/PSD/LSD • Position light ZLL for SDV103 + SDV103 manual reset	• PSD logic activated by LSHH on SC100 • LSD logic activated by LSHH on KD100 • LAHs/LAHHs on SC100 and KD100 + manual ESD/PSD/LSD • Position light ZLL for SDV102 and SDV103 + SDV102/3 manual reset	• PSD logic activated by LSHH on SC100 • LSD logic activated by LSHH on KD100 • LAHs/LAHHs on SC100 and KD100 + manual ESD/PSD/LSD	• PSD logic activated by LSHH on SC100 • LSD logic activated by LSHH on KD100 • LAHs/LAHHs on SC100 and KD100 + manual ESD/PSD/LSD • Position light ZLL for SDV102 + SDV102 manual reset
Inherent/Passive safeguards (IPS)		-	-	-	-
Plant knowledge level		H	H	H	H
Cyber complexity		M	L	M	M
Total credibility score		2	3	2	2

Table 7
CM+APS attack actions identified for node ND_2 and related credibility scores (CM4 +APS_{CM4} to CM11 +APS_{CM11}).

ND_2 (CM4 +APS_{CM4} to CM11 +APS_{CM11})						
Combinations (CM)		CM4 (CM5, CM6, CM7)	CM8	CM9	CM10	CM11
Relevant remotely manipulable components (RMC)	SDV105	-	Totally closed	-	Totally closed	-
	GAS TURBINE	-	-	Increased rotational speed	Increased rotational speed	Started and stopped cyclically
	Virtual RMCs	Manipulated as a consequence of false signal initiating ESD/ PSD/LSD	-	-	-	-
Active/Procedural safeguards (APS)		-	• PSD logic activated by PSHHs in compression train • PAHs/PAHHs in compression train + manual ESD/PSD/LSD • Position light ZLL for SDV105 + SDV105 manual reset	• PSD logic activated by PSHHs in compression train • LSD logic activated by Anti-Surge system • PAHs/PAHHs in compression train + manual ESD/ PSD/LSD	• PSD logic activated by PSHHs in compression train • LSD logic activated by Anti-Surge system • PAHs/PAHHs in compression train + manual ESD/PSD/LSD • Position light ZLL for SDV105 + SDV105 manual reset	• LSD logic activated by Anti-Surge system • GAS TURBINE unavailability alarm UA + manual ESD/ PSD/LSD
Inherent/Passive safeguards (IPS)		-	PSV101/2/3	PSV101/2/3	PSV101/2/3	-
Plant knowledge level		M	M	M	H	L
Cyber complexity		VL	L	M	M	M
Total credibility score		8	6	4	2	8

cases. For example, a medium (M) knowledge of the plant is expected for CM3 +APS_{CM3} attack action (see Table 6) since the attacker is not required to have complete technical knowledge of the system being analysed, but of similar plants: slug catchers, like SC100, typically have a single liquid outlet with a valve for level control and a shutdown valve for emergency situations; moreover, no overflow regulating element are typically present in the vessel other than a very high level alarm activating automatic response of the SIS.

Moreover, a low (L) cyber complexity is expected as the CM3+APS_{CM3} attack action requires the manipulation of different MEs present in the same zone of the OT system, i.e., the SIS (ME acting on SDV102 and PSD logic). Differently, while the "plant knowledge level" is the same for CM2+APS_{CM2} attack action, a medium (M) "cyber complexity" is expected as it requires the manipulation of MEs which are part of different zones of the OT system (i.e., both elements of the BPCS and the SIS). A total credibility score of 4 was obtained from the matrix reported in Fig. 6 for CM2+APS_{CM2}, while a value of 6 for CM3+APS_{CM3}.

4. Discussion

As proved by the results obtained in the illustrative case study, the knowledge developed through the past incident analysis (PIA) identified generic cybersecurity-related scenarios that can potentially occur in the facility analysed (i.e., an offshore Oil&Gas platform for gas compression which fall under the "petrochemical" industrial sector class considered in PIA). These generic scenarios are characterized in terms of type of attacker (accidental, intentional internal, intentional external), system affected (IT system or OT system), and type of impact caused by the cyber-attack (corruption of sensitive data, PSD/LSD, LOC/LPI).

