Process Safety and Environmental Protection 176 (2023) 226–237

Contents lists available at ScienceDirect

Process Safety and Environmental Protection

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

Process hazard and operability analysis of BPCS and SIS malicious manipulations by POROS 2.0

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
Hazard identification
Chemical and process industry
Methodology
Cyber-attack

ABSTRACT

The increasing interconnectivity with external networks and the higher reliance on digital systems make the facilities of the chemical, process, and Oil&Gas industry more vulnerable to cyber-attacks. These attacks have the potential of causing events with severe consequences on property, people, and the surrounding environment such as major event scenarios. The application of the currently available methodologies for cyber risk identification to complex plants with a large number of units may be demanding and cumbersome. The present study proposes an updated methodology, named POROS 2.0, that allows reducing time and effort in application by limiting the scope of the analysis to relevant cybersecurity scenarios. The latter are identified by investigating the potential escalation of consequences propagating among process and/or utility nodes of the manipulations of BPCS and SIS, similar to what is done in the HazOp technique in the safety domain. POROS 2.0 was demonstrated by the application to a case study addressing a fixed offshore platform for gas exploitation.

1. Introduction

With the increasing reliance on digital systems for the control and operation of industrial processes, chemical and process plants have become more vulnerable to cyber threats, including unauthorized accesses, data breaches, and manipulation of systems (Center for Chemical Process Safety, 2022; Stouffer et al., 2015). These types of attacks when accessing the OT (Operational Technology) system of the targeted facility (e.g., the BPCS – Basic Process Control System – and the SIS – Safety Instrumented System) can result in the release of hazardous chemicals, disruptions to production processes, and the potential for environmental damage (Iaiani et al., 2022; Khan et al., 2021).

In recent years, there have been a number of high-profile incidents involving cyber-attacks on chemical and process plants, including the Oil&Gas industry (Iaiani et al., 2021a). The ransomware attack on Colonial Pipeline in the USA, which occurred on May 7th, 2021, serves as a notable example (Bing, Kelly, 2021). In that case, the cyber criminals accessed the CP billing system and stole 100 GB of sensitive data (Robertson and Turton, 2021). To prevent the attackers from accessing the control and safety systems (OT system), the operators in the control room activated the pipeline shutdown, leading to significant economic losses and widespread fuel shortages at refineries, airports, and gas stations due to a 6-day production interruption. The explosion of the BTC (Baku-Tbilisi-Ceyhan) pipeline in 2008 is another noteworthy historical evidence of the potential severity of consequences of cyber-attacks on critical infrastructures (The Repository Of Industrial Security Incidents, 2015): the incident resulted in significant environmental damages, including soil and water pollution, and impacted local communities, wildlife, and crops (Lee et al., 2014).

Two fundamental assessments shall be carried out to evaluate the cyber risk in chemical and process facilities: vulnerability assessment and threat assessment (Center for Chemical Process Safety, 2022). The

Abbreviations: APS, Active/Procedural Safeguard; BPCS, Basic Process Control System; CM, CoMbination of local consequences; CMA, Category of Mechanism of Action; EC, loss of Economic value; EN, loss of ENvironmental value; HazOp, Hazard and Operability analysis; HV, loss of Human Value; IACS, Industrial Automation and Control System; IPS, Inherent/Passive Safeguard; IT, Information Technology; IV, loss of Influence Value; LC, Local Consequence; LOC, Loss Of Containment; LPI, Loss of Physical Integrity; MA, Mechanism of Action; ME, Manipulative Element; ND, NoDe; OT, Operational Technology; P&ID, Piping & Instrumentation Diagram; PFD, Process Flow Diagram; PID, Proportional-Integral-Derivative; PLC, Programmable Logic Controller; POROS, Process Operability analysis of Remote manipulations through the cOntrol System; PSV, Pressure Safety Valve; RM, Remote Manipulation; RMC, Remote Manipulable Component; SDV, Shut Down Valve; SE, Security Event; SIS, Safety Instrumented System.

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

https://doi.org/10.1016/j.psep.2023.06.024
Received 21 March 2023; Accepted 7 June 2023
Available online 8 June 2023

vulnerability assessment consists in the evaluation of the potential weaknesses (or vulnerabilities) that can be exploited by an attacker to gain access to the target system and perform the required actions: this includes the analysis of hardware and software configurations, network architecture, and the identification of any potential entry points. Differently, threat assessment consists in the identification and evaluation of the potential impacts of a cyber-attack on the physical process system, including the release of hazardous chemicals and disruptions to production processes. The results obtained from the vulnerability and threat assessments in terms of the likelihood and severity of a specific cybersecurity scenario can be combined into a value of the cyber risk related to such scenario.

The evaluation of the cyber risk is qualitatively or semi-quantitatively addressed by the classical Security Vulnerability/Risk Assessment (SVA/SRA) methodologies that have been proposed in the last two decades by professional organizations and governmental authorities (Matteini et al., 2019). Examples of such methodologies are the CCPS methodology (Center of Chemical Process Safety CCPS, 2003), the VAM-CF methodology (Jaeger, 2002), the SRA methodologies proposed by API RP 780, API RP 70, and API RP 70I American Petroleum Institute (API), 2012; American Petroleum Institute API, 2010; American Petroleum Institute API, 2013, and the RAMPCAP methodology (Moore et al., 2007). However, these methodologies are not specifically aimed at assessing the cyber threat, which is typically dealt with simplified assumptions based on expert judgement or historical evidence: no specific tools for cyber risk identification and evaluation are provided.

On the contrary, the particular issue of cybersecurity of Industrial Automation and Control Systems (IACS, such as BPCS and SIS) is covered by the ISA/IEC 62443 series of standards (International Society Of Automation ISA, 2018). It provides a comprehensive framework for the secure design, implementation, and operation of industrial control systems and networks, including those used in chemical and process plants. The standard covers key areas such as access control, incident management, and risk assessment, and is designed to help organizations to protect against cyber threats and maintain the security and reliability of their critical infrastructure. However, the standard lacks in providing tools and approaches for the systematic identification of the cybersecurity scenarios of concern, mostly basing the analysis on expert judgment and historical evidence.

Methods addressing cybersecurity issues of OT systems in chemical and process facilities were developed over the years by professional organizations, governmental authorities, and academic institutions, mostly varying in the application domain, scope, and theoretical framework: an extended review of these approaches can be found in Cherdantseva et al. (2016). Some of these methods make use of Bow-Tie approach (Abdo et al., 2018; Byres et al., 2004), Process Hazard Analysis (PHA) (Cusimano and Rostick, 2018), and diagraph model (Guan et al., 2011), some other are step-by-step procedures with a backbone structure very similar to that of SVA/SRA methodologies (Gertman et al., 2006; Song et al., 2012), while other methodologies are not based on approaches that are well-known in the safety and security domains (Beggs and Warren, 2009; Hashimoto et al., 2013). However, as discussed in Iaiani et al. (2021c), most of these approaches present limitations concerning systematicity and reproducibility, especially regarding the identification of the impacts that can be triggered by a malicious manipulation of the OT system. Thus, specific assessments addressing cyber risk identification in chemical, process, and Oil&Gas facilities, able to investigate the role that physical and instrumented safety barriers may play during the attack, are needed, and as evidenced by Ylönen et al. (2022), these approaches shall address the potential synergies with the safety domain in order to manage in an integrated way all the risks that can arise in a critical infrastructure processing and/or storing hazardous materials (e.g., EU Seveso establishments).

To this purpose, previous studies of the authors provided two rigorous methodologies, PHAROS – Process Hazard Analysis of Remote manipulations through the cOntrol System – methodology (Iaiani et al., 2021b) and POROS – Process Operability Analysis of Remote manipulations through the cOntrol System – methodology (Iaiani et al., 2021c). These methodologies allow for the systematic identification of the relevant sets of manipulations of the BPCS and SIS that can trigger major accident scenarios (PHAROS) and/or production outage scenarios (POROS) in a chemical and process facility. This output, combined with the knowledge obtained through the analysis of past cybersecurity-related incidents (Iaiani et al., 2021a), can be used to develop integrated cybersecurity scenarios of concern in terms of type of attacker, system affected, impacts of cyber-attacks, manipulations required to initiate such impacts, and cybersecurity countermeasures potentially effective in contrasting such attacks, as required by the ISA/IEC 62443 series of standards. The synergic framework is presented in Iaiani et al. (2023).

However, the application of PHAROS and POROS methodologies to case studies proved that in case of complex plants with large number of process and utility nodes, the analysis could be cumbersome and sometimes ineffective in identifying all the consequences of the manipulations beyond the node in which they are initially generated. To overcome this limitation, the present study proposes an updated version of the methodologies, named POROS 2.0 methodology, which includes a procedure for systematically addressing the analysis of the propagation of the effects of manipulations between process and/or utility nodes in a plant (similar to what is done in an HazOp study in the safety domain), allowing to catch the potential escalation of consequences throughout the plant. In this way, time and effort in application is reduced by focusing the analysis on relevant cybersecurity scenarios, whose credibility is estimated based on the plant knowledge level required by the attacker and the cyber complexity of the manipulations to be performed. The proposed methodology can be used to identify major accident scenarios (scope of old PHAROS methodology) or also production outage scenarios (scope of old POROS methodology) encompassing the scope of the analysis of both former methods.

