Outage and asset damage triggered by malicious manipulation of the control system in process plants

Outage and asset damage triggered by malicious manipulation of the control system in process plants

Matteo IAIANI, Alessandro TUGNOLI, Paolo MACINI, Valerio COZZANI*

LISES - Dipartimento di Ingegneria Civile, Chimica, Ambientale e dei Materiali
Alma Mater Studiorum - Università di Bologna
via Terracini n.28, 40131 Bologna (Italy)

(*) Author to whom correspondence should be addressed.
tel. (+39)-051-2090240
e-mail: valerio.cozzani@unibo.it

Submitted for publication in:
Reliability Engineering and System Safety

Abstract

Intentional acts consisting in remote (cyber) or physical manipulations of the BPCS (Basic Process Control System) and the SIS (Safety Instrumented System) of a process plant may result in severe consequences for the affected industrial facilities. Interruption of productivity, with or without asset damages, generally results in huge economic losses and, at times, in damages to reputation, people and the environment. Despite the existence of several international standards aimed at the assessment and management of cybersecurity of IT (Information Technology) and OT (Operational Technology) systems of a facility, only few contributions are present in the literature addressing the concrete connection between malicious manipulations of the BPCS and SIS systems and the impacts on the physical process system that can be initiated. In this panorama, the present work fills this gap by developing a systematic qualitative methodology supporting the identification of possible security events affecting the operability and/or system integrity of a process plant, of the malicious manipulations by which they may be initiated, and of the existing safeguards in place. The results can be used within the standard procedure for cyber risk management of the IT-OT system (e.g. ISA/IEC 62443), to support the identification of protection requirements and countermeasures. The methodology is complementary to current safety and security assessments and is intended for application to front-end design phase as well as to the security review of operating plants. The methodology was applied to a case study (an offshore Oil&Gas compression plant) to demonstrate the potential of the methodology and the results obtained.

Keywords

Hazard identification; Chemical and Process Industry; Security; Cyber-attack; Major accident hazard; Asset damage; Business interruption; Operability.

Highlights

- Qualitative operability assessment method for remote attacks to BPCS&SIS developed
- The method complements the cybersecurity assessment proposed by ISA/IEC 62443
- Manipulation of few plant components (even one) may generate severe security events
- The SIS results to be the most critical system in the IT-OT network architecture
- Active safety barriers may be used by attackers as means to induce security events

List of Acronyms

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
EQ: Equipment
FMEA: Failure Mode and Effect Analysis
HazId: Hazard Identification
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
MIMAH: Methodology for the Identification of Major Accident Hazards
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
QRA: Quantitative Risk Analysis
RM: Remote Manipulation
RMC: Remote Manipulable Component
SCADA: Supervisory Control And Data Acquisition
SDV: Shut Down Valve
SE: Security Event
SIS: Safety Instrumented System
SRA: Security Risk Assessment
SVA: Security Vulnerability Assessment
vRMC: virtual Remote Manipulable Component

1. Introduction

Cyber threats are becoming a growing concern for all the industrial facilities characterized by a high degree of automation [1], including those, such as chemical and process facilities, that highly rely on Operational Technology (OT) systems in their network structure (e.g. the Basic Process Control System, BPCS, and the Safety Instrumented System, SIS) [2]. Cyber threat is "any circumstance or event with the potential to adversely impact organizational operations (including mission, functions, image or reputation), organizational assets, individuals, other organizations or the nation through an information system via unauthorized access, destruction, disclosure, modification of information, and/or denial of service" [3]. According to McKinsey & Company [4], while higher level of automation can create value equivalent to efficiency improvements of 15 to 20 percent (e.g. quick and safe response to abnormal conditions, process optimization, better product quality, etc.), it exposes companies to cyber threats that can lead to negative impacts and consequences on their assets. Hausken and Levitin [5] state that the damage caused by a cyber-attack is associated with partial/total system incapacitation (reduction of the overall system performance) and with the losses of inherent value of the destroyed system elements. Among all possible impacts, business interruption (total system incapacitation) may have severe economic consequences in process facilities, as it interferes with the ability to operate and therefore to produce. For example, a survey by the Allianz Risk Barometer evidenced that business interruption and the interruption of the supply chain is the biggest concern for the 38% of the respondents [6].

As outlined by Hausken [7][8] and Cullen and Armitage [9], attackers differ in beliefs, preferences, motivations, and capabilities: they span from high-motivated (e.g. by destruction) and well-equipped terrorist organization to low-motivated (e.g. by curiosity) and poorly equipped disgruntled employees. Attackers can share information to each other (e.g. on vulnerabilities, defense measures of the targeted companies) for joint benefit and synergy to lay the foundation for future superior exploits [10], or not sharing knowledge to enhance own reputation [11]. An interdependent security (IDS) model addressing the issue of incentives for companies to invest in information protection has been developed by Kunreuther and Heal [12].

As shown by Iaiani et al. [13] in a previous study focused on the analysis of past cybersecurity-related incidents affecting the process industry and similar sectors, attackers may interrupt the business of a process facility tampering with the Basic Process Control System (BPCS), or the Safety Instrumented System (SIS) by different approaches. Examples of attack modes span from a simple direct activation of PSD (Process Shutdown) logic, to more complex strategies, typically resulting in longer downtimes for investigation and damage repair (e.g. imparting deviations of process variables which exceed the process safety limits in order to automatically activate the SIS functions of shutdown or damage the equipment). For example, in 2004 two viruses infected the control system of an upstream oil facility in Chad, causing communications failure from the wells and manifolds to the Floating Production Offshore Platform. The company suffered loss of personnel time and productivity, in addition to costs for the repair and improvement of the affected system [14]. In 2017, a serious near miss occurred in a petrochemical plant in Saudi Arabia where attackers managed to access the OT system of the facility and tried to trigger a cascading explosion by manipulating physical elements of the plant: luckily enough, an error in the malware code blocked the attack [15]. A distinctive feature of these kind of attacks is that, while they are possible through the direct access to the control room of the facility, they potentially may also be carried out remotely, accessing the external network of the company.

The development of methods for risk identification in the field of security, as well as for definition of risk mitigation and prevention strategies, may contribute to the increase of the operational resilience of systems, defined by the National Academy of Science (NAS) as "the ability to plan and

prepare for, absorb, recover from, and more successfully adapt to disruptive events" [16]. Bostik et al. [17] consider risk assessment and resilience assessment as distinct elements whose improvements can benefit from simple scorecard or metric approaches to more advanced system configuration modelling and scenario analysis. On the other hand, Bier and Gutfraind [18] consider both the aspects in a more coordinate manner under the concept of defensibility, defined as "the ability of the defender to reduce the damage to the system". An important contribution regarding resources, competence, technology, tools, and strategies in cyber resilience (i.e. resilience against cyber incidents) is provided in Hausken [7].

When addressing Security Risk Management, before quantitative methods may be applied to assess likelihood of success of the attack and severity of consequences, a systematic risk identification needs to be carried out in order to "determine what can happen to cause a potential loss, and to gain insight into how, where and why the loss can happen" (ISO/IEC 27005). This phase, though inherently qualitative, provides the necessary input information for the application of relevant methods in the Risk Analysis phase (i.e. assessment of consequences and likelihood and risk level determination), as described by ISO/IEC 27005 and ISO 31000.

A full security analysis with respect to the scenarios coming from malicious manipulations of the control system requires the investigation of both the attack to the IT-OT network and the manipulation of the physical plant (Figure 1). The methodologies dedicated to process plant security vulnerability assessment (e.g. the VAM-CF methodology [19], the CCPS methodology [20] and API RP 780 methodology [21]) consider attacks to the BPCS and the SIS in the evaluation, but no specific approaches for assessment of the link between intentional manipulations and consequences is provided [22]. The ISO/IEC 27000 series of standards [23] on information security (intended as "the preservation of confidentiality, integrity, and availability of information" [23][24]), provides a consolidated general approach to tackle a complete security analysis of the IT system, which is better specified for Industrial Automation and Control Systems (IACS) by the ISA/IEC 62443 series of standards [25][26]. These standards support the assessment of the issues related to the IT-OT part of the system, but lack in providing guidelines for the evaluation of the impacts resulting from attacks (e.g. business interruption, damage of machinery, loss of containment of a hazardous substance, etc.). Since such information is required in the security risk assessment, simplified assumptions are frequently adopted (e.g. considering the worst-case consequences, as expected from the safety assessment). However, the impacts and consequences that can be originated by an attack to the OT system are potentially different from those considered in the safety study: e.g. some abnormal states of the plant can not be induced through the BPCS and the SIS, and some combinations of induced deviations may have been dismissed as unlikely in the safety study. Therefore, a dedicated analysis addressing the identification of potential impacts and the role that physical and instrumented safety barriers may play during the malicious attack is required.

The present study aims at filling the gap in the availability of systematic risk identification procedures for security assessment of the link between malicious manipulations of the BPCS and the SIS, and impacts that affect the operability and/or system integrity of a process plant. To this aim, a rigorous methodology for operability/system integrity qualitative analysis was developed (POROS: Process Operability analysis of Remote manipulations through the cOntrol System).

The methodology exploits a reverse-HazOp concept: starting from the possible security events of concern (e.g. arrest/blockage of a piece of equipment/item or product out of specification), the remote manipulations achievable through an attack to the BPCS and the SIS and leading to such security events are identified by a systematic methodology. Physical and automated safeguards preventing or mitigating the security event are considered and rated for their effectiveness. The methodology is intended for application to front-end design phase as well as to the security review of operating plants.

In the following, a review of existing methods for risk assessments of OT systems is provided (Section 2), and subsequently the proposed POROS methodology is described (Section 3). A case study on an Oil&Gas two stage compression platform is presented (Section 4) to demonstrate the application of the methodology and the typical results obtained (Section 5 and Section 6).

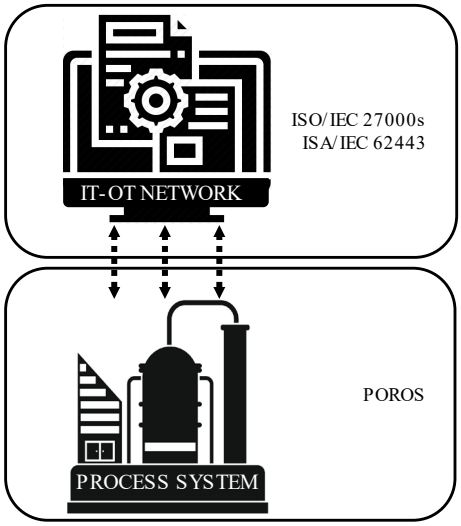

Figure 1. Schematization of the security risk assessment for malicious manipulations of the control system of a process plant.

2. State of the art

In spite of the recognized relation between safety and security (Brewer (1993) [27], Eames and Moffett (1999) [28], Firesmith (2018) [29], Kriaa et al. (2015) [30], Sørby (2003) [31]), the hazard and operability assessment techniques commonly used for process systems (HazOp, LOPA, fault tree analysis, etc.) are not suitable to account for these aspects: in fact, as stated by Baybutt [32], "security differs fundamentally from safety in regards to risk assessment and these differences must be addressed by security risk assessment methods". A review of the scientific literature identified only few contributions devoted to security of the OT system in process plants or to the assessment of the major accidents that can be triggered by malicious manipulations of the control system.

Byres et al. [33] make use of attack trees (ATs) to assess vulnerabilities of SCADA systems. ATs provide a structured view of events leading to an attack (the node of the tree is the attacker goal) and, ultimately, help with the identification of appropriate security countermeasures. Nevertheless, the scenarios resulting from the attacks are not assessed.

A scenario-based approach allowing decision makers to place financial and personnel resources in-place to protect nuclear power plants is described in Gertman et al. [34]. It consists of a step-by-step approach, very similar to the framework of SVA-SRA methodologies.

Beggs and Warren [35] developed a risk framework to measure and protect SCADA systems from the threat of cyber terrorism within Australia, consisting of three stages: 1) risk assessment, 2) capability assessment, and 3) controls. However, the general framework provided is not tailored to the specific issue of the link between remote manipulations of the BPCS and the SIS systems and the scenarios affecting the operability and system integrity of a process plant.