Depending on the level of detail required in the cyber-risk assessment, these scenarios can be directly used as input data (e.g., CRA approach proposed by ISA/IEC 62443 series of standards or SVA/SRA methodologies such as CCPS SVA, API RP 780, VAM-CF, RAMCAMP), or they can be used as reference basis to undertake a case-specific cyber-risk identification. While the use of reference scenarios is a well-established practice in the safety domain (Mannan, 2012), the considerable variety of the systems in the field of security, and particularly of cybersecurity, may require the need for case-specific assessments. Moreover, accidental and intentional cyber-attacks to the OT system of process facilities and offshore Oil&Gas facilities are rare events, and thus it is possible that some specific features of the BPCS and SIS of the facility analysed may lead to unprecedented events when they are manipulated.

For this reason, in order to explore the actual possibility of occurrence of both the LOC/LPI and the PSD/LDS impact scenarios, POROS methodology has been applied to the system described in the case study. However, it is important to underline that if, for whatever reason (e.g., concern on worst-case consequences), the scope of the analysis had been limited to major accident scenarios, PHAROS would have been applied to the case study, obtaining the same results of POROS regarding the LOC/LPI impact scenarios with a more focused resource effort (SE03 scenarios not analysed).

In particular, the application of POROS methodology to the offshore Oil&Gas platform considered in the case study supported the systematic identification of the sets of manipulations of the BPCS and SIS through which LOC/LPI and PSD/LSD impact scenarios can be triggered, as well as that of the active/procedural (APS) and inherent/passive (IPS) safeguards in place that can block the attacks. This allowed to develop case-specific knowledge on the impacts of cyber-attacks which, combined with the information on the type of attacker derived from PIA, can be used as valuable information in the context of existing methodologies for cyber-risk assessment (CRA).

A PSD/LDS impact scenario was found to be possible for the system analysed as POROS application provided a total of 5 combinations of manipulations (see CM1 in Table 6 and CM4 to CM7 in Table 7) which, if performed by attackers, can potentially cause the local shutdown of a section of the plant (LSD) or that of the entire process (PSD). Overall, these CMs consist in inducing a false signal (very high level in SC100, very high temperature in the gas discharge manifold, very high level in KD100 and KD101, and very high pressure in CR100). This information can be integrated in the generic scenarios 2 and 3 derived from PIA and formulated in Section 3.2.1 in order to develop case-specific cybersecurity scenarios to be provided to existing methodologies for CRA, consisting in the following information: type of attacker (from PIA), system infected (from PIA and POROS), type of impact (from PIA and POROS), sets of manipulations to initiate such impact and related credibility score (from POROS).

In the same way, according to the results obtained from POROS application, a LOC/LPI impact scenario was found possible for the system analysed as 8 combinations of manipulations were identified as

possible causes of a release from equipment and/or pipework present in the platform (see CM8 to CM11 in Table 7 and CM12 to CM15 in Table 8). These CMs are aimed at inducing excessive pressure or inducing damage to the GAS TURBINE with consequent gas release (LOC). Again, developed knowledge on impacts derived from POROS application, combined with one obtained from PIA on attacker type, allowed to developed case-specific cybersecurity scenarios to be provided to existing methodologies for CRA. An example of such scenarios is the following (referred to CM15+APS_{CM15} attack action, see Table 8, integrating scenario 5 derived from PIA): an intentional external attacker accesses the OT system managing the platform + manipulates the BPCS controller acting on LV101 inducing its closure (partial or total) + manipulates the SIS controller acting on SDV103 inducing its closure + disables the PSD logic activated by LSHH on SC100+ disables the LSD logic activated by LSHH on KD100. Moreover, together with this information, the procedural safeguards (high level alarms LAHs on SC100 and KD100+ HS for manual ESD/PSD/LSD, very high level alarms LAHHs on SC100 and KD100+ HS for manual ESD/PSD/LSD, position light ZLL for SDV102+ HS for manual reset of SDV102), the inherent/passive safeguards (none in this case), and the credibility score (2), are provided.

The results reported in Table 6, 7 and 8, demonstrate that, in some circumstances, only a small number of RMCs need to be manipulated in order to carry out a mechanism of action that can trigger a security event with potential severe consequences. For example, combinations CM1 to CM9 and CM11 are characterized by the manipulation of a single RMC: clearly, this finding could be index of a system with low security performances, since attackers who are able to gain access to the OT system managing the platform are not required to perform complex attacks in order to trigger security events of concern. However, if, for a given CM, there are active/procedural safeguards (APS) potentially effective in contrasting it, the attackers have to tamper with them too in order to prevent a safe response of the system being attacked, making the attacks more complex (this is the case of combinations CM2, CM3, CM8 to CM15).