In the following, POROS 2.0 methodology is described in Section 2, while is applied to an illustrative case study (fixed offshore platform for gas exploitation and processing) in Section 3. The results obtained are discussed in Section 4 and conclusions are drawn in Section 5.

2. POROS 2.0 methodology

POROS 2.0 methodology is a systematic rigorous step-by-step procedure (8 steps, see the flowchart in Fig. 1) that is designed for application either in the front-end design phase of new plants or in the security review of operating facilities for chemical and process plants. Similarly to the HazOp technique, it is performed by a team with technical knowledge on the physical process system, control system, and safety system. No specific IT skills are required by the team.

The proposed methodology addresses the identification of both the major event scenarios and the production outage scenarios. As such, it encompasses in one method the scope of both former PHAROS and POROS methodologies. Unlike in the two previous methodologies, these scenarios are identified through the systematic analysis of the propagation of the effects of manipulations between the nodes of the process/utility system, similar to what is done in an HazOp study in the safety domain. This allows to catch the potential escalation of the consequences of the events generated by the malicious manipulation of the Basic Process Control System (BPCS) and the Safety Instrumented System (SIS), and thus to estimate the real impact of such scenarios in the entire plant and not only in the specific node where the attack was addressed. Possible cut-off criteria are suggested to limit the scope of the analysis on the cybersecurity scenarios of major concern, reducing time and effort in application in comparison to former methods.

In order to support more effectively the allocation of the resources for risk mitigation on the most credible cybersecurity scenarios of concern, the concept of credibility was introduced in POROS 2.0 methodology, based on the level of knowledge of the plant that an

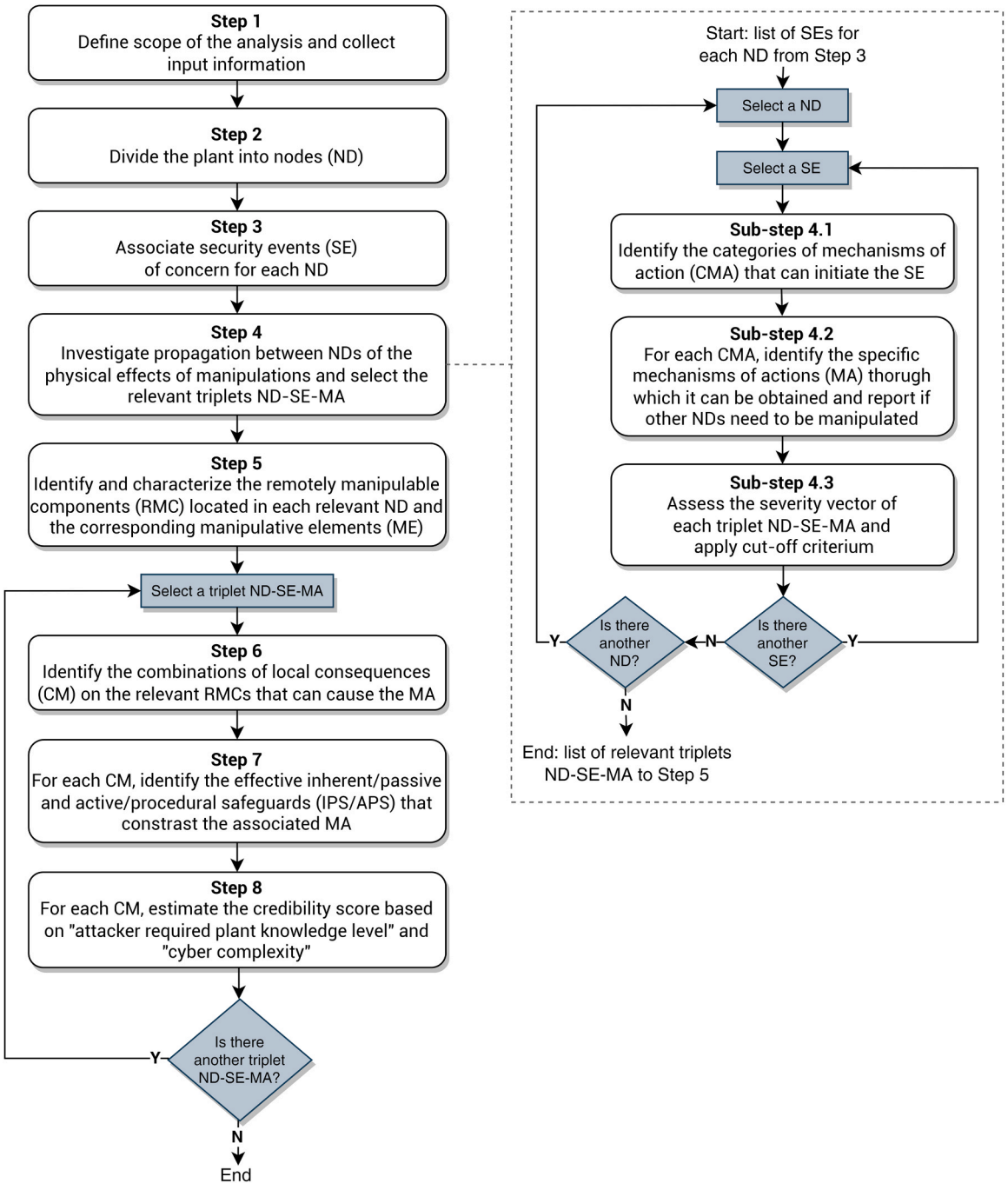

Fig. 1. Flowchart of POROS 2.0 methodology.

attacker needs in order to trigger a given scenario and on the cyber complexity of the manipulations required to initiate it. This provides a further chance of cut-off of the scenarios. The information on credibility can be used, for example, to support the division of the OT system into zones (grouping of cyber assets that share the same requirements) as suggested by the ISA/IEC 62443 series of standards: e.g., elements that require to be manipulated in a high-credibility cybersecurity scenario shall be in different zones of the OT system (more complex attack path for the attackers).

In particular, POROS 2.0 methodology provides the following outputs:

- List of the security events (SE, such as loss of containment, integrity damage, outage, etc.) on the physical process system that can be caused by manipulation of BPCS and SIS;
- Severity vector associated with each SE reporting the severity score associated to four key domains (loss of economic value, loss of influence value, loss of environmental value, loss of human value);
- Sets of BPCS and SIS components that need to be manipulated in order to trigger each SE, how they shall be manipulated, and the physical consequences on remotely manipulable components (RMC) in the physical process system;
- List of the Active/Procedural safeguards (APS) in place that may prevent/mitigate the attack;
- List of the Inherent/Passive safeguards (IPS) in place that may prevent/mitigate the attack;

- Credibility score of each attack, based on the attacker required plant knowledge level and the cyber complexity of the manipulations required to carry it out.

Therefore, POROS 2.0 can be used to identify, in a systematic way, the cybersecurity scenarios that are relevant in the context of cyber risk assessment, addressing the specificity of the physical process system under analysis. POROS 2.0 methodology is based on a reverse HazOp concept, which is graphically represented in Fig. 2. The analysis starts from the selection of the security events (SE) of concern for the physical process system under assessment (e.g., loss of containment (LOC) of hazardous material) and, subsequently, it provides for the identification of the specific mechanisms of action (MA) through which such SEs can be initiated (e.g., inducing excessive pressure in a vessel) and the corresponding sets of physical changes on the remotely manipulable components of the plant (RMC) that are required to perform each MA (e.g., closing of a valve + increased rotational speed of a compressor). Each set of physical changes on RMCs forms a combination of manipulations (CM). Active/Procedural safeguards (APS, e.g., ESD/PSD/LSD logic) and Inherent/Passive safeguards (IPS, e.g., pressure safety valves - PSV) potentially effective against each CM, are eventually identified.

In the following, each of the 8 steps of POROS 2.0 is described.

In Step 1 of POROS 2.0 methodology (see Fig. 1) the scope of the analysis is defined. The latter can be on major accident scenarios only (scope of former PHAROS methodology) or including also operability issues (scope of former POROS methodology). The possibility of adopting cut-off criteria to focus the analysis on a limited number of cybersecurity scenarios of concern shall be defined at this step. Such criteria concern a cut-off on the severity of consequences (e.g., do not consider scenarios with low-impact on people, assets, environment, and/or reputation) and/or the credibility of the scenario in being realized (e.g., eliminate low-credibility scenarios). Once the scope is defined, the input information is collected. This includes the hazardous characteristics of the substances processed and/or stored in the plant under assessment, the Process Flow Diagram (PFD), the Heat and Mass (H&M) balances, the Piping and Instrumentation Diagram (P&ID), the operating and design conditions of each equipment unit, and the control and safety logics of the BPCS and SIS.

In Step 2 of POROS 2.0 methodology (see Fig. 1) the plant is divided into nodes (ND). Only the nodes where hazardous materials are processed and/or stored are of concern in case the scope of the analysis is limited to major accident scenarios, otherwise also the utility nodes are of interest in the assessment. Guidelines supporting plant division into nodes can be found in Iaiani et al. (2021c).