A cybersecurity risk assessment methodology that may be exploited in the process of the design of instrumentation and control systems in nuclear power plants is suggested by Song et al. [36]. Possible attack scenarios are listed to be used in threat analysis, but no systematic tools for identification are provided.

Guan et al. [37] developed a digraph model of a SCADA system for a chemical distillation column. The model provides a formal representation of the structure and behaviour of a SCADA system and may be exploited for risk impact assessment and fault diagnosis, but is limited in applicability to the specific case.

Hashimoto et al. [38] developed a systematic, qualitative and quantitative approach to evaluate the detectability and reachability of process plant manipulations, but the identification of the specific set of manipulations required to trigger specific events as outage and/or asset damages are out of the scope of the methodology.

Abdo et al. [39] proposed an approach that allows to assess the vulnerabilities and hacking techniques that can be exploited by the attackers to infect the IT-OT system and initiating security events, but no support is provided to the identification of the manipulations of the physical devices of the process system that can lead to such security events.

Cusimano and Rostick [40] developed the CyberPHA methodology as a safety-oriented methodology to conduct a cybersecurity risk assessment for industrial control and safety systems. The proposed methodology is a consequence-driven approach based upon industry standards such as ISA/IEC 62443-3-2. However, the absence of guidelines in systematic identification of adverse scenarios and manipulation required may undermine reproducibility in application.

3. Methodology

3.1 Overview

The POROS methodology aims at the identification of the security events that may lead to the plant arrest (outage) and consequent interruption of productivity for a certain period of time (downtime) caused by a malicious manipulation of the OT system. The output of the methodology includes the identification of the set of manipulations through which a security event can be initiated, and the effective safety barriers (procedural, active, inherent and passive barriers) that can prevent such security events. The method aims to address part of the risk identification step foreseen by the risk assessment framework introduced by ISO/IEC 27005 and ISA/IEC 62443. Actually, even if the methodology is qualitative, the output information is suitable to support the quantitative or semi-quantitative methods used in the steps of assessment of consequences and of assessment of likelihood. Examples of methods that can use input information from POROS include the approach for likelihood estimation proposed by the German DIN VDE V 0831-104 [41], the CyberPHA developed by Cusimano et al. [40], the scenario-based approach developed by Gertman et al. [33], and the safety/security risk analysis approach using cyber bowties developed by Hashimoto et al. [39].

Figure 2 shows the integration of POROS with the ‘detailed cybersecurity risk assessment workflow’ of ISA/IEC 62443. With particular focus on the analysis of the process system part of the plant (Figure 1), POROS provides the information needed for the characterization of the impacts potentially originated form the malicious manipulation of the BPCS and the SIS (ZCR 5.3), the evaluation of the unmitigated and mitigated likelihood (ZCR 5.4 and ZCR 5.8) and for the assessment of additional countermeasures or design modifications (ZCR 5.12).

The methodology focuses on the response of the physical process system to malicious manipulation of the BPCS and SIS. Hence, it is based on the assumption that the attacker successfully managed to infect the IT-OT network of the target system by overcoming any IT-OT defence barrier and, therefore, is able to impart any instruction. This assumption clearly portraits a worst-case scenario, as effective access of the attacker to all the devices of the target system may be limited by IT countermeasures (e.g. presence of suitably configured firewall between IT and OT systems) as analysed by the standard ISA/IEC 62443.

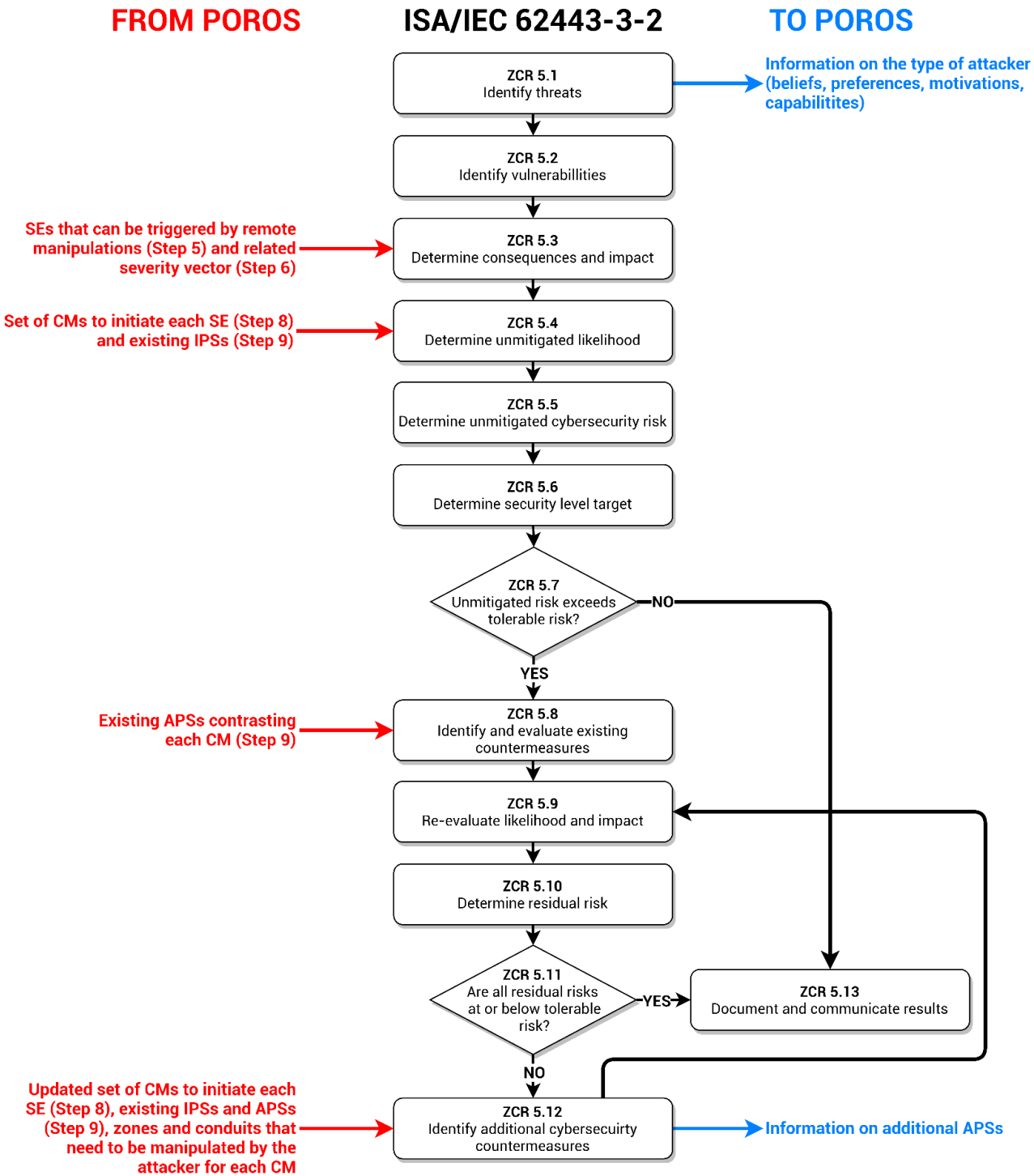

Figure 2. Integration of POROS with the 'detailed cybersecurity risk assessment workflow' of ISA/IEC 62443.

POROS methodology is a systematic, qualitative and formally rigorous methodology of process schemes and should be performed by a team with knowledge of the process plant system, the control system and the loss prevention system. As for HazOp and Hazid analyses [42][43], a typical team includes a team leader, a secretary, a project engineer, a process design engineer, an instrumentation and control engineer, and a safety engineer. Given the initial assumption on full access of the attacker to the IT-OT system, only generic IT skills are required in the team. The application of the methodology is possible since the front-end design phase.

According to the classification of system structures proposed by Hausken and Levitin [44], the POROS methodology is intended for application to “networks” and “interdependent systems” (both IT-OT network and physical process plant have such characteristic). POROS is able to account for the effects of defence measures classified as “multilevel defence”, “redundancy”, and “separation of system elements” [44]. The methodology can consider attack tactics described as “attack against single element”, “attacks against multiple elements” and “random attack” [44].

Figure 3 shows the conceptual model of the attack as considered by the methodology. An attacker pursuing a goal based on his/her beliefs, preferences and motivations, aims at causing an undesired event in a plant (i.e. a security event, SE, such as a production shutdown or a loss of containment of hazardous material) [45][9][7][8]. He/she exploits his/her capabilities of control over the BPCS and SIS systems and his/her knowledge of the system to remotely initiate a physical mechanism (mechanism of action, MA) leading to such SE. An example is inducing a LSD (local shutdown) by rising the liquid level in a process separator. The MA is achieved by manipulating the RMCs in the plant (remote manipulable components, such as valves, motors, etc.) according to a certain pattern. The remote manipulation (RMs, e.g. set point change) of a RMC occurs through a manipulative element (ME) (e.g. the PID controller of the BPCS) and results in a local effect on the physical plant (local consequence, LC, e.g. valve closed). Typically, a MA requires to successfully implement a combination of more than one LC (combination of local consequences, CM).

The success of an MA in causing a SE can be limited by the presence of effective safeguards (e.g. safety instrumented functions and physical safety devices).

In order to reduce the subjectivity in application of the method and promote repeatability of results, the method was developed as a structured step-by-step procedure, similar to well-known procedures of HazOp, Hazid and FMEA [42][43]. In addition, guideline tables (see e.g. Tables A2-A4 in the Appendix) provide reference checklists of the more common classes of SE, RMC, ME, RM, LC and MA for process plants.

The POROS methodology, described in detail in the following, consists in nine steps (Figure 4) which guide through the systematic identification of the elements described above in the conceptual model of the attack.

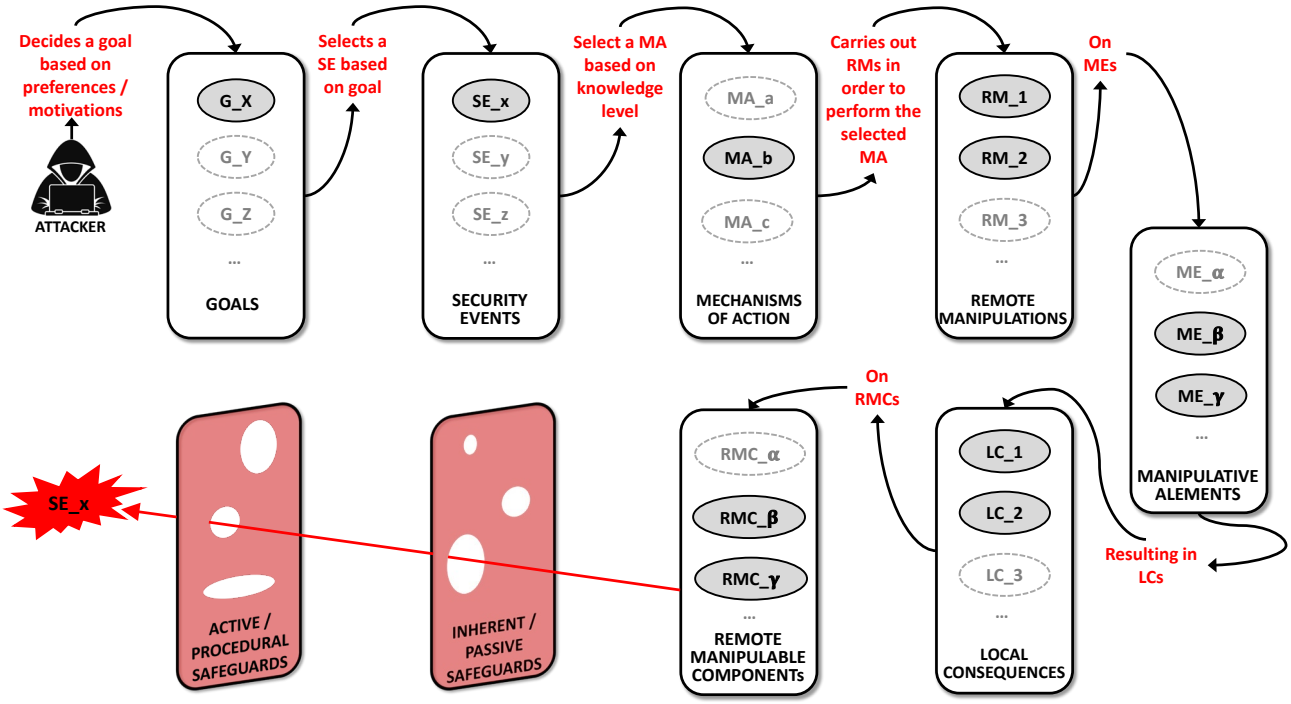

Figure 3. Relationship between, RMs, MEs, LCs, RMCs, CMs, MAs and SEs (RM: Remote Manipulation; ME: Manipulative Element, LC: Local Consequence; RMC: Remote Manipulable Component; CM: CoMbination of local consequences; MA: Mechanism of Action; SE: Security Event).