Another important remark is that combinations CM8, CM9, and CM10 (i.e., the ones that are aimed at increasing pressure, see Table 7) differ from all the others as they present passive safeguards (the PSVs, pressure safety valves) among the identified barriers potentially able to contrast the attack, which are not controlled by the OT system, and thus can not be remotely manipulated by attackers. In case of proper design, the PSVs can be considered fully effective in avoiding pressurization and thus in avoiding the corresponding SE (i.e., the gas release): this means that even if attackers are able to perform the manipulations required by CM8, CM9, and CM10 and bypass the PSD logic of the SIS activated by PSHH, the three PSVs can prevent the pressurization of the system in case they are able to manage the pressure condition generated by the manipulations.

Therefore, it is important to take into account security cases originating by the malicious manipulation of the OT system (e.g., BPCS and SIS) when sizing inherent/passive safeguards (IPS): for example, considering the scenarios related to cybersecurity in addition to those reported in standard API 521 for the sizing of pressure-relieving and depressurizing systems such as PSVs. However, the result obtained in the case study proved that IPSs may not be effective against the totality of the mechanisms of action: in fact, the MAs aimed at overfilling the slug catcher (MA2 in Table 5) or the knockout drums (MA11 in Table 5) can not be prevented by the IPSs in place.

Among all the combinations (CMs) provided in Table 6, 7 and 8, CM1, CM4 CM5, CM6 and CM7 resulted the ones with the highest credibility score (equal to 8). In fact, a very low (VL) cyber complexity is required due to the fact that only a single ME of the SIS needs to be manipulated and that no APSs are present contrasting such manipulations. Moreover, a medium (M) plant knowledge level of the attacker is deemed to be sufficient to impart these CMs (attacker with general technical knowledge on the plant or on similar plants). Therefore, SE03 (activation of ESD/PSD/LSD logic), resulted a very credible impact scenario for the offshore Oil&Gas platform analyzed as a consequence of malicious manipulation of the BPCS and SIS.

A total credibility score equal to 8 (low (L) plant knowledge level and medium (M) cyber complexity) was estimated also for combination CM11 aimed at damaging the GAS TURBINE with start and stop cycles, resulting a very credible attack path to initiate SE06 (LOC or LPI). Another credible combination through which this security event can be initiated is CM8 aimed at inducing high pressure in the compression stage (a total credibility score of 6 was obtained).

On the contrary, CM10 resulted the combination with the lowest credibility score (equal to 2): this is due to the fact that both the BPCS and the SIS need to be manipulated even if without a specific sequence and timing (medium (M) cyber complexity) and that complete technical knowledge on the plant is required by the attacker (high (H) plant knowledge level).

The proposed framework is currently limited to the scope of the identification of security events and attack actions (malicious manipulations of the BPCS and the SIS) in the physical process system. As such, it does not provide quantitative evaluation of the risk associated to cyber-attacks. However, the clear identification of the CMs, APSs, and IPSs provided by the current framework of methods, which define the cyber-attack actions to be contrasted, paves the way for future developments aimed at the quantification of the probability of success of a cyber-attack action, which is a key part of the quantitative evaluation of the cyber-risk.

The practical application of PHAROS and POROS methodologies may require considering large numbers of SEs and CM+APS attack actions when applied to complex plants with many nodes. This limitation may, in the future, be overcome by the development of software tools allowing easy management of relevant data and automation of some steps of the procedures (e.g., identification of RMCs).

5. Conclusions

The present study fills the gap in the availability of systematic operating procedures for the security assessment of the link between malicious manipulations of the BPCS and SIS and the impacts on the physical process system that can be initiated. A framework of synergic methods aimed at supporting cyber-risk identification in process plants is described and applied for demonstration to an illustrative case study.

The framework consists of a past incident analysis (PIA) that can be used to define generic cybersecurity-related scenarios that can potentially occur in a facility, and of two rigorous methodologies aimed at the systematic identification of the major accident scenarios (PHAROS methodology) and of the production outage scenarios (POROS methodology) that can generate in a facility.