In step 3 of POROS 2.0 methodology (see Fig. 1) the compatible security events (SE) are identified for each selected ND. A SE is intended as an undesired event that affects the operability and/or the physical integrity of the physical process system under assessment. A loss of containment (LOC) or a loss of physical integrity (LPI) involving a hazardous material are of concern in case the scope of the analysis is limited to major accident scenarios, while undesired events such as stop of plant operation and operation out of specification are also considered if the scope covers operability issues. The reader is referred to Table A.1 in the Supplementary Material where a list of possible SEs is provided.

In Step 4 of POROS 2.0 methodology (see Fig. 1) the propagation between NDs of the physical effects of manipulations is investigated and the scenarios relevant for security risk assessment are selected. This step, not systematized in the former PHAROS and POROS methodologies, allows to analyze the interdependencies between nodes (similar to what is done in a HazOp study (International Electrotechnical Commission, 2016) for propagation of deviations), enabling to catch potential escalation of the consequences of the actions carried out by an attacker in a node. In fact, a low-severity security event occurring in a ND may initiate a high-severity security event in another ND due to nodes interdependencies. Therefore, investigating these interdependencies allows to identify those scenarios that have, in the node where they occur or in other nodes of the plant, high-severity consequences, and thus to limit the analysis on those scenarios that are relevant in the context of security risk assessment, making it less demanding. The relevant scenarios are defined in terms of the triplet node - security event - mechanism of action (ND-SE-MA).

To guide the systematic application, this step has been divided in 4 sub-steps (steps 4.1–4.3 in Fig. 1), which shall be carried out for each node.

Sub-step 4.1 consists in the identification of the categories of mechanisms of action (CMA) for each SE associated to the ND under assessment. CMAs are general mechanisms, based on a hypothetical facility, that can initiate a security event: reference categories of mechanisms of action (CMA) are proposed in Table A.1 in the Supplementary Material. For example, “damage of the construction material of the containment system” is a possible generic CMA that initiates a LOC of a hazardous material (which is the SE).

Sub-step 4.2 consists in the identification of the specific mechanisms of action (MA) through which each CMA can be obtained in the plant analysed and the ND where such MA shall be carried out. MAs are specific mechanisms (based on the features of the plant analysed) that can initiate a security event. For example, “inducing high pressure in the separator” is a possible MA which can be grouped into the CMA mentioned above initiating a LOC. It is important to underline that, in some cases, in order to obtain a CMA, it is possible that MAs carried out in nodes different from the one under assessment are required: in this case the information is propagated from a node to another similarly to deviations propagating among different nodes in a traditional HazOp study (e.g., more flowrate in a stream of a node causes high level in an equipment unit in a nearby node). Once this sub-step has been carried out, for each SE of each ND, all the possible MAs initiating the SE are listed with reference to the node where they shall occur.

Sub-step 4.3 consists in the assessment of the severity vector associated with each triplet ND_i-SE_j-MA_k in the node under assessment. The severity vector evaluates the impact of SE_j initiated by MA_k in ND_i using four severity levels: minor (1), medium (2), major (3), and extensive (4). The severity is based on four target values according to Center For Chemical Process Safety (2011) and Hausken (2018): economic value (EC), influence value (IV), environmental value (EN), and human value (HV). The severity scale is provided in Table A.2 in the Supplementary Material. Therefore, the severity vector for each triplet ND-SE-MA is in the form [EC, IV, EN, HV]. The loss of economic value is calculated by adding direct and indirect costs. The loss of human value includes both

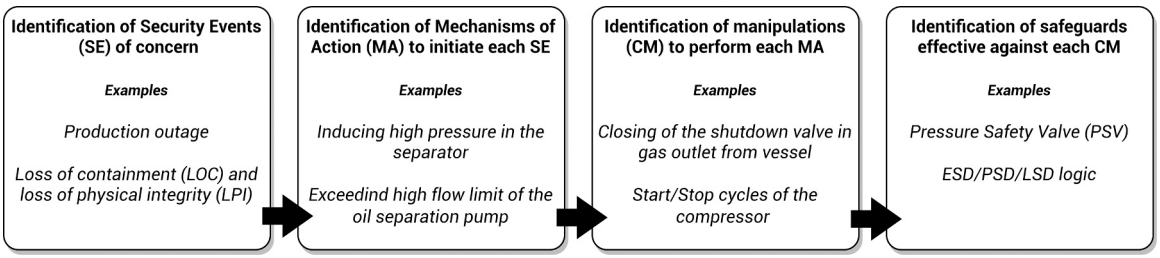

Fig. 2. Reverse HazOp concept in POROS 2.0 application.

physical injuries and fatalities. The loss of influence value is closely tied to reputation. The loss of environmental value accounts for the long- or short-term effects on the physical environment requiring environmental remediation.

It is important to underline that the severity vector for each triplet ND_i-SE_j-MA_k shall be estimated considering the effect that SE_j initiated through MA_k has in the entire plant, not only in the specific node where it occurs. In other words, when estimating the severity level for EC, IV, EN, and HV for a triplet, the interdependencies among the nodes investigated in the previous sub-step shall be taken into account.

Sub-step 4.3 provides also for the selection of the relevant triplets ND-SE-MA. A straightforward cut-off criterium that prioritizes SEs with the most severe impact (i.e., a severity level of 3 or higher for at least one target value) is suggested. However, alternative cut-off criteria may be appropriate, especially when considering well-defined cyber threat sources or specificities of the facility analysed.

Once all the sub-steps from 4.1 to 4.3 have been applied, a list of high-severity scenarios that can be initiated by remote manipulations of the BPCS and the SIS in the physical process system analysed, is provided in the form of triplets ND-SE-MA. The following steps (i.e., steps from 5 to 8 in Fig. 1) are then limited in the scope to these scenarios, strongly reducing the effort that shall be spent for application with respect to former PHAROS and POROS methodologies.

In Step 5 of POROS 2.0 methodology (see Fig. 1), the remotely manipulable components (RMC) located in the nodes where relevant scenarios may occur (i.e., the NDs that appear in the relevant triplets ND-SE-MA selected in the previous step) and their manipulative elements (ME) are identified and characterized. RMCs are the physical objects in the plant whose operation is regulated by the BPCS and the SIS (e.g., automatic control and shut-off valves, pumps, compressors, etc.), while MEs are the elements of the BPCS and the SIS that regulate RMCs (e.g., PID and PLC controllers and their logics). The reader is referred to Iaiani et al. (2021c) where a list of typical RMCs and corresponding MEs in chemical and process plants is provided.

Characterization of MEs consists in the identification of the remote manipulations (RMs) that an attacker can carry out on them such as changing the setpoint of a PID (Proportional-Integral-Derivative) controller or reprogramming the functions of a PLC (Programmable Logic Controller). Analogously, characterization of RMCs consists in the identification of the physical changes that occur on them as a consequence of RMs on the ME by which the RMCs are regulated, named local consequences (LC). The reader is referred to Iaiani et al. (2021c) where examples of RMs on categories of MEs and related LCs on categories of RMCs are provided.

In Step 6 of POROS 2.0 methodology (see Fig. 1) the combinations (CM) of local consequences on the RMCs located in the ND that are required to perform the MA, are identified. Those RMCs that need to be manipulated are called relevant RMCs for the MA.

Steps from 6 to 8 are intended to be performed for each relevant triplet ND-SE-MA selected in Step 4.

In Step 7 of POROS 2.0 methodology (see Fig. 1) the Active/Procedural safeguards (APS) and the Inherent/Passive safeguards (IPS) that can be effective in contrasting the MA, are identified. APSs are automated or human-mediated actions that perform their function through the OT system (e.g., ESD/PSD/LSD logics), while IPSs are safety barriers that are not controlled by the OT system (e.g., Pressure Safety Valves – PSV) and thus can not be manipulated by the attackers in the context of a cyber-attack.

Therefore, the manipulations required by the CM and the deactivation of the APSs contrasting the MA to which the CM refers, constitute a "CM+APS attack action" for the triplet ND-SE-MA. The CM+APS attack action thus results to be the complete set of all the actions that an attacker has to carry out in order to trigger a specific security event in a node through a specific mechanism of action.

In Step 8 of POROS 2.0 methodology (see Fig. 1) the credibility score of each CM+APS attack action associated to the triplet ND-SE-MA under assessment, is evaluated. The score is estimated combining in a matrix a score on two dimensions: the "plant knowledge level" required by the attacker and the "cyber complexity" of the CM+APS attack action. The "plant knowledge level" refers to the level of technical knowledge on the plant under assessment or on similar plants that is required by an attacker to carry out a specific CM+APS attack action. A ranking based on three levels (high, medium, low) is proposed in Table A.3 in the Supplementary Material. The "cyber-complexity" of a CM+APS attack refers to how complex the attack is in terms of the number of relevant RMCs, the number of zones that need to be accessed in the OT system, and whether a specific sequence and timing is required. A ranking based on four levels (high, medium, low, very low) is proposed in Table A.4 in the Supplementary Material. The 4×3 matrix for the combination of the two scores into the total credibility score value of the CM+APS attack action is instead reported in Fig. A.1 in the Supplementary Material. Clearly enough, the credibility score of a triplet ND-SE-MA is the greater among the credibility scores of the CM+APS attack actions associated to it.