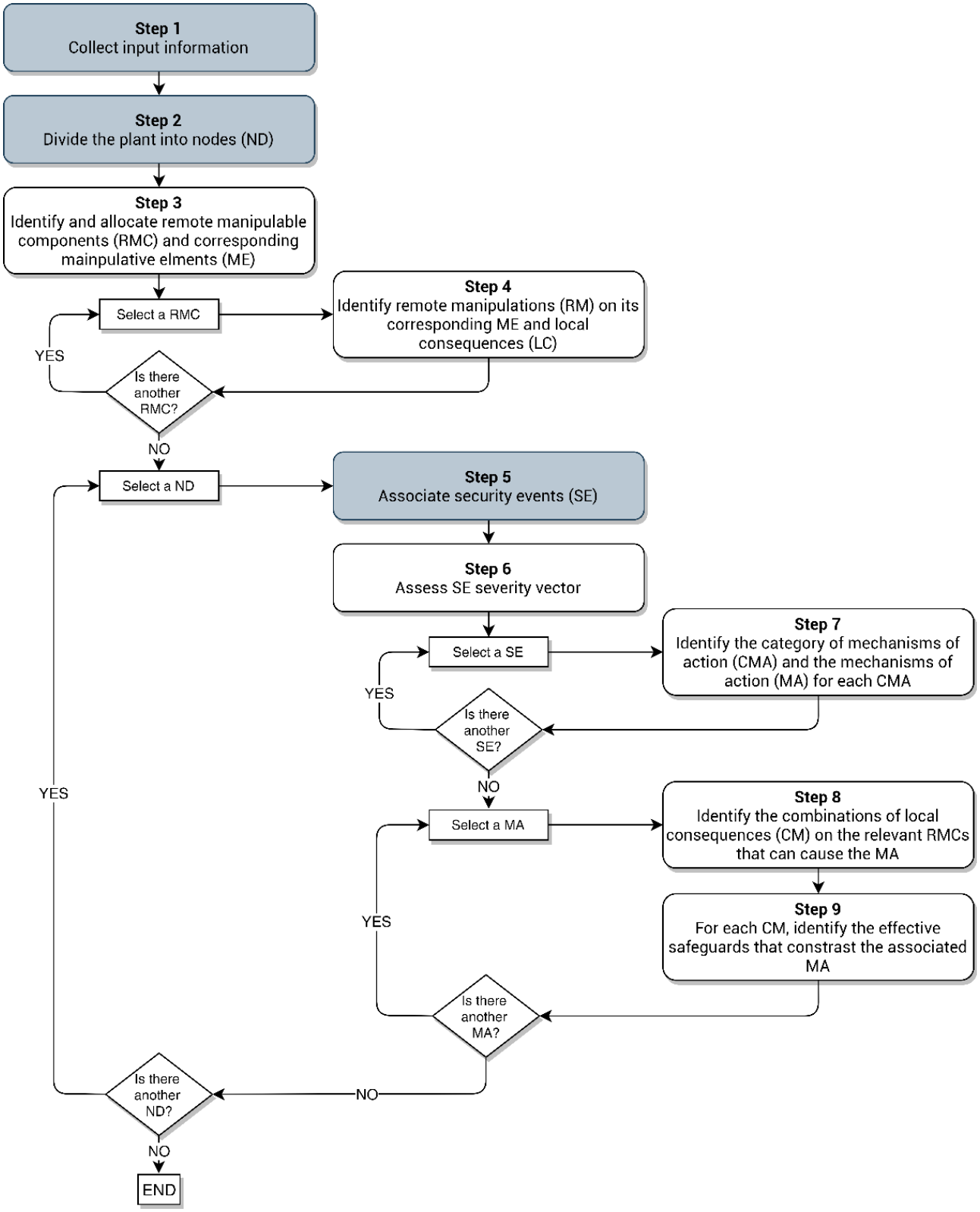

Figure 4. Flowchart of the POROS methodology. Shaded steps (grey coloured) can be integrated with conventional safety studies.

3.2 Detailed description of the methodology

In Step 1 of POROS the input information for the application of the methodology is collected. This consists in: the PFD (Process Flow Diagram) and the material balances, the P&ID (Piping and

Instrumentation Diagram), the list of substances stored or handled and their hazardous properties, the datasheets of tagged items (e.g. equipment units, motors, valves), the safety instrumented functions (SIFs) and the control philosophy (e.g. the cause-effect matrix, the functional block diagrams, etc.).

In Step 2, the plant is divided into nodes (NDs). Each node comprises a main process equipment (e.g. storage vessel, column, reactor, etc.), the auxiliary equipment (e.g. pump, drum, etc.), and the pipework. Table A.1 in the Appendix reports the main general categories of plant items based on the classification provided by ARAMIS [46][47]. Utilities (e.g. cooling water system, power generation system, instrument air system), if included in the scope of the assessment, are also considered as nodes. The division in nodes is conceptually similar to that adopted in HazOp studies (described by the IEC 61882 standard [42]): if such a study is already available for the same plant, the HazOp nodes can be adopted.

Step 3 consists in compiling a list of the remote manipulable components (RMCs) present in each ND. RMCs are the physical components in the plant whose operation is regulated by the OT system (e.g. automatic valves, pumps, compressors, etc.). For each RMC, the manipulation may be carried out through one or more manipulative elements (MEs), which are elements of the OT system (e.g. the process and safety controllers). Table A.2 in the Appendix provides a classification of the most common RMCs and MEs in process plants.

Each RMCs should be allocated to one or more ND. RMCs present on a line or equipment internal to a ND are allocated only to that ND. If a RMC is located on a line that connects the ND to another ND, it is allocated to both the upstream and downstream NDs.

The division into nodes (Step 2) and the identification of RMCs and related MEs (Step 3) are based on a review of process documentation (PFD, P&IDs, valve and motor datasheets, etc.).

Step 4 consists in identifying, for each ME, all possible remote manipulations (RMs) that an attacker can carry out (e.g. set-point change or signal shutdown for a PID controller). This is based on information from implemented control philosophies and safety instrumented functions. Table A.2 in the Appendix proposes typical RMs possible for each ME.

Then, for each ME, the local consequences (LCs) on the controlled RMC are identified (e.g. the increase in the opening of a control valve as a result of a setpoint change). Table A.3 in the Appendix shows typical associations of RMs and LCs. A particular attention should be devoted to this step, since specific features of the RMC may lead to different LCs as a result of the same RM (e.g. a fail closed valve behaves differently than a fail open valve in case of signal shutdown).

Step 5 consists in associating to each ND the compatible security events (SEs). A SE is an undesired event that affects the operability and/or the physical integrity of the system under investigation. Examples of SE may include loss of containment (LOC) or loss of physical integrity (LPI), stop of plant operations (e.g. activation of shutdown logics), equipment damage (e.g. failure of equipment components), operation out of specification (e.g. product out of specifications, emissions out of limits, waste of raw materials), etc.

The categories of LOCs and LPIs proposed e.g. by the standard API 581 [48], the MIMAH methodology [46] and the “Purple Book” [49] can be used as reference. Table A.4 in the Appendix reports a suggested list of possible SEs. Case specific LOC or LPI emerging from available safety and operability studies (e.g. HazOp [42], failure modes and effect analysis (FMEA) [50], DyPASI [43]), shall be included in the list of SEs for the node. This step is based on the review of the P&IDs, of the list of substances stored or handled and their hazardous properties, of the control philosophies, and safety instrumented functions.

In Step 6 a severity level is associated to each SE. A qualitative severity scale is proposed in Table 1. The scale is compliant with the guidelines on severity scales outlined by Baybutt [51], and it was developed starting from the process safety metrics [52] proposed by the Center for Chemical Process Safety (CCPS) and the categorization of impacts sketched by Hausken [53]. Four severity levels are

considered (1 - minor impact, 2 - medium impact, 3 - major impact and 4 - extensive impact), exploring four types of target values (EC: economic value, IV: influence value, EN: environmental value, HV: human value). In Table 1, the loss of economic value is given by the sum of direct costs (e.g. repair or replacement of process equipment) and indirect costs (e.g. loss of profits due to production downtime); loss of human value accounts both for the injuries (e.g. amputations, diseases, physical damages) and/or on-site and/or off-site fatalities following the security event; loss of influence value is associated to the reduction of the symbolic, political and economic prestige of the affected facility and thus it is strongly related to reputation; loss of environmental value is accounted for the long- or short-term effects on the physical environment (air, water or soil) requiring environmental remediation. A severity vector is defined for each SE reporting the scores for the four target values ([EC, IV, EN, HV]).
Useful information for evaluating the severity score concerns the material balances, the datasheets of tagged items, the list of substances stored/handled and their hazardous properties.

The ranking of SE severity provided supports the evaluations of the worst-case impact scenario as requested in the framework of the ISA/IEC 62443 series of standards (more specifically in step ZCR 5.3 "Determine consequences and impact" of ISA/IEC 62443-3-2 in Figure 2).

A high number of SEs is usually identified at step 5. However, it is recognized that efforts in improvement of preventive and mitigation measures shall target primary the SEs with the higher level of concern for a given context. The application of a cut-off criteria (Step 6) setting a threshold value for the severity level is suggested. The use of threshold values in the analysis of scientific uncertainty related to a threat (i.e. the cyber threat in this case) is customary among the authors in the literature (e.g. see Hausken [8], Bschir [54], and Koch at al. [55]).

A simple cut-off focusing on SE with the highest level of severity (i.e. severity level ≥ 3 for at least one target type) is suggested for general application, based the high risk aversion typically expected for severe scenarios [56].

Nevertheless, other cut-off criteria are possible, especially when well characterised cyber-threat sources are of concern. In facts, the generic cut-off suggested above does not take into account that the goal of the attacker is influenced by factors such as his/her beliefs, preferences, motivations, and capabilities [45][9][7][8]: for example, while triggering a major event with severe consequences in terms of human value may be a likely goal for a well-equipped and high-motivated terrorist organization, it is not expected to be the case for non-violent activists motivated by pacific rebellion.

While categorization of the goals of the attacker lays beyond the scope of current methodology, it is commonly performed as part of conventional Security Assessment methods (see e.g. “Identify Threat” step ZCR 5.1 in ISA/IEC 62443-3-2, or “Adversary Identification” step 3.1 in CCPS SVA methodology). The categorization of SEs from step 5 in terms of severity vector will help the identification of the ones matching the goals of specific attackers. Table A.5 in the Appendix proposes an example of expected ranges for the severity vector values for the SE selection with reference to different types of attacker (classification of attacker adapted from ISO/IEC 27005).

Step 7 consists in identifying all the mechanisms of action (MAs) that may generate each SE through an attack to the OT system. The MAs are the physical mechanisms that the attackers may use to initiate the SE (e.g. increase the internal pressure of a vessel by closing the gas outlets). Table A.4 in the Appendix shows reference categories of mechanisms of actions (CMAs) for each SE and some examples of MAs. The categories of mechanism of action (CMAs) can support the identification of the MAs by grouping them in conceptually similar categories. As a matter of facts, more than one MA can typically be identified based on the same CMA (e.g. considering a chemical reactor, the category “CMA01: composition/phase out of specification” may be realized through different mechanisms of action: by changing flowrates of reactants, by changing temperature, by changing pressure, by changing residence time, etc.).

Although the CMAs in Table A.4 in the Appendix provide a guideline for the identification of the mechanisms of action, developing MAs tailored to the design features of the ND under assessment is required, as some mechanisms of action may be case specific (e.g. number and arrangement of input/output lines may vary). Therefore, process documentation such as PFDs, P&IDs, control philosophies, and safety instrumented functions, supports identification of MAs. If a HazOp study or a fault tree analysis [46] are available for the ND, they can complement this step of MA identification, since many of the applicable mechanisms of action are possibly identified by such studies.