The new concept of credibility of the attack action was effectively applied to rank the probability of success of identified attack actions based on the required plant knowledge level of the attacker and the cyber complexity of the manipulations. This provides valuable information on how to allocate resources in order to make the system analysed more secure against those manipulations that are believed to be more credible (higher credibility scores).

The outcomes of the application of the synergic framework of methods (list of credible attackers, list of credible impact scenarios that can be initiated by malicious manipulations of the BPCS and the SIS, ranking of the possible consequences of such impact scenarios, list of the sets of manipulations (attack actions) required to perform the attacks and related credibility, identification of the safeguards of the process system that can block the attacks) provide information suitable to support the application of the steps regarding the characterization of the facility, the threat assessment, the vulnerability assessment, and countermeasures identification of SVA/SRA methodologies such as CCPS SVA, API RP 780, VAM-CF, RAMCAP, CRA of ISA/IEC 62443 series of standards.

Declaration of Competing Interest

The authors declare that they have no known competing financial interests or personal relationships that could have appeared to influence the work reported in this paper.

Acknowledgments

This work was supported by INAIL (Istituto Nazionale per l'Assicurazione contro gli Infortuni sul Lavoro, Italy) in the framework of the 4th SAF€RA call.

Appendix A. Supporting information

Supplementary data associated with this article can be found in the online version at doi:10.1016/j.psep.2023.01.078.

References

American Petroleum Institute (API), 2013. API RP 780 - Security Risk Assessment Methodology for the Petroleum and Petrochemical Industries.

Bing, C., Kelly S., 2021. Cyber attack shuts down U.S. fuel pipeline 'jugular,' Biden briefed | Reuters [WWW Document]. Reuters. URL ⟨https://www.reuters.com/technology/colonial-pipeline-halts-all-pipeline-operations-after-cybersecurity-attack-2021–05-08/⟩ (accessed 10.13.22).

Center for Chemical Process Safety (CCPS), 2022. Managing Cybersecurity in the Process Industries - A Risk-based Approach. Wiley.

Center of Chemical Process Safety (CCPS), 2003. Guidelines for Analyzing and Managing the Security Vulnerabilities of Fixed Chemical Sites. Wiley/AIChE, New York.

Cozzani, V., Yang, M., 2022. Special issue: process safety in times of a pandemic. J. Loss Prev. Process Ind. 76. https://doi.org/10.1016/J.JLP.2022.104746.

Cusimano, J., Rostick, P., 2018. If It Isn't Secure, It Isn't Safe: Incorporating Cybersecurity into Process Safety. AIChE Spring Meet. Glob. Congr. Process Saf.

DIN VDE V 0831–104: Electric signalling systems for railways - Part 104: IT Security Guideline based on IEC 62443., 2015.

Faramondi, L., Setola, R., 2019. Identification of vulnerabilities in networked systems. Adv. Sci. Technol. Secur. Appl. 79–96. https://doi.org/10.1007/978-3-030-00024-0_5/TABLES/1.

Gertman, D., Folkers, R., Roberts, J., 2006. Scenario-based approach to risk analysis in support of cyber security. Proc. 5th Int. Top. Meet. Nucl. plant Instrum. Control. Hum. Mach. interface Technol.

Hashimoto, Y., Toyoshima, T., Yogo, S., Koike, M., Hamaguchi, T., Jing, S., Koshijima, I., 2013. Safety securing approach against cyber-attacks for process control system. Comput. Chem. Eng. 57, 181–186. https://doi.org/10.1016/j.compchemeng.2013.04.019.

Iaiani, M., Tugnoli, A., Bonvicini, S., Cozzani, V., 2021a. Analysis of cybersecurity-related incidents in the process industry. Reliab. Eng. Syst. Saf. 209. https://doi.org/10.1016/j.ress.2021.107485.

Iaiani, M., Tugnoli, A., Bonvicini, S., Cozzani, V., 2021b. Major accidents triggered by malicious manipulations of the control system in process facilities. Saf. Sci. 134, 105043 https://doi.org/10.1016/J.SSCI.2020.105043.

Iaiani, M., Tugnoli, A., Macini, P., Cozzani, V., 2021c. Outage and asset damage triggered by malicious manipulation of the control system in process plants. Reliab. Eng. Syst. Saf. 213, 107685 https://doi.org/10.1016/j.ress.2021.107685.

Iaiani, M., Tugnoli, A., Cozzani, V., 2022. Risk identification for cyber-attacks to the control system in chemical and process plants. Chem. Eng. Trans. 90, 409–414. https://doi.org/10.3303/CET2290069.