The concept of credibility is used to group identified scenarios on the basis of the skills and complexity required for their realization. It also provides a ranking of the CM+APS attack actions that can be used to allocate more effectively the resources for risk mitigation with reference to the most credible sets of manipulations of the BPCS and SIS and, in turn, to the most credible security events.

3. Illustrative case study

3.1. Description of the case study

A fixed offshore platform for gas exploitation and processing is considered in the illustrative application of POROS 2.0 methodology.

Fig. 3 shows the simplified block diagram of the system analyzed. The platform processes fluid from three wells with dual completion through six strings (Well Head System). The gas/water mixture is directed to the Separators System for water separation. The system includes three vertical separators, each operating at wellhead pressure, and one chock valve per string for equalizing pressure. The separated oily-water is sent to the Oily Water Treatment System for degassing and discharge. The natural gas with reduced pressure and with injected glycol to prevent hydrates formation is instead conveyed to the Gas Collector Header and is sent to gas sealine. A low-pressure and a high-pressure vent gather and disperse into the atmosphere both continuous and emergency gas discharges. The Fuel Gas System provides fuel gas to all platform users including the Electrical Generation System and Glycol System. Similarly, the Compressed Air System provides instrument and utility air to all platform users. The Electrical Generation System provides electric power during normal operation. The Drains System collects oily drains, potentially oily water, and rainy water. Tags of equipment units are described in Table 1.

The OT system managing the platform operations is composed by two zones as defined by the ISA/IEC 62443 series of standards: the Basic Process Control System (BPCS) and the Safety Instrumented System (SIS). This means that, once access is obtained by the attacker to one of these zones, he/she can potentially manipulate all the manipulative elements (MEs) within that zone.

4. Results of POROS 2.0 application

Both system integrity and operability issues are of concern for the offshore Oil&Gas platform considered in the illustrative case study. Therefore, both major event scenarios and production outage scenarios are within the scope of POROS 2.0 application in the current example (Step 1, see Fig. 1). However, the scope was limited to scenarios with severe consequences on people, assets, environment, and/or reputation (severity-based cut-off criterium, with severity threshold set to 3 for at least one key domain).

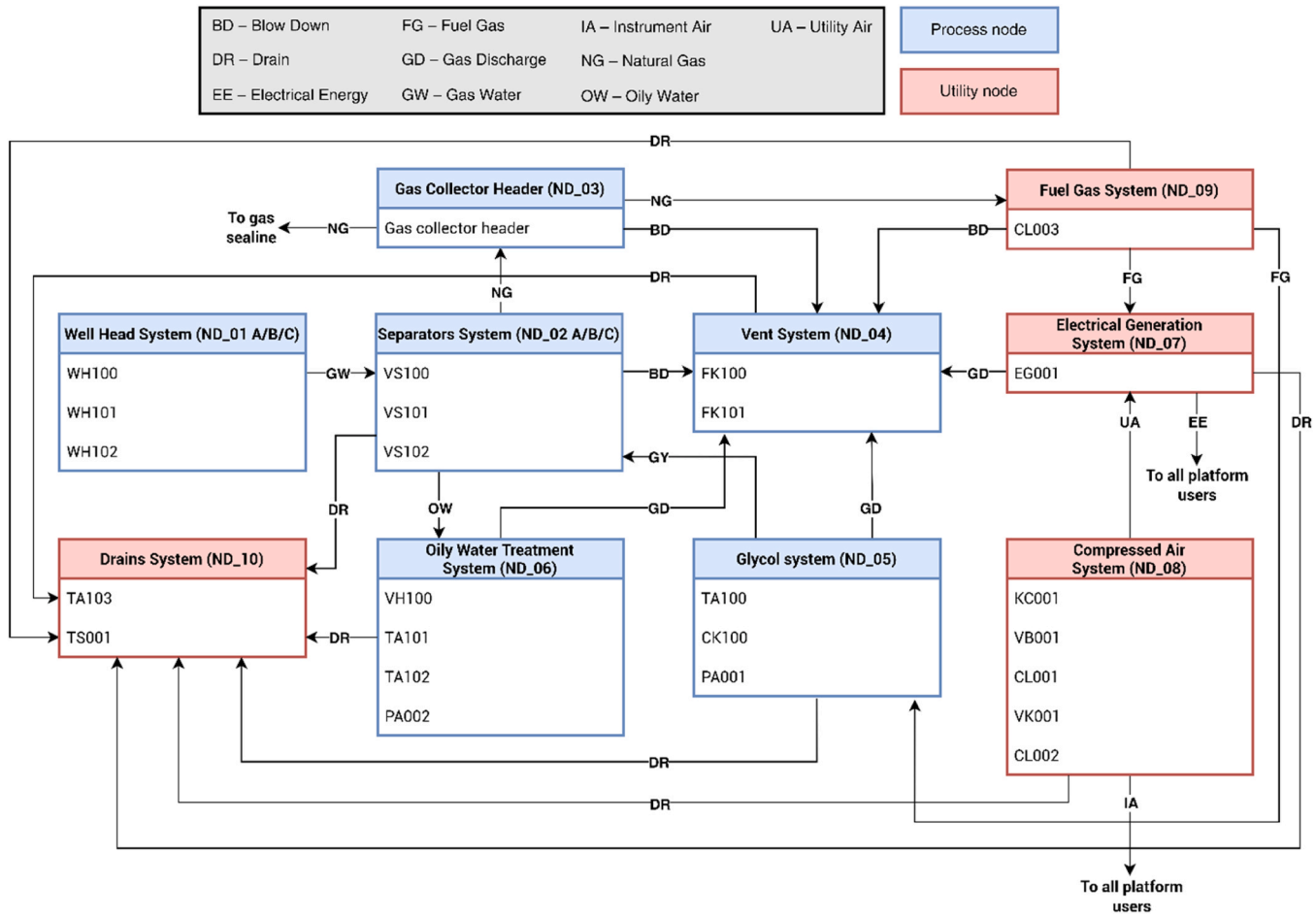

Fig. 3. Block diagram of the offshore Oil&Gas platform considered in the illustrative case study. Tags of equipment units are described in Table 1.

Table 1
Nodes (ND) identified in the application of Step 2 of POROS 2.0 methodology. C.P.: Connecting Pipework.

Node	Type	Equipment items
ND_01 A	Process	Well head WH100; C.P.
ND_01 B	Process	Well head WH101; C.P.
ND_01 C	Process	Well head WH102; C.P.
ND_02 A	Process	Separator VS100; C.P.
ND_02 B	Process	Separator VS102; C.P.
ND_02 C	Process	Separator VS103; C.P.
ND_03	Process	Gas collector header; C.P.
ND_04	Process	HP vent FK100; LP vent FK101; C.P.
ND_05	Process	Glycol storage tank TA100; Glycol filter CK001; Glycol injection pump PA001; C.P.
ND_06	Process	Degasser VH100; Coalescence separator TA101; Oil separation pump PA002; Fresh water tank TA102; C.P.
ND_07	Utility	Electrical generator EG001
ND_08	Utility	Air compressor KC001; Wet air accumulator VB001; Pre filter CL001; Air dryer VK001; Post filter CL002; C.P.
ND_09	Utility	Fuel gas filter CL003; C.P.
ND_10	Utility	Drains recovery tank TA103; Sump Caisson TS001; C.P.

After collecting the needed information (Step 1), the physical process system was divided into nodes (Step 2, see Fig. 1). According to the scope of the analysis, both process and utility nodes were identified following the guidelines reported in Iaiani et al. (2021c), all described in Table 1 in terms of node type (process/utility) and equipment items involved. Process nodes include (see Fig. 1 and Table 1) the Well Head System (ND_01 A/B/C), the Separators System (ND_02 A/B/C), the Gas Collector Header (ND_03), the Vent System (ND_04), the Glycol System (ND_05), and the Oily Water Treatment System (ND_06). Utility nodes include (see Fig. 1 and Table 1) the Electrical Generation System (ND_07), the Compressed Air System (ND_08), the Fuel Gas System (ND_09), and the Drains System (ND_10).

The selection of the security events (SE) of concern for each identified node (Step 3, see Fig. 1) was carried out with the support of the guiding list provided in Table A.1 in the Supplementary Material. In particular, for each ND, the applicability of the SE categories reported in the reference source was checked considering the specificities of the equipment items involved, the function they have in the physical process system, and the characteristics of the substances processed. The obtained sets of SEs for each node are reported in Table B.1 in the Supplementary Material. The six categories considered are: product out of specification (SE01), arrest/blockage of a piece of equipment/item (SE02), activation of ESD (emergency shutdown) / PSD (process shutdown) / LSD (local shutdown) (SE03), exceeding design specification for construction materials (SE04), damage of moving components/machinery (SE05), and loss of containment (LOC) and loss of physical integrity (LPI) (SE06).