If there are no possible MAs for a SE, the SE is removed from those previously associated to the ND under investigation. Some MAs may require actions from a nearby node to occur (i.e. manipulation of RMCs belonging to a nearby node is required). In these cases, the information is propagated from a node to another similarly to deviations propagating among different nodes in a traditional HazOp study.

Step 8 consists in identifying the combinations (CMs) of LCs on the allocated RMCs by means of which the MAs identified for the ND under investigation can be carried out. In general, not all the RMCs allocated to a ND need to be manipulated for carrying out a MA: those that need to be manipulated constitute the set of relevant RMCs for a CM of the given MA. This step can be supported for each ND by a worksheet that collects all the relevant information. An example of worksheet is provided in the next section. This step is based on a review of process documentation such as PFDs, P&IDs, control philosophies, and safety instrumented functions.

Step 9 consists in identifying, for each CM, the effective safeguards (i.e. safety barriers) which are present in the ND under investigation. "Effective" means that the safeguard is able to contrast, directly or indirectly, the MA associated to a particular CM, avoiding the occurrence of the SEs that may be originated through that MA. Therefore, a safeguard can be effective for one CM and not for another. Effectiveness shall be checked case by case, as it also depends on design specifications of the barrier. Safeguards can be identified by a review of P&IDs, safety instrumented functions, and cause-effect matrices.

Safeguards can be classified in active/procedural safeguards (APSs) and inherent/passive safeguards (PSs) [57]. The first ones are automated or human-mediated actions, which involve response by the same IT-OT system under attack (e.g. alarms triggering operator reaction, safety instrumented functions for shutdown/blowdown). The IPSs are devices that provide their safety action independently of the IT-OT system (e.g. PSVs, burst disks).

It is important to emphasize that attackers can manipulate the active/procedural safeguards, but not the inherent/passive ones. Nevertheless, the identification of the active/procedural safeguards is included in the method for two main reasons. First, it may be argued that the attackers, despite being able to manipulate the OT system, may not have full knowledge or ability to deactivate all the APSs that can contrast the MAs. Second, the identification of the relevant APSs allows for taking specific IT-OT countermeasures to protect the APSs more relevant in preventing a successful cyber-attack, which is a very useful information for the design of the IT-OT network.

Similarly to an HazOp study, once all the steps have been performed, a completeness check is required. It consists in verifying that all the NDs have been analysed, and that all the MAs, through which the associated SEs can be originated, were developed as CMs. Particular attention shall be given to completeness check in case of SEs that require manipulations on RMC in more than one ND.

Table 1. Severity scale adopted for severity ranking of the SEs. Adapted from CCPS [52] and Hausken [53].

		TARGET VALUES				
Severity level		**LOSS OF ECONOMIC VALUE (EC)**		**LOSS OF INFLUENCE VALUE (IV)**	**LOSS OF ENVIRONMENTAL VALUE (EN)**	**LOSS OF HUMAN VALUE (HV)**
1	**MINOR IMPACT**	**Cost of total losses <** $100K	No disruption or possible short disruption of operations/business	No loss of reputation. OR Minor and short-lived impact in the locality. OR Local media coverage.	Short-term remediation to address acute environmental impact. No long-term cost or company oversight.	Injury requiring treatment beyond first aid to employees or contractors (but no lost time injury).
2	**MEDIUM IMPACT**	**Cost of total losses** between $100K and $1MM	Medium time/medium change to resume operations/business. Unit repair/replacement needed.	Significant potential damage to the regional reputation. OR Regional media coverage.	Environmental remediation required with cost less than $1MM. No other regulatory oversight required.	Lost time injury to employees or contractors. OR Minor off-site impact with precautionary shelter-in-place
3	**MAJOR IMPACT**	**Cost of total losses** between $1MM and $10MM	Long time/major change to resume operations/business. Unit repair/replacement needed.	Serious/permanent damage to the ability of the Company to sustain business position in the location, some broader implications for the Company. OR National media coverage.	Environmental remediation required and cost in between $1MM - $2.5 MM. State government investigation and oversight of process.	On-site fatality employees or contractors; multiple lost time injuries or one or more serious offsite injuries. OR Shelter-in-place or community evacuation.
4	**EXTENSIVE IMPACT**	**Cost of total losses > $**10MM	Total loss of operations/business. Revamping necessary to resume the process.	Potential loss of future business position in the location/region and significant broader implications for the Company. OR National media coverage over multiple days.	Environmental remediation required and cost in excess of $2.5 MM. Federal government investigation and oversight of process.	Off-site fatality or multiple on-site fatalities. OR Other significant community impact.

4. Case study

An offshore Oil&Gas platform for gas compression was considered as a Case Study. Figure 5 shows the process flow diagram (PFD) of the system. 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 analysis), 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.

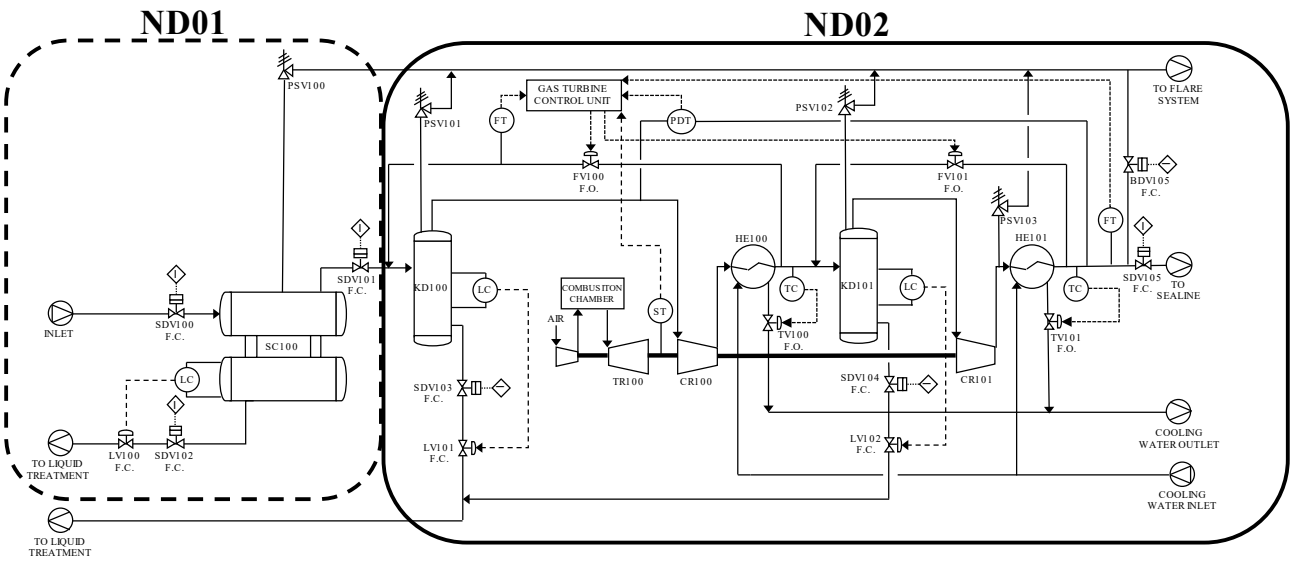

Figure 5. Process flow diagram (PFD) of the gas compression platform and division into nodes (ND01 and ND02).

5. Results

The analysis of the case study described in section 3 provides an example of the results that may be obtained from the application of the methodology. Following the collection of the input data (Step 1 of the methodology), the process under investigation was divided into NDs according to the typical rules of the HazOp study [42] (Step 2). In particular, two NDs were identified (ND01 and ND02) as shown in Figure 5. ND01 includes the slug catcher SC100 and the connected pipework. ND02 includes the gas turbine, the KO drums KD100 and KD101, the heat exchangers HE100 and HE101, and the connected piping.

After the division into NDs, the remote manipulable components (RMCs) which are present in the plant under assessment and the associated manipulative elements (MEs) were identified following the guidelines provided in Table A.2 in the Appendix (Step 3 of the methodology). The identified RMCs and associated MEs were then allocated to the two nodes (ND01 and ND02) in accordance with the rules described in Section 2.2 (Table 2 summarizes the results). In this specific case, the RMCs include emergency valves (blowdown valve and shutdown valves), control valves and a motor-driven gas turbine. The shutdown valves and the blowdown valve are shut-off valves controlled by the SIS by means of controllers such as PLCs (Programmable Logic Controllers), that are the MEs on which an attacker can act. The control valves are controlled by the BPCS by means of controllers such as PIDs (Proportional Integral Derivative), while the gas turbine is controlled by both BPCS and SIS systems.

The remote manipulations (RMs) for the MEs were identified in accordance with the guidelines provided in Table A.2 in the Appendix (Step 4 of the methodology). "Signal shutdown" (code RM1) and "function reprogramming" (code RM3) were considered for the PLCs of the SIS (acting on the shut-off and blowdown valves) and of the BPCS (acting on the gas turbine); "signal shutdown" (code RM1) and "setpoint change" (code RM2) were considered for the PIDs controllers of the BPCS (acting on the control valves).

The local consequences (LCs) on the RMCs that result from the RMs associated to each ME were then identified applying the typical associations of RMs and LCs shown in Table A.3 in the Appendix. This requires to consider the fail-safe nature of all the automatic valves [58], the control action of the PID controllers (direct or reverse), the logics of the PLCs and the safety instrumented functions of the SIS.

Table 2 summarizes the remote manipulations (RMs) and the local consequences (LCs) on the total RMCs that are present in the plant under investigation. For example, the control valve LV100 (see Table 2 and Figure 5), as a consequence of a signal shutdown (RM1) to the PID controller by which the valve is managed (i.e. its ME), stops the flow (LC2) as it fails in the closed position.

Table 2. Remote manipulations (RMs) and local consequences (LCs) for each RMC allocated to the nodes ND01 and ND02.

RMCs (Step 3)	RMC code (Step 3)	Allocated to (Step 3)	ME code (Step 3)	RM code (Step 4)	LC code (Step 4)
SDV100 SDV101 SDV102 SDV103 SDV104 SDV105	RMC1: shut-off valves (F.C.)	ND01 ND01 – ND02 ND01 ND02 ND02 ND02	ME2: Safety Instrumented System devices	RM1: signal shutdown RM3: function reprogramming	LC2: valve closing LC2: valve closing
BDV105	RMC1: shut-off valve (F.O.)	ND02	ME2: Safety Instrumented System devices	RM1: signal shutdown RM3: function reprogramming	LC1: valve opening LC1: valve opening
LV100 LV101 LV102	RMC2: control valves (F.C)	ND01 ND02 ND02	ME1: Basic Process Control System devices (PID controllers)	RM1: signal shutdown RM2: setpoint change	LC2: valve closing LC7: increase in valve opening degree LC8: decrease in valve opening degree LC9: opening-closing cycles of the valve
TV100 TV101 FV100 FV101	RMC2: control valves (F.O)	ND02 ND02 ND02 ND02	ME1: Basic Process Control System devices (PID controllers)	RM1: signal shutdown RM2: setpoint change	LC1: valve opening LC7: increase in valve opening degree LC8: decrease in valve opening degree LC9: opening-closing cycles of the valve
GAS TURBINE (TR100 + CR100 + CR101)	RMC4: gas turbine (launched by electric motor)	ND02	ME1: Basic Process Control System device (PLC)	RM1: signal shutdown RM3: function reprogramming	LC5: stop of the gas turbine LC5: stop of the gas turbine LC10: Increase of the rotational speed of the gas turbine LC11: Decrease of the rotational speed of the gas turbine LC12: cycles of increase-decrease of the rotational speed of the gas turbine LC13: start of the gas turbine LC14: start and stop cycles of the gas turbine
			ME2: Safety Instrumented System device	RM1: signal shutdown RM3: function reprogramming	LC5: stop of the gas turbine As for RM3 on ME1

The identification of the security events (SEs) for ND01 and ND02 was performed in accordance with the guidelines provided in Table A.4 in the Appendix, taking into account the specific features of the physical equipment/components in the assessed process (Step 5 of the methodology). In particular, all the SEs listed in the table were considered applicable for ND02, while for ND01 only SE05 (damage of moving machinery/component) was not selected.