International Society of Automation (ISA), International Electrotechnical Commission (IEC), 2018. ISA/IEC 62443 Series of Standards: Industrial Automation and Control Systems Security.

Kaspersky and ARC Advisory Group, 2020. The State of Industrial Cybersecurity in the Era of Digitalization.

Khan, F., Amyotte, P., Adedigba, S., 2021. Process safety concerns in process system digitalization. Educ. Chem. Eng. 34, 33–46. https://doi.org/10.1016/J.ECE.2020.11.002.

Kopbayev, A., Khan, F., Yang, M., Halim, S.Z., 2022. Fault detection and diagnosis to enhance safety in digitalized process system. Comput. Chem. Eng. 158, 107609 https://doi.org/10.1016/J.COMPCHEMENG.2021.107609.

Landucci, G., Reniers, G., 2019. Preface to special issue on quantitative security analysis of industrial facilities. Reliab. Eng. Syst. Saf. 191, 106611 https://doi.org/10.1016/j.ress.2019.106611.

Lee, R.M., Assante, M.J., Conway, T., 2014. ICS CP/PE (Cyber-to-Physical or Process Effects) case study paper – Media report of the Baku-Tbilisi-Ceyhan (BTC) pipeline Cyber Attack.

Mannan, S., 2012. Lees' Loss Prevention in the Process Industries: Hazard Identification, Assessment and Control, 4th ed. Elsevier, UK: Butterworth-Heinemann.

Matteini, A., Argenti, F., Salzano, E., Cozzani, V., 2019. A comparative analysis of security risk assessment methodologies for the chemical industry. Reliab. Eng. Syst. Saf. 191. https://doi.org/10.1016/j.ress.2018.03.001.

Paulsen, C., Byers, R., 2019. NISTIR 7298 Rev. 3: Glossary of Key Information Security Terms. ⟨https://doi.org/10.6028/NIST.IR.7298r3⟩.

Reniers, G., 2011. Terrorism security in the chemical industry: results of a qualitative investigation. Secur. J. 24, 69–84. https://doi.org/10.1057/sj.2009.10.

Robertson, J., Turton, W., 2021. Colonial Hackers Stole Data Thursday Ahead of Shutdown - Bloomberg [WWW Document]. Bloom. News. URL ⟨https://www.bloomberg.com/news/articles/2021–05-09/colonial-hackers-stole-data-thursday-ahead-of-pipeline-shutdown⟩ (accessed 10.13.22).

Stouffer, K., Falco, J., Scarfone, K., 2008. Guide to Industrial Control Systems (ICS) Security.

Sun, H., Wang, H., Yang, M., Reniers, G., 2022. A STAMP-based approach to quantitative resilience assessment of chemical process systems. Reliab. Eng. Syst. Saf. 222, 108397 https://doi.org/10.1016/J.RESS.2022.108397.

The ARIA Database - La référence du retour d'expérience sur accidents technologiques [WWW Document], 2022. URL ⟨https://www.aria.developpement-durable.gouv.fr/the-barpi/the-aria-database/?lang=en⟩ (accessed 12.8.20).

Thomas, H.W., Day, J., 2015. Integrating Cybersecurity Risk Assessments Into the Process Safety Management Work Process. 49th Annual Loss Prevention Symposium 2015, LPS 2015 - Topical Conference at the 2015 AIChE Spring Meeting and 11th Global Congress on Process Safety, pp. 360–378.

Tukey, J.W., 1977. Exploratory Data Analysis. Addison-Wesley.

Ylönen, M., Tugnoli, A., Oliva, G., Heikkilä, J., Nissilä, M., Iaiani, M., Cozzani, V., Setola, R., Assenza, G., van der Beek, D., Steijn, W., Gotcheva, N., Del Prete, E., 2022. Integrated management of safety and security in Seveso sites - sociotechnical perspectives. Saf. Sci. 151, 105741 https://doi.org/10.1016/J.SSCI.2022.105741.

Zinetullina, A., Yang, M., Khakzad, N., Golman, B., Li, X., 2021. Quantitative resilience assessment of chemical process systems using functional resonance analysis method and Dynamic Bayesian network. Reliab. Eng. Syst. Saf. 205, 107232 https://doi.org/10.1016/j.ress.2020.107232.