It is important to underline that the LOC/LPI security event was selected also for those nodes not processing hazardous substances. In fact, even if this SE may not be relevant for the node itself, it can become so if this node provides a fundamental service for the normal operation of the entire process due to its long-term unavailability (e.g., a utility

node not handling hazardous substances such as the Compressed Air System). This possibility of escalation of consequences due to nodes interdependencies was investigated in the application of Step 4 of POROS 2.0 methodology (see Fig. 1).

With the information on SEs for each ND, application of sub-steps from 4.1 to 4.3 led to the identification of the relevant scenarios in terms of triplets "ND-SE-MA" on which further steps of the analysis will be focused. In particular the categories of mechanisms of action (CMA) for each SE (Sub-step 4.1, see Fig. 1) were selected according to the list provided by Iaiani et al. (2021c). They are reported in the third column of Table B.1 in the Supplementary Material (codes refer to the ones used in the reference source (Iaiani et al., 2021c)). For example, the unavailability of essential services (CMA12) and the direct activation of ESD/PSD/LSD logic (CMA07) are common categories of mechanisms of action that initiate an emergency / process / local shutdown (SE03).

Starting from the selected CMAs, in application of Sub-step 4.2 (see Fig. 1), the specific mechanisms of action (MA) were identified based on the characteristics of the physical process system described in Section 3.1, together with the node where they shall be executed. In fact, some CMAs require mechanisms of action in nodes other than the one under assessment. This way, the interdependencies among the nodes were identified, similar to what is done in a HazOp application in the safety domain. A total of 52 triplets ND-SE-MA were identified. Table 2 reports some examples of such triplets, while the complete list is present in Table B.1 in the Supplementary Material. For example, with reference to Table 2, the category CMA01 (composition/phase out of specification) that initiates security event SE01 (product out of specification) in node ND_03 (Gas Collector Header) requires MA2.1 (inducing liquid fraction in gas outlet stream from separator) in at least one of the nodes ND_02 A/B/C. Another example is that the unavailability of electrical energy (e.g., obtained by damaging the generator through open-close circles of the breakers out of sync, see MA7.3 in Table 2) and of instrument air (e.g., obtained by stopping the air compressor, see MA8.1 in Table 2, or by inducing overpressure in the wet air accumulator to generate a LOC, see MA8.4 in Table 2) activates the process shutdown (PSD), and thus SE03 (activation of ESD/PSD/LSD logic) in all the other nodes.

In order to identify the relevant scenarios, the severity vector in the form [EC, IV, EN, HV] (see Section 2) was evaluated for each triplet ND-

Table 2
Examples of triplets ND-SE-MA among the ones identified in application of Steps 3 and 4 (the complete list is provided in Table B.1 in the Supplementary Material).

Node	SE (Step 3)	CMA (Step 4.1)	MA (Step 4.2)	Manipulation in (Step 4.2)	Expected consequences (Step 4.3)	Severity vector (Step 4.3)
ND_02 A (B/C)	SE01 - Product out specification	CMA01 - Phase out of specification	MA2.1 - Inducing liquid fraction in gas outlet stream from separator	ND_02 A (B/C)	No direct economic impact on ND_02 A/B/C; no damage to reputation, environment, and people.	[1;1;1;1]
	SE03 - Activation of ESD/PSD/LSD logic	CMA12 - Unavailability of essential services	Inducing electrical energy (EE) unavailable by manipulating ND_07 (e.g., see MA7.3)	ND_07	See ND_07-SE05-MA7.3	See ND_07-SE05-MA7.3
			Inducing instrument air (AI) unavailable by manipulating ND_08 (e.g., see MA8.1 and MA8.4)	ND_08	See ND_08-SE02-MA8.1 and ND_08-SE06-MA8.4	See ND_08-SE02-MA8.1 and ND_08-SE06-MA8.4
ND_03	SE01 - Product out specification	CMA01 - Composition/ Phase out of specification	Inducing liquid fraction in gas outlet streams from separators by manipulating ND_02 A/B/C (e.g., see MA2.1)	ND_02 A (B/C)	See ND_02-SE01-MA2.1	See ND_02-SE01-MA2.1
ND_06	SE01 - Product out specification	CMA01 - Composition/ phase out of specification	MA6.1 - Inducing oil fraction out of spec. in oil-free water stream to sea	ND_06	Costs of total losses between $1MM - $10 MM (costs between $1MM - $2.5MM for environmental remediation); significant damage to the regional reputation; no damage to people.	[3;2;3;1]
			MA6.2 - Inducing gas in oil-free water stream to sea	ND_06	Costs of total losses between $1MM - $10MM (cost less than $1MM for environmental remediation); significant damage to the regional reputation; no damage to people.	[3;2;2;1]
	SE06 - Loss of containment (LOC) and loss of physical integrity (LPI)	CMA23 - Damage of the construction material of the containment system (see SE04)	MA6.5 - Inducing excessive pressure in the coalescence separator	ND_06	Production outage: recovery requires repair and replacement of the coalescence separator (expected downtime of 4 weeks); potential damage to the regional reputation; no damage to environment (catch basin) and people.	[4;2;1;1]
ND_07	SE05 - Damage of moving components/ machinery	CMA18 - Inducing component failure of moving systems	MA7.3 - Inducing open-close circles of the breakers out of sync	ND_07	Production outage: recovery requires repair and replacement of the generator (expected downtime of 2 weeks); potential damage to the regional reputation; no damage to environment and people.	[3;2;1;1]
ND_08	SE02 - Arrest/ blockage of a piece equipment/item	CMA05 - Motor or driver arrest	MA8.1 - Stop of air compressor	ND_08	Production outage: recovery requires normal start-up procedures (expected downtime of 4 h); no damage to reputation, environment, and people.	[2;1;1;1]
	SE06 - Loss of containment (LOC) and loss of physical integrity (LPI)	CMA23 - Damage of the construction material of the containment system (See SE04)	MA8.4 - Inducing high pressure in wet air accumulator	ND_08	Production outage: recovery requires repair and replacement of the wet air accumulator (expected downtime of 4 weeks); significant potential damage to the regional reputation; no damage to environment and people.	[4;2;1;1]

SE-MA previously identified and a severity-based cut-off criterium was applied (Sub-step 4.3 in Fig. 1). The results are shown in the sixth column of Table B.1 in the Supplementary Material. Table 2 reports the reasoning under the choice of the severity levels for EC, IV, EN, HV for some of the identified triplets ND-SE-MA. For example, a severity vector [4,2,1,1] was estimated for the triplet ND_06-SE06-MA6.5 (see Table 2). In fact, with an average economic loss of $25′000 per hour of operations outage, the formation of a breach in the coalescence separator (LOC) causes a damage of about $17MM due to platform downtime (about 4 weeks). Therefore, even without considering the cost of repair/replacement of the separator, a severity level of 4 was selected with regard to the loss of economic value (EC) according to the scale proposed in Table A.2 in the Supplementary Material. It shall be noted as this represents a relevant escalation of severity in comparison to the local consequence (i.e., damage to coalescence separator) which would have been scored as 2 for EC (cost of repair/replacement of the unit of about $0.5MM) and therefore eliminated according to the adopted cut-off criterium; this stresses one more time the value of the systematic approach proposed by the present methodology. A severity level of 2 was instead evaluated for the loss of influence value (IV) as the scenario considered may affect the regional reputation. For both the loss of environmental value (EN) and loss of human value (HV), a severity level of 1 was considered as the liquid release is contained in the deck floor and, typically, there are no people on the platform (the latter is unmanned, but personnel for e.g. maintenance operations may be present). With similar considerations, all the severity vectors were estimated.

Triplets ND-SE-MA with a severity level of 3 or 4 for at least one target value (EC, IV, EN, HV) were selected as relevant for the offshore platform under assessment (severity-based cut-off criterium). In particular, a total of 29 out of 52 triplets were considered relevant: the reader is referred to Table B.1 in the Supplementary Material (seventh column) where the information whether a triplet was selected or not is reported.

The remotely manipulable components (RMC) that are present in the nodes where relevant scenarios may occur (i.e., the nodes of the selected triplets ND-SE-MA) were then identified and characterized together with their corresponding manipulative elements (ME) of the BPCS and SIS (Step 5 in Fig. 1). MEs were characterized in terms of remote manipulations (RM), while RMCs were characterized in terms of local consequences (LC) caused by such RMs. For the sake of brevity and for illustrative purposes, in the following only the results obtained for ND_06 (Oily Water Treatment System) are shown and discussed. The simplified P&ID of the node is shown in Fig. 4. The system is fed in discontinuous mode (based on the separators level control valves operation) by the oily-water phase separated in the separators VS100, VS101, and VS102. First, the fluid is routed to the degasser VH100 where the entrained gas is separated, and then flows by gravity to the hydrocarbon separation section. The coalescence separator TA101 achieves the oil phase separation due to the difference in density between the oil and the water phases. The oil-free water is routed by the pump PA002 to the oil content analyser AT100: if the concentration is acceptable (below a specific threshold value), the water is discharged into the sea, otherwise the water is sent back to the degasser by means of the three-way valve SDV104. A conductivity sensor measures the thickness of the oil buffer in the dome of the oil separator TA101: when the corresponding level is reached it transmits a signal to the electric switching system, changing the rotation direction of the oil separation pump. The pump will draw fresh water from the fresh water tank TA102 and will sent it to the coalescence separator, pushing out the oil buffer towards closed drains system.