The SEs associated to the two NDs under investigation were scored for their severity according to the scale proposed in Table 1. The severity scoring was based on a preliminary estimation of the consequences expected by each SE for the selected node (Table 3). For example, inducing or directly activating an Emergency Shut Down (ESD) leading to the arrest and depressurization of the two compressors (ND01-SE03 or ND02-SE03 in Table 3) is expected to cause a downtime of the plant (i.e. total amount of time without productivity) of about 6 hours, with no loss of containment or energy release. Hence, no damage to environment, people, and reputation is expected (severity level 1: minor impact). However, considering an average value of production of 1'420'000 $/day, a total cost of losses of about 355'400$ was estimated (i.e. medium impact according to Table 1). Therefore, a severity level of 2 was assigned to SE03 for both the nodes in Table 3.

Table 3 shows that tangible adverse consequences are expected for most SEs. This further confirms that operability and asset integrity issues induced by remote manipulation of the control system are of interest for facilities as the one analysed in the current case study. However, in this particular case, given e.g. the low potentiality of the plant, the economic losses resulting from short production downtimes (e.g. by stopping compressors with a dedicated command, as in ND02-SE02) score medium to minor impacts. High severity levels are obtained for cases that trigger permanent damage to the equipment (ND01-SE04, ND02-SE04 and ND02-SE05), which are characterized by longer downtimes and high costs of replacement, as well as by cases leading to loss of containment of flammable gases (SE06 for both nodes). In particular, the high cost of the compressors in ND02 leads to identify any permeant damage to this equipment as level 4 severity SE for loss of economic value.

The following, the discussion of the results of the case study will focus on the most severe SEs (at least one element of the severity vector ≥ 3), for which dedicated countermeasures at IT-OT level are a priority. Interestingly enough the selection criterion matched the one presented for "state-sponsored organization" attacks identified in Table A.5 in the Appendix. Table 3 lists the selected SEs.

Table 3. Security events (SEs) considered applicable for each ND and severity vector assessed according to the severity scale proposed in Table 1.

Node	Items	SE code (Step 5)	Expected consequences (Step 6)	Severity vector [EC, IV, EN, HV] (Step 6)	Cut-off (Step 6)
ND01	Slug catcher SC100 Piping	SE01: product out of specification (incomplete separation)	No direct economic effect on ND01. No damage to people or environment.	[1, 1, 1, 1]	Not selected
		SE02: arrest/blockage of a piece of equipment/item (closing liquid or gas outlet)	Stop of production: recovery follows normal start-up procedures (expected downtime 3h). No damage to people or environment.	[2, 1, 1, 1]	Not selected
		SE03: activation of ESD/PSD/LSD logic	Stop of production: recovery follows normal start-up procedures (expected downtime 6h). No damage to people or environment.	[2, 1, 1, 1]	Not selected
		SE04: exceeding design specification for construction materials	Stop of production: recovery requires repair and replacement of equipment (expected downtime of 2 weeks). No damage to people or environment.	[4, 1, 1, 1]	Selected
		SE06: loss of containment (LOC) and loss of physical integrity (LPI)	Stop of production: recovery requires repair and replacement of equipment (expected downtime of 4 weeks). Resulting fire may damage nearby equipment. No damage to people. Negligible damage to environment.	[4, 2, 1, 1]	Selected
ND02	KO drum KD100 KO drum KD101 Turbine TR100 Compressor CR100 Compressor CR101 Heat exchanger HE100 Heat exchanger HE101 Piping	SE01: product out of specification (pressure)	Stop of production: recovery follows abnormal start-up procedures (expected downtime 3h). No damage to people or environment.	[2, 1, 1, 1]	Not selected
		SE02: arrest/blockage of a piece of equipment/item (stop of electric motor)	Stop of production: recovery follows normal start-up procedures (expected downtime 3h). No damage to people or environment.	[2, 1, 1, 1]	Not selected
		SE03: activation of ESD/PSD/LSD logic	Stop of production: recovery follows normal start-up procedures (expected downtime 6h). No damage to people or environment.	[2, 1, 1, 1]	Not selected
		SE04: exceeding design specification for construction materials	Stop of production: recovery requires repair and replacement of equipment (expected downtime of 2 weeks). No damage to people or environment.	[4, 1, 1, 1]	Selected
		SE05: damage of moving components/machinery	Stop of production: recovery requires repair and replacement of equipment (expected downtime of 4 weeks). High costs for compressor repair and replacement. No damage to people or environment.	[4, 2, 1, 1]	Selected
		SE06: loss of containment (LOC) and loss of physical integrity (LPI)	Stop of production: recovery requires repair and replacement of equipment (expected downtime of 4 weeks). Resulting fire may damage nearby equipment. No damage to people. Negligible damage to environment.	[4, 2, 1, 1]	Selected

Note: no damage to people is considered as expected consequence of any SE since the platform is normally unmanned.

The credible mechanisms of action (MAs) by means of which an attacker can initiate any of the selected SEs for the node ND02, were identified (Step 7 of the methodology). The identification was based on the applicable categories of mechanisms of action (CMAs) provided in Table A.4 of the Appendix. The list of MAs was generated tailoring the CMAs to the process equipment and items that are present in the node ND02.

Table 4 summarizes the results obtained from Step 7. For example, MA4 (inducing excessive pressure by closing the gas outlets), MA5 (inducing excessive pressure by increasing the rotation speed of the gas turbine), and a combination of these two (MA6), are some of the MAs that may initiate SE04 (exceeding design specification for construction materials), all related to CMA14 (material damage by load). All the identified MAs will be at the basis for the definition of the combination of local consequences (CMs) in the next step.

The analysis carried out and the results of an available HazOp study evidenced that some CMAs identified can be obtained manipulating the nearby node ND01. In particular, CMA18 (inducing component failure of moving systems) can be obtained through the mechanism of action MA8 (liquid fraction in the compressor suction line) which needs the manipulation of RMCs on ND01. This deviation, propagating among the two nodes, was tracked by re-selecting SE01, i.e. “product out of specification”, and more specifically in this case “liquid fraction in the gas outlet”, for the node ND01. A “virtual RMC” (vRMC100) was then added to ND02, representing the RMCs allocated to ND01 that need to be manipulated in order to initiate such security event (i.e. SDV102 or LV100). Similarly, another virtual RMC (vRMC101), corresponding to the RMCs associated to the cooling system, was included in the list of the node ND02: in facts, a damage to the construction material of the equipment by temperature in ND02 (CMA13) is deemed possible through an induced unavailability of the cooling system (mechanism of action MA3). However, the node corresponding to the cooling system was not further developed in the current case study for sake of brevity.

No suitable MA was identified for SE04 and SE06 of node ND01 (not reported in Table 4): the specific features of the equipment present in this node and the processed fluids do not allow many of the mechanisms listed in Table A.4 (e.g. no change of temperature is possible, pressure from upstream lines is always lower than design pressure).

Table 4. Mechanism of action (MAs) identified for SE in the nodes ND01 and ND02. Names of plant items are referred to Figure 5.

Node	SE	CMA code (Step 7)	MA code (Step 7)
ND01	SE01: product out of specification (liquid fraction in the gas outlet)	CMA25: over-filling	MA1: over-filling of SC100 by closing the liquid outlet
ND02	SE04: exceeding design specification for construction materials	CMA13: material damage by temperature	MA2: increasing temperature by closing the cooling water line in HE100 and HE101 MA3: increasing temperature by making the cooling water unavailable
		CMA14: material damage by load	MA4: inducing excessive pressure by closing the gas outlet from HE101 MA5: inducing excessive pressure by increasing the rotation speed of the GAS TURBINE MA6: inducing excessive pressure by closing the gas outlet from HE101 + increasing rotation speed of the GAS TURBINE
	SE05: damage of moving components/machinery	CMA18: inducing component failure of moving systems	MA7: start and stop cycles or speed variation cycles of the GAS TURBINE by manipulating the fuel gas feed and the electric starter motor MA8: liquid fraction in CR100 and CR101 suctions by over-filling KD100 and KD101
		CM19: exceeding operative limits (surge limit)	MA4: inducing excessive pressure by closing the gas outlet from HE101 MA5: inducing excessive pressure by increasing the rotation speed of the GAS TURBINE MA6: inducing excessive pressure by closing the gas outlet from HE101 + increasing rotation speed of the GAS TURBINE
	SE06: loss of containment (LOC) and loss of physical integrity (LPI)	CMA23: damage of the construction material of the containment system	MA4: inducing excessive pressure by closing the gas outlet from HE101 MA5: inducing excessive pressure by increasing the rotation speed of the GAS TURBINE MA6: inducing excessive pressure by closing the gas outlet from HE101 + increasing rotation speed of the GAS TURBINE
		CMA24: damage of moving components in the containment system	MA7: start and stop cycles or speed variation cycles of the GAS TURBINE by manipulating the fuel gas feed and the electric starter motor MA8: liquid fraction in CR100 and CR101 suctions by over-filling KD100 and KD101

Table 5 shows the results obtained in the assessment of Step 8 (identification of combinations of local consequences, CMs) and Step 9 (identification of effective active/procedural, and inherent/passive safeguards, APSs and IPSs) of the methodology for both the nodes ND01 and ND02.

For the sake of brevity, only the RMCs (and virtual RMCs) that need to be manipulated in at least one CM are shown in the table. In some cases, the manipulation of alternative RMCs is possible to achieve the same effect on the physical process (it is generally the case of a control valve and a shutdown valve on the same process stream). For example, an attacker can increase the outlet temperature from HE100 or HE101 either by closing one or both the control valves TV100 and TV101 (MA2) through the change (increase) of the setpoint of the corresponding controller (with consequent decrease in valves opening degree, LC8), or alternatively, by making unavailable the cooling water system (i.e. manipulation of the virtual component vRMC101, MA3).

With respect to the identification of the effective safeguards (Step 9 of the methodology), taking as an example CM2.5 (see Table 5), the APSs that were identified through the revision of the P&IDs and relevant documentation are the LSD/PSD logics activated by PSHHs, the high and very high pressure alarms PAHs, the hand switch (HS) for manual activation of ESD/PSD/LSD logic, the position light for closed position (ZLL) of SDV105, the HS for its manual reset and the anti-surge loop, while the IPSs are the pressure safety valve PSV100, PSV101 and PSV102 (see Figure 5).

Table 5. List of combinations (CMs) of local consequences (LCs) on the relevant RMCs for each MA of the nodes ND01 and ND02. For each CM, effective active/procedural safeguards (APSs) and inherent/passive safeguards (IPSs) are reported.

Node	MA code	CM code (Step 8)	Relevant RMCs and LCs (Step 8)	Effective APSs (Step 9)	Effective IPSs (Step 9)
ND01	MA1	CM1.1	SDV102 totally closed (LC2)	PSD logic activated by LSHH on SC100 High level alarm LAH on SC100 + HS for manual ESD/PSD/LSD Very high level alarm LAHH on SC100 + HS for manual ESD/PSD/LSD Position light ZLL for SDV105 + HS for manual reset of SDV105	None
		CM1.2	LV100 partially or totally closed (LC8 or LC2)	PSD logic activated by LSHH on SC100 High level alarm LAH on SC100 + HS for manual ESD/PSD/LSD Very high level alarm LAHH on SC100 + HS for manual ESD/PSD/LSD	None
ND02	MA2	CM2.1	TV100 partially or totally closed (LC8 or LC2)	High temperature alarms TAHs + HS for manual ESD/PSD/LSD Very high temperature alarms TAHHs + HS for manual ESD/PSD/LSD	None
		CM2.2	TV101 partially or totally closed (LC8 or LC2)	High temperature alarms TAHs + HS for manual ESD/PSD/LSD Very high temperature alarms TAHHs + HS for manual ESD/PSD/LSD	None
		CM2.3	TV100 partially or totally closed (LC8 or LC2) TV101 partially or totally closed (LC8 or LC2)	High temperature alarms TAHs + HS for manual ESD/PSD/LSD Very high temperature alarms TAHHs + HS for manual ESD/PSD/LSD	None
	MA3	CM2.4	vRMC101 manipulated (unavailable cooling water)	High temperature alarms TAHs + HS for manual ESD/PSD/LSD Very high temperature alarms TAHHs + HS for manual ESD/PSD/LSD APSs present in the cooling system	None
	MA4	CM2.5	SDV105 totally closed (LC2)	LSD/PSD logics activated by PSHHs and Anti-Surge system High pressure alarms PAHs + HS for manual ESD/PSD/LSD Very high pressure alarms PAHHs + HS for manual ESD/PSD/LSD Position light ZLL for SDV105 + HS for manual reset of SDV105	PSV101 PSV102 PSV103
	MA5	CM2.6	GAS TURBINE with increased rotational speed (LC10)	LSD/PSD logics activated by PSHHs and Anti-Surge system High pressure alarms PAHs + HS for manual ESD/PSD/LSD Very high pressure alarms PAHHs + HS for manual ESD/PSD/LSD	PSV101 PSV102 PSV103
	MA6	CM2.7	SDV105 totally closed (LC2) GAS TURBINE with increased rotational speed (LC10)	LSD/PSD logics activated by PSHHs and Anti-Surge system High pressure alarms PAHs + HS for manual ESD/PSD/LSD Very high pressure alarms PAHHs + HS for manual ESD/PSD/LSD Position light ZLL for SDV105 + HS for manual reset of SDV105	PSV101 PSV102 PSV103
	MA7	CM2.8	GAS TURBINE started and stopped cyclically (LC14)	LSD logic activated by Anti-Surge system GAS TURBINE unavailability alarm UA + HS for manual ESD/PSD/LSD	None

Table 5 (continued). List of combinations (CMs) of local consequences (LCs) on the relevant RMCs for each MA of the nodes ND01 and ND02. For each CM, effective active/procedural safeguards (APSs) and inherent/passive safeguards (IPSs) are reported.