The RMCs that were allocated to node ND_06 and the corresponding manipulative elements (ME) are reported in Table 3. The table also reports the remote manipulations (RM) that can be carried out by an attacker to each ME and the local consequences (LC) that are caused by such RMs on the controlled RMCs. For example, the on-off control valves LV100, LV101, and LV102 (see Fig. 4), failing in the close position (FC), close as a consequence of a signal shutdown to the BPCS controllers through which they are regulated.

Starting from the list of characterized RMCs, the combination of local consequences (CM) that can cause each MA in the selected triplets were identified (Step 6 in Fig. 1). For illustrative purposes, Table 4 shows the results obtained for the triplets ND_06-SE01-MA6.1 and ND_06-SE01-MA6.2 which consist in the discharge in the sea of the oil-free water with oil fraction out of specification and with natural gas respectively (severity vector of [3,2,3,1] and [3,2,2,1] respectively, see Table 2), and the triplet ND_06-SE06-MA6.5, consisting in the loss of containment from the coalescence separator TA101 by inducing internal excessive pressure (severity vector of [4,2,1,1], see Table 2). For example (see Table 4), CM6.2.1 consists in the opening of the level control valves LV100, LV101, and LV102 by changing the level thresholds with which the on-off controllers are set, plus the starting of pump PA002 in the

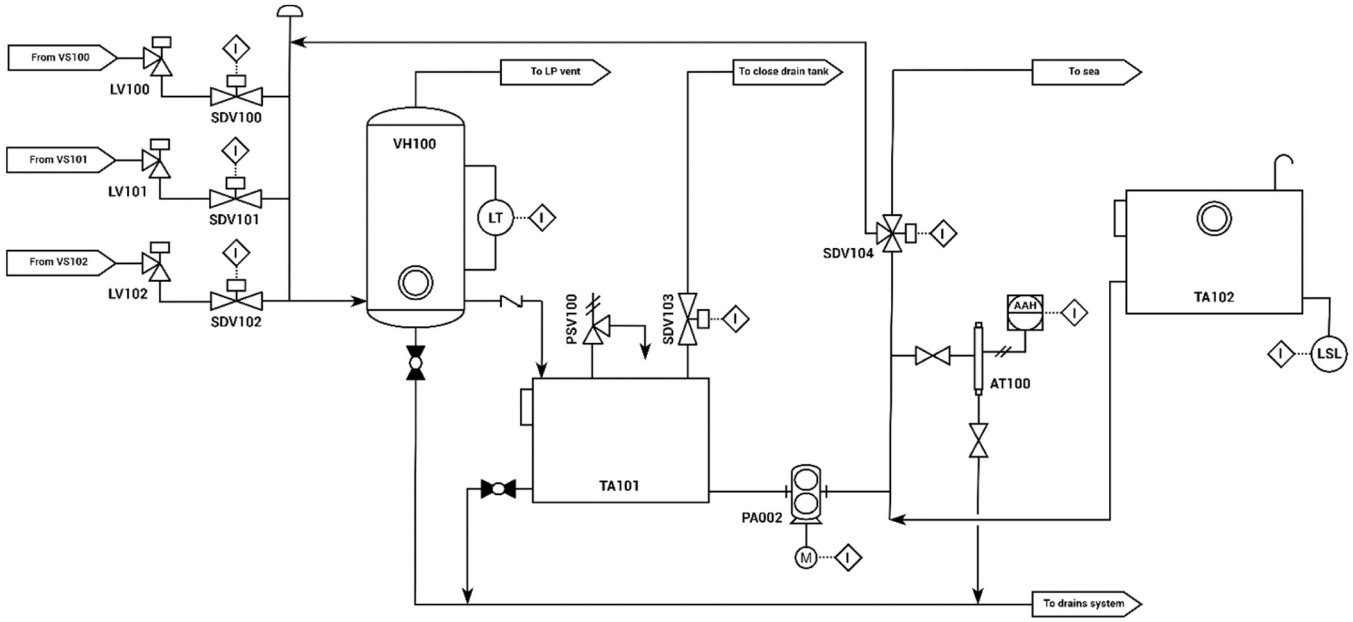

Fig. 4. Simplified P&ID of node ND_06 (Oily Water Treatment System). Equipment tags are defined in Table 1.

Table 3
Remotely manipulable components (RMC) allocated to ND_06 and corresponding manipulative elements (ME). Tags are referred to Fig. 4.

RMC tag (Step 5)	RMC type (Step 5)	ME type (Step 5)	RM on ME (Step 5)	LC on RMC (Step 5)
LV100, LV101, LV102	On-Off control valve (FC)	On-Off controller (BPCS)	Signal shutdown	Valve closing
			Function reprogramming	Valve opening; Valve closing
SDV100, SDV101, SDV102, SDV103	Shut-off valve (FC)	PLC (SIS)	Signal shutdown	Valve closing
			Function reprogramming	Valve closing
SDV104	Three-way shut-off valve (FC)	PLC (BPCS)	Signal shutdown	Valve in "closed" mode
			Function reprogramming	Change of valve position ("recirculation" mode / "discharge to sea" mode / "closed" mode)
PA002	Gear pump and its driver	PLC (BPCS), PLC (SIS)	Signal shutdown	Stop of the pump
			Function reprogramming	Change in rotation direction Cycles of change in rotation direction Stop/Start of the pump Start-stop cycles of the pump

direction opposite to TA101 (i.e., towards the discharge into the sea) by reprogramming the PLC of the BPCS regulating the operation of the pump. These RMCs, that require to be manipulated, are the relevant RMCs for combination CM6.2.1 among the ones allocated to node ND_06 (see Table 3).

The active/procedural safeguards (APS) effective in contrasting the CMs of concern were identified (Step 7 in Fig. 1) through the revision of the P&IDs and the relevant documentation (e.g., cause/effects matrices). In this way, all the CM+APS attack actions were defined for each relevant triplet ND-SE-MA. As introduced in Iaiani et al. (2023), a CM+APS attack action is a list of actions (RCMs to manipulate and APSs to overcome) that, if performed by an attacker, can initiate a specific security event (SE) in the physical process system. Taking as example combination CM6.2.1 in Table 4, the local shutdown logic (LSD) activated by the very low level switch (LSLL) on the separators, the low and very low level alarms (LAL and LALL), the hand switch (HS) for manual activation of LSD, the position lights for the open position (ZLH) of the valves LV100, LV101, LV102 and the HS for their manual reset, are the identified APSs potentially effective in contrasting it. The actions aimed at performing the manipulations required by CM6.2.1, together with those aimed at overcoming the aforementioned APSs, form the $CM_{6.2.1}$ $+APS_{6.2.1}$ attack action, that, if performed, initiates the scenario ND_06-SE01-MA6.2. No inherent/passive safeguards (IPS) are present in the system analyzed that can potentially prevent or mitigate the security event of concern. The pressure safety valve (PSV100, see Fig. 4) is a IPS potentially able to prevent the LOC from the coalescence separator TA101 (ND_06-SE06-MA6.5): its effectiveness in managing the pressure condition induced by the attack action $CM_{6.5.1}$ $+APS_{6.5.1}$ (see Table 4) shall be checked (see Discussion Section).

Table 4
Combinations (CM) of local consequences (LC), effective active/procedural (APS) and inherent/passive (IPS) safeguards, and related credibility score for sample relevant triplets selected for node ND_06.