Node	MA code	CM code (Step 8)	Relevant RMCs and LCs (Step 8)	Effective APSs (Step 9)	Effective IPSs (Step 9)
ND02	MA8	CM2.9	SDV103 totally closed (LC2) vRMC100 manipulated (see MA1)	PSD logic activated by LSHH on SC100 LSD logic activated by LSHHs on KD100 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 SDV103 + HS for manual reset of SDV103 (if manipulated) Position light ZLL for SDV102 + HS for manual reset of SDV102	None
		CM2.10	LV101 partially or totally closed (LC8 or LC2) vRMC100 manipulated (see MA1)	PSD logic activated by LSHH on SC100 LSD logic activated by LSHHs on KD100 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 (if manipulated) Position light ZLL for SDV102 + HS for manual reset of SDV102	None

6. Discussion

Although the results of the case study should not be directly generalized, they demonstrate that, besides inducing a Process Shut Down (PSD) or a production outage, malicious manipulations of the control system may induce more severe scenarios, as equipment damage and/or major accidents. This applies not only to equipment in the process section of the plant, but also to utilities and services (e.g. instrument air, power supply or cooling water). While an induced shutdown of an essential service leads to consequences similar to the shutdown of the process area, inducing damage (e.g. SE04, SE05, SE06) in these units may result in a prolonged downtime of the entire plant, with consequences that exceed the direct repair cost of the damaged units. This may be of particular interest for attackers aiming at causing economic value or influence value losses for the company, but characterized by a non-violent beliefs (i.e. no human value or environmental value losses). Moreover, if shutdown procedures are inhibited by the attacker, the manipulation of utilities may also lead to widespread consequences around the plant. This is the case of manipulations to the cooling water system in the case study, which may lead to compressor damage in node ND02.

As evidenced by the case study, POROS supports the systematic identification of all the possible SEs, but also the selection of a limited number of SEs for a more in-depth assessment. While generic security and cybersecurity countermeasures (e.g. well-configured firewalls, patched software, presence of AV software, user authentication, network segmentation, etc.) are able to appropriately prevent all the SEs, including those with low severity, specific measures, providing a redundancy and thus increasing the level of protection, can be identified for the high severity SEs. As shown in the case study, the analysis of the MAs for the selected cases allows the identification of RMCs that may require targeted implementation of additional countermeasures and/or safer plant design (inherent safety).

The guideline tables from A.2 to A.4 provided in the Appendix were found adequate for the definition of all the code classes required throughout the POROS application to the case study (SE, RMC, ME, RM, LC, MA), confirming their use to achieve of repeatable results and low subjectivity in the assessment of oil & gas operations.

Table 5 shows that, in some cases, relatively few remote manipulable components (RMCs) need to be manipulated in order to execute a mechanism of action (MA) that can initiate a high severity security event (SE). Many CMs consist of a single manipulated component: it is the case of 7 out of 12 combinations identified through POROS analysis (Table 5). This is obviously not in favour of security, since attackers must not carry out a complicated attack pattern in order to affect the operability and/or the physical integrity of the target system.

In cases where the manipulation of a single RMC is required to carry out a MA, the attacker apparently needs to infect only the BPCS or the SIS for a successful action. For example, in the case study CM1.1 is obtained by manipulating the PLC connected to the SIS in order to close SDV102, and CM2.1 is achieved by manipulating the PID controller of the BPCS that control the valve TV100. However, SEs as those shown in Table A.4 in the Appendix, are prevented by specific safeguards in the process system. If active and/or procedural safeguards are present, the attacker needs to manipulate the SIS in order to prevent a safe response of the system. This, combined with the presence of CMs involving only RCMs controlled by the SIS, makes the latter system the most critical element of the automation system as regards attacks aiming at severe SEs. This leads to a possible conflict between instrumented safety and security issues, which deserves appropriate assessment. On the other hand, physical safeguards (e.g. pressure safety valves, rupture disks, catch basins, etc.), as they do not contain RCMs, can not be manipulated through an attack to the IT-OT system and, therefore, they can be considered fully effective in avoiding the SE in case of proper design. Hence, the proper sizing of inherent/passive safeguards must consider security cases that can be generated through the

malicious manipulation of the BPCS and the SIS systems (e.g. considering the cyber-attack scenario in addition to those reported in API standard 521 [59] for the sizing of PSVs). However, as evidenced from the results of the case study, IPSs may be effective only for the prevention and mitigation of some of the MAs (e.g. those involving pressure or temperature out of design specifications, while no IPSs was identified in other cases, e.g. to prevent the overfill of ND01).

Procedural safeguards (e.g. manual resets for shut-off valves controlled by the SIS, hand switches for manual stop of operating machines, alarms, position lights, etc.) share with automated safeguards the possibility to be de-activated by an attacker. However, as shown by the results in Table 5, a large number of elements belonging to procedural safety exist for each MA, if compared to the active and passive safeguards. This seems to suggest that a high level of complexity of the CMA is needed to de-activate all of them, requiring a detailed knowledge of updated process details, reasonably possible only when the attack involves insiders. Therefore, it can be argued that procedural safeguards may play as well a role in preventing a SE, though they may be negatively affected by human reliability factors.

Table 6 presents how the results of POROS can support the definition of the IT-OT protection requirements for the elements that act on the physical components of the plant (i.e. the manipulative elements, MEs) according to ISA/IEC 62443. The risk assessment described in ISA/IEC 62443-3-2 divides the IT-OT system into separate zones (i.e. grouping of logical or physical assets based upon risk or other criteria [26]) and conduits (i.e. logical grouping of communication channels that share common security requirements connecting two or more zones [26]), and defines for each zone/conduit the security level target required for tolerable risk. The assessment of proposed countermeasures (i.e. safeguards in the IT-OT system) and the design of additional ones is based on this information. The definition of the security level target also requires an evaluation of "worst-case impact on risk areas as personnel safety, financial loss, business interruption and environment" (ISA/IEC 62443-3-2). The severity level for the SEs triggered by a malicious manipulation of MEs belonging to a zone can be used to provide such evaluation.

Table 6 shows the SEs than can be triggered by the manipulation of elements in one zone, as identified by POROS. The worst-case SE severity can be taken as a reference severity for the security level target definition of the zone. As discussed above, sometimes manipulation of elements belonging to different zones may be required to cause the worst-case SE, making the attack more complex and, possibly, decreasing likelihood. Thus, the division of IT-OT system in smaller zones can be identified as a good strategy to reduce the risks of concern in the current assessment. Table 6 shows that only a limited number of all the SIS elements require high levels of security: the definition of smaller zones with dedicated countermeasures, when possible, may lead to a more effective protection of these parts of the OT system, allowing less stringent requirement to be applied to the rest of the system.

Although the division into zones and conduits of the network system suggested by ISA/IEC 62443 lead to the advantages discussed above, they may affect the operational reliability of the overall system [60]. In fact, when interdependent subsystems are required to work together for maintaining regular operation, the introduction of segregation and barriers may increase the probability of failures, reducing system availability. This can be critical in case of the SIS system since it executes safety functions, where given performances of reliability shall be met (e.g. SIL rating as for IEC 61511). Thus, a cost-benefit analysis of the separation of the network system into smaller zones and conduits that take into account both advantages in terms of system safety/security and disadvantages in terms of system operational reliability is of central importance and it will be part of future research.

Other areas of future research which will complement the findings of the current study concern the development of a quantitative approach to assess the probability of success of a cyber-attack aiming at interfering with the operability / system integrity of a process plant. This study will benefit

from a clear identification of the CMs, APS and IPS provided by current methodology, which define the attacker path to be contrasted.

A further issue concerns the automation of the procedure. As discussed above, POROS consists in a structured step-by-step procedure, similar to well-known procedures of HazOp, Hazid and FMEA [42][43]. This framework, which sets the basis of the systematic and formally rigorous nature of POROS methodology, leads to the possibility of its implementation by dedicated software tools supporting an automated or semi-automated assessment. Actually, most of the required input information is available in document management tools nowadays more and more frequently used in the process industry, and a wide range of similar tools for automated or semi-automated hazard identification techniques (including the HazOp analysis) exists. The automation of the procedure is expected to be particularly valuable in complex projects, where it allows for an easier and more practical application [56]. Examples of similar tools are the automated security risk identification using AutomationML-based engineering data developed by Eckhart et al. [61], and the automated tool for batch hazard and operability studies developed by Palmer and Chung [62]. A description of the models for automated and semi-automated HazOp analyses are present in the literature review performed by Taylor J.R [63]. Given the similarities that the POROS methodology shares with the HazOp analysis, it is envisaged that these may be reflected also in the core-structures of the automated models, or at least in some parts of them.

Table 6. Information for ISA/IEC 62443 3-2 (step ZCR 5.8 e 5.12) provided by POROS.

Zones	SEs	Severity vector [EC, IV, EN, HV]	RMCs belonging to the current Zone	Active safeguards belonging to the current Zone	Active safeguards belonging to other Zones
Zone 1: BPCS-1 (gas turbine - control)	ND02-SE04 (material damaged by load)	[4, 1, 1, 1]	GAS TURBINE	None	LSD/PSD logics activated by PAHHs (Zone 3) LSD/PSD logic activated by Anti-Surge (Zone 3)
	ND02-SE05 (gas turbine damaged by surge)	[4, 2, 1, 1]	GAS TURBINE	None	LSD/PSD logics activated by PAHHs (Zone 3) LSD/PSD logic activated by Anti-Surge (Zone 3)
	ND02-SE05 (gas turbine damaged by start/stop cycles)	[4, 2, 1, 1]	GAS TURBINE	None	LSD/PSD logic activated by Anti-Surge (Zone 3)
Zone 2: BPCS-2 (rest of the plant - control)	ND02-SE04 (material damaged by temperature)	[4, 1, 1, 1]	TV100, TV101	None	None
	ND02-SE05 (gas turbine damaged by liquid)	[4, 2, 1, 1]	LV100, LV101	None	PSD logic activated by LSHH on SC100 (Zone 4) LSD logic activated by LSHHs on KD100 (Zone 4)
Zone 3: SIS-1 (gas turbine - safety)	ND02-SE04 (material damaged by load)	[4, 1, 1, 1]	GAS TURBINE	LSD/PSD logic activated by Anti-Surge	LSD/PSD logics activated by PAHHs (Zone 4)
	ND02-SE05 (gas turbine damaged by surge)	[4, 2, 1, 1]	GAS TURBINE	LSD/PSD logic activated by Anti-Surge	LSD/PSD logics activated by PAHHs (Zone 4)
	ND02-SE06 (ND02-SE05/ND02-SE04 + LOC or LPI)	[4, 2, 1, 1]	GAS TURBINE	LSD/PSD logic activated by Anti-Surge	LSD/PSD logics activated by PAHHs (Zone 4)
	ND02-SE05 (gas turbine damaged by start/stop cycles)	[4, 2, 1, 1]	GAS TURBINE	LSD/PSD activated by Anti-Surge	None
	ND02-SE06 (ND02-SE05 + LOC or LPI)	[4, 2, 1, 1]	GAS TURBINE	LSD/PSD activated by Anti-Surge	None
Zone 4: SIS-2 (rest of the plant - safety)	ND02-SE04 (material damaged by load)	[4, 1, 1, 1]	SDV105	LSD/PSD logics activated by PAHHs	LSD/PSD logic activated by Anti-Surge (Zone 3)
	ND02-SE05 (gas turbine damaged by surge)	[4, 2, 1, 1]	SDV105	LSD/PSD logics activated by PAHHs	LSD/PSD logic activated by Anti-Surge (Zone 3)
	ND02-SE06 (ND02-SE05/ND02-SE04 + LOC or LPI)	[4, 2, 1, 1]	SDV105	LSD/PSD logics activated by PAHHs	LSD/PSD logic activated by Anti-Surge (Zone 3)
	ND02-SE05 (gas turbine damaged by liquid)	[4, 2, 1, 1]	SDV102, SDV103	PSD logic activated by LSHH on SC100 LSD logic activated by LSHH on KD100	None
	ND02-SE06 (ND02-SE05 + LOC or LPI)	[4, 2, 1, 1]	SDV102, SDV103	PSD logic activated by LSHH on SC100 LSD logic activated by LSHH on KD100	None

7. Conclusions

POROS is a systematic qualitative methodology aiming at the security assessment of the link between malicious manipulations of the BPCS and the SIS, addressing the impacts that can affect the operability and/or system integrity of the target process plant (e.g. interruption of productivity, asset damage, damage to people, environment or reputation). The methodology identifies the sets of remote manipulations that can lead to such adverse impacts, pinpointing the critical components of the plant and the effective physical and automated safeguards against such manipulations. This allows for establishing the adequate security level in the design of the IT-OT system against cyber threats.

The results of the case study carried out, addressing an offshore Oil&Gas compression plant, evidence that the cyber threat to process plants is not limited only to conventional impacts common to all services and sectors, as data theft or corruption, but also to specific and potentially more severe impacts, as induced production outage and asset damage. These scenarios are possible when the attackers succeed in affecting the BPCS and the SIS systems of the target process facility. The results remark the importance of taking into account security issues as well as safety issues when designing both the network architecture and the process plant in order to implement effective "defence in depth" strategies for these threats.

Overall, the results obtained confirm that POROS can support the identification of consequences and impacts associated to cyber threats, as well as the definition of the protection requirements and countermeasures for the manipulative elements of the plant (e.g. controllers and logics) according to international standards (e.g. ISA/IEC 62443).

The methodology developed paves the way to future developments in strategies for a more secure OT system architecture design (e.g. zone and conduit segregation) and supports quantitative approaches for assessing the probability of success of a cyber-attack aiming at interfering with the operability / system integrity of a process plant.

Acknowledgments

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

References

[1] Casson Moreno V, Reniers G, Salzano E, Cozzani V. Analysis of physical and cyber security-related events in the chemical and process industry. Process Saf Environ Prot 2018;116:621–31. https://doi.org/10.1016/j.psep.2018.03.026

[2] Thomas HW, Day J. Integrating Cybersecurity Risk Assessments Into the Process Safety Management Work Process. 49th Annu. Loss Prev. Symp. 2015, LPS 2015 - Top. Conf. 2015 AIChE Spring Meet. 11th Glob. Congr. Process Saf., 2015; p. 360–378.

[3] National Institute of Standards and Technology (NIST). Glossary of Key Information Security Terms. 2nd ed. Gaithersburg: 2013.

[4] Behrendt A, Müller N, Odenwälder P, Schmitz C. Industry 4.0 demystified-lean's next level. McKinsey & Company, https://www.mckinsey.com/business-functions/operations/our-insights/industry-4-0-demystified-leans-next-level; 2017 [accessed 22 January 2019].

[5] Hausken K, Levitin G. Minmax defense strategy for complex multi-state systems. Reliab Eng Syst Saf 2009;94:577–87. https://doi.org/10.1016/j.ress.2008.06.005.

[6] Allianz Global Corporate & Specialty. Allianz Risk Barometer. Top Business Risks for 2018; 2018.

[7] Hausken K. Cyber resilience in firms, organizations and societies. Internet of Things 2020;11:100204. https://doi.org/10.1016/j.iot.2020.100204.
[8] Hausken K. The precautionary principle as multi-period games where players have different thresholds for acceptable uncertainty. Reliab Eng Syst Saf 2021;206:107224. https://doi.org/10.1016/j.ress.2020.107224.
[9] Cullen A, Armitage L. A human vulnerability assessment methodology. 2018 Int. Conf. Cyber Situational Awareness, Data Anal. Assessment, CyberSA 2018, Institute of Electrical and Electronics Engineers Inc.; 2018. https://doi.org/10.1109/CyberSA.2018.8551371.
[10] Hausken K. Security Investment, Hacking, and Information Sharing between Firms and between Hackers. Games 2017;8:23. https://doi.org/10.3390/g8020023.
[11] Ritchie C. A Look at the Security of the Open Source Development Model. Corvallis: United States: 2000.
[12] Kunreuther H, Heal G. Interdependent Security. J Risk Uncertain 2003;26:231–49. https://doi.org/10.1023/A:1024119208153.
[13] Iaiani M, Tugnoli A, Bonvicini S, Cozzani V. Analysis of Cybersecurity-related Incidents in the Process Industry. Reliab Eng Syst Saf 2021;209:107485. https://doi.org/10.1016/j.ress.2021.107485.
[14] Department of Homeland Security. RISI - The Repository of Industrial Security Incidents, https://www.risidata.com/Database [accessed 10 December 2019].
[15] Creighton J. A Dangerous Cyberattack On A Petrochemical Plant Could Be The First Of Many. Cyberwarfare won't just be restricted to our digital lives. Futurism, https://futurism.com/saudi-arabia-cyberattack; 2018 [accessed 17 January 2020].
[16] Cutter SL, Ahearn JA, Amadei B, Crawford P, Eide EA, Galloway GE, et al. Disaster Resilience: A National Imperative. Environ Sci Policy Sustain Dev 2013;55:25–9. https://doi.org/10.1080/00139157.2013.768076.
[17] Bostick TP, Connelly EB, Lambert JH, Linkov I. Resilience science, policy and investment for civil infrastructure. Reliab Eng Syst Saf 2018;175:19–23. https://doi.org/10.1016/j.ress.2018.02.025.
[18] Bier V, Gutfraind A. Risk analysis beyond vulnerability and resilience – characterizing the defensibility of critical systems. Eur J Oper Res 2019;276:626–36. https://doi.org/10.1016/j.ejor.2019.01.011.
[19] Jaeger CD. Vulnerability Assessment Methodology for Chemical Facilities (VAM-CF). Chem Heal Saf 2002;9(6):15–9. https://doi.org/10.1016/S1074-9098(02)00389-1
[20] American Institute of Chemical Engineers, Center of Chemical Process Safety (AIChE-CCPS). Guidelines for analysing and managing the security vulnerabilities of fixed chemical sites. New York: American Institute of Chemical Engineers, Center of Chemical Process Safety; 2003.
[21] American Petroleum Institute (API). ANSI/API 780 standard – Security risk assessment methodology for the petroleum and petrochemical industry. New York: American Petroleum Institute; 2013.
[22] Matteini A, Argenti F, Salzano E, Cozzani V. A comparative analysis of security risk assessment methodologies for the chemical industry. Reliab Eng Syst Saf 2019;191. https://doi.org/10.1016/j.ress.2018.03.001.
[23] International Organization for Standardization, International Electrotechnical Commission (ISO-IEC). ISO/IEC 27000 series of standards: Information technology - Security techniques - Information security management systems. International Organization for Standardization, International Electrotechnical Commission; 2018.
[24] Gordon LA, Loeb MP. The Economics of Information Security Investment. ACM Trans Inf

Syst Secur 2002;5:438–57. https://doi.org/10.1145/581271.581274.
[25] International Society of Automation, International Electrotechnical Commission (ISA/IEC). ISA/IEC 62443 series of standards: Industrial Automation and Control Systems Security. International Society of Automation, International Electrotechnical Commission; 2018.
[26] International Society of Automation, International Electrotechnical Commission (ISA/IEC). ISA/IEC 62443-3-2 standard: Security for industrial automation and control systems - Part 3-2: Security risk assessment and system design. International Society of Automation, International Electrotechnical Commission 2018.
[27] Brewer DFC. Applying security techniques to achieving safety. In: Redmill F., Anderson T. (eds) Directions in Safety-Critical Systems. Springer, London; 1993, p. 246–256. https://doi.org/10.1007/978-1-4471-2037-7_16
[28] Eames DP, Moffett J. The Integration of Safety and Security Requirements. In: Felici M., Kanoun K. (eds) Computer Safety, Reliability and Security. SAFECOMP 1999. Lecture Notes in Computer Science, vol 1698. Springer, Berlin, Heidelberg; 1999, p. 468–480. https://doi.org/10.1007/3-540-48249-0_40
[29] Firesmith D. Common Concepts Underlying Safety, Security, and Survivability Engineering 2018. https://doi.org/10.1184/R1/6572621.v1
[30] Kriaa S, Pietre-Cambacedes L, Bouissou M, Halgand Y. A survey of approaches combining safety and security for industrial control systems. Reliab Eng Syst Saf 2015;139:156–178. https://doi.org/10.1016/j.ress.2015.02.008
[31] Sørby K. Relationship between security and safety in a security-safety critical system: Safety consequences of security threats. MSc Thesis 2003.
[32] Baybutt P. Issues for security risk assessment in the process industries. J Loss Prev Process Ind 2017;49:509–18. https://doi.org/10.1016/J.JLP.2017.05.023.
[33] Byres EJ, Franz M, Miller D. The Use of Attack Trees in Assessing Vulnerabilities in SCADA Systems. Proc Int Infrastruct Surviv Work 2004.
[34] Gertman D, Folkers R, Roberts J. Scenario-based approach to risk analysis in support of cyber security. Proc 5th Int Top Meet Nucl Plant Instrum Control Hum Mach Interface Technol 2006.
[35] Beggs C, Warren M. Safeguarding Australia from cyber-terrorism: a proposed cyber-terrorism SCADA risk framework for industry adoption. Aust Inf Warf Secur Conf 2009.
[36] Song JG, Lee JW, Lee CK, Kwon KC, Lee DY. A cyber security risk assessment for the design of L&C systems in nuclear power plants. Nucl Eng Technol 2012;44:919–28. https://doi.org/10.5516/NET.04.2011.065.
[37] Guan J, Graham JH, Hieb JL. A digraph model for risk identification and mangement in SCADA systems. Proc. 2011 IEEE Int. Conf. Intell. Secur. Informatics, ISI 2011, 2011, p. 150–5. https://doi.org/10.1109/ISI.2011.5983990.
[38] Hashimoto Y, Toyoshima T, Yogo S, Koike M, Hamaguchi T, Jing S, et al. Safety securing approach against cyber-attacks for process control system. Comput Chem Eng 2013;57:181–186. https://doi.org/10.1016/j.compchemeng.2013.04.019
[39] Abdo H, Kaouk M, Flaus JM, Masse F. A safety/security risk analysis approach of Industrial Control Systems: A cyber bowtie – combining new version of attack tree with bowtie analysis. Comput Secur 2018;72:175–195. https://doi.org/https://doi.org/10.1016/j.cose.2017.09.004
[40] Cusimano J, Rostick P. If It Isn't Secure, It Isn't Safe: Incorporating Cybersecurity into Process Safety. AIChE Spring Meet Glob Congr Process Saf 2018.
[41] DIN VDE V 0831-104: Elektrische Bahn-Signalanlagen - Teil 104: Leitfaden für die IT-Sicherheit auf Grundlage IEC 62443. 2015.