Triplet	Description	CM code (Step 6)	Relevant RMCs and required LCs (Step 6)	Effective APSs (Step 7)	Effective IPSs (Step 7)	Plant knowledge level (Step 8)	Cyber complexity (Step 8)	Total credibility score (Step 8)
ND_06-SE01-MA6.1	Inducing oil fraction out of specification (higher) in oil-free water stream discharged into sea	CM6.1.1	Start/no stop PA002 + SDV104 in "discharge to sea" mode	Analytical alarm high AAH	None	High	Low	3
ND_06-SE01-MA6.2	Inducing gas in oil-free water stream discharged into sea	CM6.2.1	LV100 / LV101 / LV102 opened + Start/no stop PA002 in the direction of outflow from TA101	• LSD logic activated by very low level switch LSLL on VS100 / VS101 / VS102 • Low and very low level alarms LAL/LALL on VS100 / VS101 / VS102 + HS for manual LSD • Position light ZLH for LV100 / LV101 / LV102 + HS for manual reset	None	High	Medium	2
ND_06-SE06-MA6.5	Inducing overpressure in coalescence separator TA101 to generate LOC	CM6.5.1	SDV103 closed + start PA002 in the direction of inflow to TA101	Position light ZLL for SDV103 + manual reset	PSV100	High	Medium	2

The credibility score associated to each CM+APS attack action identified in previous step was estimated according to the plant knowledge level required by the attacker to carry out such manipulations and their cyber complexity (Step 8 in Fig. 1). The guidelines provided in Table A.3 and Table A.4 in the Supplementary Material were adopted. Due to the specificities in the operation of the equipment units present in node ND_06 that have been described above (e.g., change of rotation direction of pump PA002 based on oil concentration in the oil-free water stream leaving coalescence separator TA101), the attacker needs complete technical knowledge on the process under assessment, i.e., complete access to plant documentation in order to initiate security events in this node. For this reason, a required plant knowledge level "high" was considered for all the CM+APS attack actions reprted in Table 4. As regards the cyber complexity, a "low" level is considered for $CM_{6.1.1}$ +$APS_{6.1.1}$ attack action as it requires the remotely manipulation, with no specific sequence, of RMCs of different type, whose corresponding MEs are grouped in the same zone of the OT system, which is the BPCS. Differently, for both $CM_{6.2.1}$ +$APS_{6.2.1}$ and $CM_{6.5.1}$ +$APS_{6.5.1}$ attack actions, a "medium" cyber complexity is considered as elements (RMCs and/or shutdown logics) belonging to different zones of the OT system (BPCS and SIS) shall be manipulated with no specific sequence and timing. Therefore, using the 4 × 3 matrix reported in Fig. A.1 in the Supplementary Material, a total credibility score of 3 was obtained for $CM_{6.1.1}$ +$APS_{6.1.1}$ attack action, while a score of 2 was obtained for $CM_{6.2.1}$ +$APS_{6.2.1}$ and $CM_{6.5.1}$ +$APS_{6.5.1}$ attack actions. In absolute terms (credibility score ranges from 1 (not credible) to 16 (highly credible)), all the three CM+APS attack actions are low-credibility scenarios due to the high knowledge level required by the attacker to carry them out. Nevertheless, these cybersecurity scenarios are of concern for the platform analyzed because of the high severity of consequences (cut-off criterium defined in Step 1) and shall be considered for the definition of risk mitigation strategies.

5. Discussion

In POROS 2.0, the identification of high-severity cybersecurity scenarios that can be triggered by the malicious manipulation of the Basic Process Control System (BPCS) and the Safety Instrumented System (SIS) is performed by the analysis of the propagation of the effects of such manipulations between process and/or utility nodes (Step 4). This allows to catch the potential escalation of the consequences of a security event occurring in a node and thus to determine the real extent of damage. This kind of scenarios may not have been systematically captured by the application of previous methods (PHAROS and POROS methodologies) which rely on the experience of the analysists to assess propagations among nodes.

The application of POROS 2.0 to the case study addressing a fixed offshore platform for gas exploitation and processing proved the ability of the methodology in reducing the time and effort in application by limiting, through a severity-based cut-off criterium, the analysis to 29 of the total 52 cybersecurity scenarios that have been identified in terms of triplets node (ND) – security event (SE) – mechanism of action (MA). These 29 cybersecurity scenarios are those with potential for the most severe consequences in terms of damage to people, assets, environment, and/or reputation. Thanks to the procedure described in Step 4, the possibility of such security events to be caused even by minor local actions is clearly identified. For example, with reference to node ND_08 (Compressed Air System, see Fig. 3), inducing a local damage to the wet air accumulator (see ND_08-SE06-MA8.4 in Table 2) escalates severity beyond the value of the equipment itself: the unit is part of an essential service for the platform operation (i.e., the instrument air, IA) and its unavailability induces the entire process to shutdown and a loss of production with huge economic losses (severity vector of [4,2,1,1]). Similar considerations can be made for node ND_07 (Electrical Generation System, see Fig. 3) as also electrical energy (EE) is an essential service: the damage of the electrical generator (see ND_07-SE05-MA7.3 in Table 2) is thus a high-severity scenario for the platform normal operation (severity vector of [3,2,1,1]).

The results obtained for node ND_06 (Oily Water Treatment System, see Fig. 3), and summarized in Table 5, show that high-severity scenarios may be triggered by manipulating a few components. For example, both attack actions $CM_{6.1.1}$ +$APS_{6.1.1}$ and $CM_{6.5.1}$ +$APS_{6.5.1}$ consist in the manipulation of two remotely manipulable components: this means that an attacker only needs to manipulate the two manipulative elements of the BPCS and SIS in order to trigger the associated security events (release of oil into the sea (SE01) and loss of containment (SE06) from coalescence separator respectively).

However, the cyber complexity of the CM+APS attack actions is not the only element to take into account in order to estimate the credibility of a specific cybersecurity scenario. In fact, the knowledge about the process required by the attacker in order to perform a particular CM+APS attack action plays an important role. In fact, even if only a few components need to be manipulated, the fact that a complete knowledge of the control and safety logics is required by the attacker, makes a low-complexity combination less credible. This is the case of $CM_{6.5.1}$ +$APS_{6.5.1}$ attack action as the particular operation of pump PA002 regarding the rotation direction based on the thickness of the oily phase in the coalescence separator TA001 makes the attacker requiring specific knowledge on the process, reducing the credibility score of this CM+APS attack action.

Among the three CM+APS attack actions summarized in Table 5, only for $CM_{6.5.1}$ +$APS_{6.5.1}$ attack action a passive safeguard is present, which is the pressure safety valve PSV100. Its effectiveness in managing the internal pressure condition that is generated by $CM_{6.5.1}$ +$APS_{6.5.1}$ attack action shall be checked: in case the valve sizing is able to manage the overpressure, it plays an important role in preventing/mitigating the effects of ND_06-SE06-MA6.5 as the attacker can not manipulate it as the PSV is not controlled by the OT system of the platform (BPCS and SIS). Hence the sizing of inherent/passive safeguards shall take into account security scenarios that may arise from malicious manipulation of BPCS and SIS systems (i.e., cybersecurity scenarios shall be considered in addition to the sizing cases specified in API standard 521 (American Petroleum Institute API, 2014) for PSVs). Nevertheless, as shown in the case study, IPSs may only be effective in preventing and mitigating certain mechanisms of action, and not the totality.

The results obtained in the case study proved that POROS 2.0 methodology supports the case-specific identification of the cyber-risks as required by the classical Security Vulnerability/Risk Assessment (SVA/SRA) methodologies and the detailed cybersecurity risk assessment procedure proposed by the ISA/IEC 62443 series of standards. For example, the list of identified security events and the associated severity vectors (Table 5) support step ZCR 5.3 "determine consequences and impacts" of ISA/IEC 62443. Similarly, the estimated credibility score associated to each CM+APS attack action is a precious input for step ZCR 5.4 "determine unmitigated likelihood" and the identified active/procedural safeguards potentially effective in contrasting the attack actions can be considered in step ZCR 5.6 "determine security level target". Finally, the identified sets of BPCS and SIS components that require to be manipulated (i.e., the manipulative elements), the related manipulations, and the physical consequences on the remotely manipulable components of the plant support application of step ZCR 5.12 "identify additional cybersecurity countermeasures" of ISA/IEC 62443. In a similar way, other approaches addressing cybersecurity issues, such as the ones proposed by Abdo et al. (2018), Byres et al. (2004), Cusimano and Rostick (2018), Guan et al. (2011), Gertman et al. (2006), Song et al. (2012), Beggs and Warren (2009), and Hashimoto et al. (2013), can benefit from the cybersecurity scenarios that can be identified through the application of POROS 2.0 methodology.

Overall, the outputs that can be obtained through the application of POROS 2.0 methodology pave the way for future developments aimed at the understanding and the modeling of the dynamics of Industrial Automation and Control Systems (such as BPCS and SIS) of critical

Table 5
Summary of the results obtained from POROS 2.0 application to ND_06 and link with steps of the detailed cybersecurity risk assessment procedure proposed by ISA/IEC 62443 series of standards.

Cybersecurity scenario (info to ZCR 5.3)	**Corresponding CM+APS attack action**	**Severity vector [EC, IV,EN,HV]** (info to ZCR 5.3)	**Credibility** (info to ZCR 5.4)	**Elements that require manipulation** (info to ZCR 5.12)	**Safeguards in place** (info to ZCR 5.6)
Oil fraction out of specification (higher) in oil-free water stream discharged into sea	$CM_{6.1.1}$ +$APS_{6.1.1}$	[3,2,3,1]	3 (low)	PLC (BPCS) regulating SDV104 operation; PLC (BPCS) regulating pump PA002 operation	Analytical alarm high AAH
Gas in oil-free water stream discharged into sea	$CM_{6.2.1}$ +$APS_{6.2.1}$	[3,2,2,1]	2 (low)	On-Off controllers (BPCS) regulating LV100, LV101, LV102 operation; PLC (BPCS) regulating pump PA002 operation; LSD logic (SIS)	• LSD logic activated by very low level switch LSLL on VS100 / VS101 / VS102 • Low and very low level alarms LAL/LALL on VS100 / VS101 / VS102 + HS for manual LSD • Position light ZLH for LV100 / LV101 / LV102 + HS for manual reset
LOC from coalescence separator TA101	$CM_{6.5.1}$ +$APS_{6.5.1}$	[4.2.1.1]	2 (low)	PLC (SIS) regulating SDV103 operation; PLC (BPCS) regulating pump PA002 operation	Position light ZLL for SDV103 + manual reset; pressure safety valve PSV100

infrastructures processing and/or storing hazardous materials (e.g., chemical, process, and Oil&Gas facilities) when targeted by cyber-attacks. In fact, the cybersecurity scenarios identified with the proposed methodology can be used as basis for the definition of the entire network of cybersecurity events to be analyzed probabilistically: from emergence of the threat analyzed in terms of foreseen attack scenarios, through its evolution through the system, ending up in dynamic modeling of the attack effects in terms of equipment damage and production outages. Moreover, the systematic and formally rigorous nature of POROS 2.0 methodology leads to the possibility of implementation in software tools supporting an automated or semi-automated assessment which will further reduce application time and effort.

6. Conclusions

POROS 2.0 is a rigorous systematic methodology for process hazard and operability analysis of malicious manipulations of the Basic Process Control System (BPCS) and the Safety Instrumented System (SIS) in chemical, process, and Oil&Gas facilities. In particular, the methodology allows to identify the specific sets of remote manipulations of BPCS and SIS components that can initiate events of concern such as major event scenarios and production outage scenarios with severe consequences on people, assets, environment, and/or reputation. It allows the identification of the passive and active safeguards against such manipulations, and supports the definition of the protection requirements for the different zones of the control and instrumented safety systems. POROS 2.0 includes scoring methods for severity and credibility of cyber-attacks which allow to limit the scope of the assessment on the most relevant cybersecurity scenarios, allowing a streamlined analysis of systems with large number of process and/or utility nodes. Moreover, a specific procedure is defined to support the analysis of the propagation of the effects of the manipulations of the elements of the BPCS and the SIS among different process and/or utility nodes of the plant, allowing to catch the potential escalation of the consequences of such manipulations. These features, poorly supported in the previous versions of the methodology, constitute a step forward for enhancing the practical application of the method.

The proposed case study addressing an offshore fixed platform for gas exploitation and processing demonstrated as the outcomes of cyber-attacks can be described by triplets ND (node) – SE (security event) – MA (mechanism of action). The key role of some utility areas of the plant, providing essential services for process operations, is stressed: even minor disruptions to these sections may escalate into severe consequences for the entire plant as evidenced in the case study for prolonged outage or oil releases. The application also presented the typical outputs as regards identified manipulations and requirements for passive and active safeguards.

Overall, POROS 2.0 methodology supports the systematic definition of the cyber risk information required by Security Vulnerability/Risk Assessment (SVA/SRA) methodologies applicable to the chemical and process industry (e.g., CCPS SVA, API RP 780, RAMCAP, VAM-CF, ISA/IEC 62443 series) and to the offshore Oil&Gas industry (e.g., API RP 70 and API RP 70I). Furthermore, POROS 2.0 methodology paves the way for future developments aimed at the quantitative assessment of the cyber threat to BPCS and SIS of critical infrastructures processing and/or storing hazardous materials (e.g., calculation of the conditional probability of success of a cyber-attack given the attempt which is one of the elements that contributes to the evaluation of the cyber risk).

Acknowledgements

This work was partially supported by project SERICS (PE00000014) under the MUR National Recovery and Resilience Plan funded by the European Union – NextGenerationEU, and by the 4STER Project under the framework of the 4th SAF€RA call funded by INAIL (Istituto Nazionale per l'Assicurazione contro gli Infortuni sul Lavoro, Italy).

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.

Appendix A. Supporting information

Supplementary data associated with this article can be found in the online version at doi:10.1016/j.psep.2023.06.024.

References

Abdo, H., Kaouk, M., Flaus, J.M., Masse, F., 2018. A safety/security risk analysis approach of Industrial Control Systems: A cyber bowtie – combining new version of attack tree with bowtie analysis. Comput. Secur 72, 175–195. https://doi.org/10.1016/j.cose.2017.09.004.

American Petroleum Institute (API), 2012. API RP 70I: Security for Worldwide Offshore Oil and Natural Gas Operations.

American Petroleum Institute (API), 2010, API RP 70: Security for Offshore Oil and Natural Gas Operations.

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

American Petroleum Institute (API), 2014, API RP 521: Pressure-Relieving and Depressuring Systems.
Beggs, C., Warren, M., 2009. Safeguarding Australia from Cyber-terrorism: A Proposed Cyber-terrorism SCADA Risk Framework for Industry Adoption Keywords. Proceedings of the 10th Australian Information Warfare and Security Conference. Edith Cowan University,, Perth Western Australia. https://doi.org/10.4018/978-1-4666-0197-0.ch021.
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).
Byres, E.J., Franz, M., Miller, D., 2004, The Use of Attack Trees in Assessing Vulnerabilities in SCADA Systems. Proceedings of the international infrastructure survivability workshop.
Center for Chemical Process Safety, 2022. Managing Cybersecurity in the Process Industries - A Risk-based Approach (CCPS). Wiley,.
Center For Chemical Process Safety (CCPS), 2011, Process Safety Leading and Lagging Metrics. "You don't improve what you don't measure"
Center of Chemical Process Safety (CCPS), 2003. Guidelines for Analyzing and Managing the Security Vulnerabilities of Fixed Chemical Sites. Wiley/AIChE,, New York.
Cherdantseva, Y., Burnap, P., Blyth, A., Eden, P., Jones, K., Soulsby, H., Stoddart, K., 2016. A review of cyber security risk assessment methods for SCADA systems. Comput. Secur 56, 1–27. https://doi.org/10.1016/j.cose.2015.09.009.
Cusimano, J., Rostick, P., 2018, If It Isn't Secure, It Isn't Safe: Incorporating Cybersecurity into Process Safety. AIChE Spring Meeting and Global Congress on Process Safety.
Gertman, D., Folkers, R., Roberts, J., 2006, Scenario-based approach to risk analysis in support of cyber security. Proceedings of the 5th international topical meeting on nuclear plant instrumentation controls, and human machine interface technology.
Guan, J., Graham, J., Hieb, J., 2011, A digraph model for risk identification and mangement in SCADA systems, in: Proceedings of 2011 IEEE International Conference on Intelligence and Security Informatics, ISI 2011. https://doi.org/10.1109/ISI.2011.5983990.
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.
Hausken, K., 2018. A cost–benefit analysis of terrorist attacks. Def. Peace Econ. 29, 111–129. https://doi.org/10.1080/10242694.2016.1158440.
Iaiani, M., Tugnoli, A., Cozzani, V., 2022. Risk of cascading effects in digitalized process systems. In: Faisal, K., Pasman, H., Yang, M. (Eds.), Methods in Chemical Process Safety, Methods to Assess and Manage Process Safety in Digitalized Process System, Volume 6. Elsevier, pp. 353–388. https://doi.org/10.1016/bs.mcps.2022.04.010.
Iaiani, M., Tugnoli, A., Cozzani, V., 2023. Identification of cyber-risks for the control and safety instrumented systems: a synergic framework for the process industry. Process Saf. Environ. Prot. 172, 69–82. https://doi.org/10.1016/j.psep.2023.01.078.
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 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 https://doi.org/10.1016/j.ress.2021.107685.
International Electrotechnical Commission (IEC), 2016, IEC 61882: Hazard and operability studies (HAZOP studies) - Application guide.
International Society Of Automation (ISA), International Electrotechnical Commission (IEC), 2018, ISA/IEC 62443 Series of Standards: Industrial Automation and Control Systems Security.
Jaeger, C.D., 2002. Vulnerability assessment methodology for chemical facilities (VAM-CF). Chem. Health Saf. 9, 15–19. https://doi.org/10.1016/S1074-9098(02)00389-1.
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.
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.
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, 106083 https://doi.org/10.1016/j.ress.2018.03.001.
Moore, D.A., Fuller, B., Hazzan, M., Jones, J.W., 2007. Development of a security vulnerability assessment process for the RAMCAP chemical sector. J. Hazard Mater. 142, 689–694.
Robertson, J., Turton, W., 2021, Colonial Hackers Stole Data Thursday Ahead of Shutdown - Bloomberg [WWW Document]. Bloomberg News. URL https://www.bloomberg.com/news/articles/2021–05-09/colonial-hackers-stole-data-thursday-ahead-of-pipeline-shutdown (accessed 10.13.22).
Song, J.G., Lee, J.W., Lee, C.K., Kwon, K.C., Lee, D.Y., 2012. A cyber security risk assessment for the design of L&C systems in nuclear power plants. Nucl. Eng. Technol. 44, 919–928. https://doi.org/10.5516/NET.04.2011.065.
Stouffer, K., Pillitteri, V., Lightman, S., Abrams, M., Hahn, A., 2015, NIST Special Publication 800–82 Revision 2 Guide to Industrial Control Systems (ICS) Security. https://doi.org/10.6028/NIST.SP.800–82r2.
The Repository Of Industrial Security Incidents (RISI) [Www Document], 2015. URL https://www.risidata.com/Database (accessed 12.8.20).
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.