[42] International Electrotechnical Commission (IEC). IEC 61882 standard: Hazard and operability studies (HAZOP studies) - Application guide. International Electrotechnical Commission; 2016.
[43] Paltrinieri N, Tugnoli A, Buston J, Wardman M, Cozzani V. Dynamic Procedure for Atypical Scenarios Identification (DyPASI): A new systematic HAZID tool. J Loss Prev Process Ind 2013;26(4):683–695. https://doi.org/10.1016/j.jlp.2013.01.006
[44] Hausken K, Levitin G. Review of systems defense and attack models. Int J Performability Eng 2012;8:355–66.
[45] International Organization for Standardization, International Electrotechnical Commission (ISO-IEC). ISO/IEC 27005: Information technology - Security techniques - Information security risk management 2018.
[46] Delvosalle C, Fievez C, Pipart A, Debray B. ARAMIS project: A comprehensive methodology for the identification of reference accident scenarios in process industries. J Hazard Mater 2006;130(3):200–219. https://doi.org/10.1016/j.jhazmat.2005.07.005
[47] Tugnoli A, Landucci G, Salzano E, Cozzani V. Supporting the selection of process and plant design options by Inherent Safety KPIs. J Loss Prev Process Ind 2012;25(5):830–842. https://doi.org/10.1016/j.jlp.2012.03.008
[48] American Petroleum Institute (API). API RP 581 standard: Risk-Based Inspection Technology. American Petroleum Institute; 2016.
[49] Uijt de Haag PAM, Ale BJM. Guidelines for Quantitative Risk Assessment (Purple Book). The Hague, The Netherlands: Committee for the Prevention of Disasters; 1999.
[50] Center for Chemical Process Safety (CCPS). Guidelines for hazard evaluation procedures. 3rd ed. New York: Wiley/AlChE; 2008.
[51] Baybutt P. Guidelines for designing risk matrices. Process Saf Prog 2018;37:49–55. https://doi.org/10.1002/prs.11905.
[52] Center for Chemical Process Safety (CCPS). Process Safety Leading and Lagging Metrics. "You don't improve what you don't measure". Center for Chemical Process Safety; 2011.
[53] Hausken K. A cost–benefit analysis of terrorist attacks. Def Peace Econ 2018;29:111–29. https://doi.org/10.1080/10242694.2016.1158440.
[54] Bschir K. Risk, Uncertainty and Precaution in Science: The Threshold of the Toxicological Concern Approach in Food Toxicology. Sci Eng Ethics 2017;23:489–508. https://doi.org/10.1007/s11948-016-9773-2.
[55] Koch FH, Yemshanov D, McKenney DW, Smith WD. Evaluating critical uncertainty thresholds in a spatial model of forest pest invasion risk. Risk Anal 2009;29:1227–41. https://doi.org/10.1111/j.1539-6924.2009.01251.x.
[56] Mannan S. Lees' Loss Prevention in the Process Industries: Hazard Identification, Assessment and Control. 4th ed. UK: Butterworth-Heinemann: Elsevier; 2012.
[57] Kletz T and Amyotte P. Process Plants: A Handbook for Inherent Safer Design. 2nd ed. Philadelphia, PA: Taylor & Francis; 1998.
[58] Meier F, Meier C. Valve fail action. International Society of Automation, https://www.isa.org/standards-and-publications/isa-publications/intech-magazine/2008/august/automation-basics-valve-fail-action/; 2008 [accessed 20 February 2020].
[59] American Petroleum Institute (API). API 521 standard: Pressure-Relieving and Depressuring Systems. American Petroleum Institute; 2014.
[60] Center for Chemical Process Safety (CCPS). CCPS Process Safety Glossary

[61] Eckhart M, Ekelhart A, Weippl ER. Automated Security Risk Identification Using AutomationML-based Engineering Data. IEEE Trans Dependable Secur Comput 2020. https://doi.org/10.1109/tdsc.2020.3033150.
[62] Palmer C, Chung PWH. An automated system for batch hazard and operability studies. Reliab Eng Syst Saf 2009;94:1095–106. https://doi.org/10.1016/j.ress.2009.01.001.
[63] Taylor JR. Automated HAZOP revisited. Process Saf Environ Prot 2017;111:635–51. https://doi.org/10.1016/j.psep.2017.07.023.

Appendix

Table A.1. Main general categories proposed for the classification of plant items [46][47].

General categories	Sub-categories	Code
Vessel-like equipment	Atmospheric vessel (storage, process, etc.)	EQ1.1
	Pressurized vessel (storage, column, reactor, etc.)	EQ1.2
	Mobile vessel (tank wagon, road tanker)	EQ1.3
Tube bundle equipment	S&T heat exchanger, reactor, etc.	EQ2.1
Plate and frame equipment	Filter, plate heat exchanger, etc.	EQ3.1
Pipe	Pipeline, manifold, loading arm, etc.	EQ4.1
Pumping equipment	Pump (centrifuge, alternative, etc.)	EQ5.1
	Compressor (centrifuge, alternative, etc.)	EQ5.2
Warehouse	Packed materials (bags, barrels, etc.)	EQ6.1
	Spare materials (piles, etc.)	EQ6.2
Special equipment	Solid handling (conveyors crushers, etc).	EQ7.1
	Other	EQ7.2

Table A.2. Proposed classes for remote manipulable components (RMCs), manipulative elements (MEs) and remote manipulations (RMs).

Remote manipulable component (RMC)	Code	Manipulative element (ME)	Code	Remote manipulation (RM)	Code
Shut-off valve	RMC1	Basic Process Control System device (e.g. PID controller)	ME1	Signal shutdown Setpoint change Function reprogramming	RM1 RM2 RM3
Control valve	RMC2				
Mechanical pump and its driver	RMC3				
Compressor/fan and its driver	RMC4	Safety Instrumented System device (e.g. PLC controller)	ME2	Signal shutdown Function reprogramming	RM1 RM3
Other (e.g. conveyor belts, rotary filters, mills, extruders, rotary furnaces, etc.)	…				

Table A.3. Proposed classes for local consequences (LCs) and their association with RMs.

Remote manipulation (RM)	Local consequence on RMCs (LC)	Code
RM1 to ME1 and ME2	Valve opening (F.O., fail open)	LC1
	Valve closing (F.C., fail close)	LC2
	Valve actuator lock (F.L., fail locked)	LC3
	Indeterminate position of the valve actuator (F.I., fail indeterminate)	LC4
	Stop of the operating machine	LC5
	The operating machine continues to run (as for fail safe specification)	LC6
RM2 to ME1	Increase in valve opening degree, also up to 100%	LC7
	Decrease in valve opening degree, also up to 0%	LC8
	Opening-closing cycles of the valve	LC9
	Increase of the rotational speed of the operating machine	LC10
	Decrease of the rotational speed of the operating machine	LC11
	Cycles of increase-decrease of the rotational speed of the operating machine	LC12
RM3 to ME1 and ME2	Valve opening	LC1
	Valve closing	LC2
	Stop of the operating machine	LC5
	The operating machine continues to run	LC6
	Increase in valve opening degree, also up to 100%	LC7
	Decrease in valve opening degree, also up to 0%	LC8
	Opening-closing cycles of the valve	LC9
	Increase of the rotational speed of the operating machine	LC10
	Decrease of the rotational speed of the operating machine	LC11
	Cycles of increase-decrease of the rotational speed of the operating machine	LC12
	Start of the operating machine	LC13
	Start and stop cycles of the operating machine	LC14

Table A.4. Proposed classes for security events (SEs) and related categories of mechanisms of action (MAs).

Security event (SE)	Category of mechanisms of action (CMA)	Example
SE01: product out of specification	CMA01: composition/phase out of specification	Contamination of the product
	CMA02: temperature out of specification	Excessive viscosity of the product
	CMA03: pressure out of specification	Steam out of specification
	Other	
SE02: arrest/blockage of a piece of equipment/item	CMA04: valve closure/opening	Production stop by closure of a remotely operated block valve Production stop by opening of a remotely operated valve on bypass line Production stop by opening of a remotely operated depressurization valve
	CMA05: motor or driver arrest	Stop of the electric motor of a pump Stop of the electric motor of a compressor Stop of the electric motor of a conveyor
	CMA06: induce the plugging/packing	Alteration of set point controlling the solid/liquid ratio of a slurry Stop of the agitator
	Other	
SE03: activation of ESD/PSD/LSD logic	CMA07: direct activation of ESD/PSD/LSD logic	Generating a false signal from a manual activation button of ESD/PSD/LSD
	CMA08: temperature exceeding safety limits	Change of operative conditions, inducing a TAHH
	CMA09: pressure exceeding safety limits	Change of operative conditions, inducing a PAHH
	CMA10: level exceeding safety limits	Change of operative conditions, inducing a LALL
	CMA11: composition exceeding safety limits	Change of operative conditions, inducing a decrease of pH Change of a reactant dosage in a highly exothermic reaction system
	CMA12: unavailability of essential services	Stop of instrument air generator Inducing failure of the pilot flame of a flaring system
	Other	

Table A.4. (continued). Proposed classes for security events (SEs) and related categories of mechanisms of action (MAs).

Security event (SE)	Category of mechanisms of action (CMA)	Example
SE04: exceeding design specification for construction materials	CMA13: material damage by temperature	Lowering temperature below brittle point Rising temperature above creep condition
	CMA14: material damage by load	Inducing excessive pressure/vacuum Inducing excessive thermal expansion Inducing fatigue failure by load cycles
	CMA15: material damage by chemical incompatibility	Adding corrosive material Adding plasticizer material
	CMA16: material damage by mechanical action	Inducing erosion (excessive solid) Inducing cavitation
	Other	
SE05: damage of moving components/machinery	CMA17: inducing driver failure	Inducing electric motor failure in a pump Inducing membrane actuator failure
	CMA18: inducing component failure of moving systems	Cycling of a valve leading to excessive wearing of seals Stop of lubrication or cooling
	CMA19: exceeding operative limits	Exceeding surge/stonewall limit in a compressor Exceeding low/high flow limits of the pump
	Other	
SE06: loss of containment (LOC) and loss of physical integrity (LPI)	CMA20: induce a thermal or chemical decomposition	Exceeding onset temperature for decomposition
	CMA21: induce an explosion	Mixing incompatible materials
	CMA22: start a fire	Deactivation of inerting system for pyrophoric materials
	CMA23: damage of the construction material of the containment system (see SE04)	See examples in SE04
	CMA24: damage of moving components in the containment system (see SE05)	See examples in SE05
	CMA25: over-filling	Overfilling of an atmospheric storage tank
	Other	
SE07: Other	Other	

Table A.5. Example of classifications of the type of attackers, their motivations, the possible consequences that can be generated, and expected ranges for the severity vector values associated to the possible consequences.

ATTACKER	MOTIVATIONS / PREFERENCES	POSSIBLE CONSEQUENCES	EXPECTED TARGET SEVERITY OF IMPACTS (see Table 1)
Hacker, Cracker, Non-violent hacktivist	Challenge, ego, rebellion, status, monetary gain, media coverage	— Hacking — Social engineering — System intrusion, break-ins — Unauthorized system access	EC: minor (1) to extensive (4) IV: medium (2) to extensive (4) EN: minor (1) HV: minor (1)
Insider	Curiosity, ego, intelligence, monetary gain, revenge	— Assault on an employee — Blackmail — Browsing of proprietary information — Computer abuse — Fraud and theft — Information bribery — Input of falsified, corrupted data — Interception — Malicious code — Sale of personal information — System bugs — System intrusion — System sabotage — Unauthorized system access	EC: medium (2) to extensive (4) IV: medium (2) to extensive (4) EN: minor (1) HV: minor (1)
Nation-state State-sponsored organization	Competitive advantage, economic espionage	— Defence advantage — Political advantage — Economic exploitation — Information theft — Intrusion on personal privacy — Social engineering — System penetration — Unauthorized system access	EC: major (3) to extensive (4) IV: major (3) to extensive (4) EN: major (3) to extensive (4) HV: major (3) to extensive (4)
Terrorist, Violent hacktivist, Cyber-criminal	Destruction, exploitation, revenge, political gain, media coverage	— Bomb/terrorism — Information warfare — System attack — System penetration — System tampering	EC: medium (2) to extensive (4) IV: medium (2) to extensive (4) EN: medium (2) to extensive (4) HV: medium (2) to extensive (4)