CHEMICAL ENGINEERING TRANSACTIONS
VOL. 90, 2022
A publication of AIDIC
The Italian Association of Chemical Engineering
Online at www.cetjournal.it
Guest Editors: Aleš Bernatík, Bruno Fabiano

ISBN 978-88-95608-88-4; **ISSN** 2283-9216
DOI: 10.3303/CET2290069

Risk Identification for Cyber-Attacks to the Control System in Chemical and Process Plants

Matteo Iaiani, Alessandro Tugnoli*, Valerio Cozzani

LISES – Dipartimento di Ingegneria Civile, Chimica, Ambientale e dei Materiali, Alma Mater Studiorum – Università di Bologna, Italy
tugnoli@unibo.it

Cyber-attacks are becoming a growing concern for process facilities that highly rely on Operational Technology (OT) systems for the potential severity of the consequences on humans, assets, and the environment that can be generated. The study is based on the development of synergic tools aimed at filling the gap in the availability of specific approaches to support cyber risk identification phase required by Security Vulnerability/Risk Assessment methodologies and the cybersecurity risk assessment proposed by ISA/IEC 62443 series of standards on cybersecurity of Industrial Automation and Control Systems (IACS).

1. Introduction

Cyber-attacks to the Operational Technology (OT) system of chemical and process facilities, i.e. the Basic Process Control System (BPCS) and the Safety Instrumented System (SIS), are of major concern due to the potential severity of consequences on humans, assets, and the environment, which are comparable to those caused by safety-related causes (Landucci and Reniers, 2019). For example, in 2008 cyber criminals over-pressurized remotely a section of the BTC (Baku-Tbilisi-Ceyan) pipeline causing an explosion, the release of more than 30,000 barrel of oil in an area above a water aquifer, a fire lasting more than two days and outage losses of $5 million a day (RISI database, 2015).
In this panorama, the ISA/IEC 62443 series of standards provide a systematic and practical approach to address cybersecurity issues of Industrial Automation and Control Systems (IACS). In particular, it requires the evaluation of all the impacts (including those on the physical process plant) that can result from intentional malicious attacks to the OT system in order to evaluate the actual level of cyber risk of a facility and implementing proper cybersecurity countermeasures for its reduction. However, neither specific methods nor guidelines are provided to conduct the proposed approach.
Similarly, also the common methodologies dedicated to process plant Security Vulnerability/Risk Assessment (SVA/SRA) such as the VAM-CF methodology, the CCPS methodology, and the one proposed by API RP 780, consider attacks to the BPCS and the SIS in the evaluation, but no specific procedures for assessment of the link between intentional manipulations and consequences is provided (Matteini et al., 2019).
Moreover, few academical contributions devoted to the security of the OT systems of process plants are available in the literature, most of them lacking in reproducibility in application or do not assess the actual link between manipulations and consequences: it is worth to mention the approach to evaluate the detectability and reachability of plant manipulations developed by Hashimto et al. (2013), the approach based on safety/security cyber-bowties proposed by Abdo et al. (2018), and the CyberPHA methodology developed by Cusimano and Rostik (2018).
In the framework outlined, a toolbox was developed to fill the gap in the availability of tools aimed at supporting cyber risk identification in the context of SVA/SRA and cybersecurity risk assessment of ISA/IEC 62443.

Paper Received: 12 January 2022; Revised: 6 March 2022; Accepted: 17 April 2022
Please cite this article as: Iaiani M., Tugnoli A., Cozzani V., 2022, Risk Identification for Cyber-Attacks to the Control System in Chemical and Process Plants, Chemical Engineering Transactions, 90, 409-414 DOI:10.3303/CET2290069

2. Toolbox developed for cyber risk identification

Three synergic tools have been developed in order to support cyber risk identification.

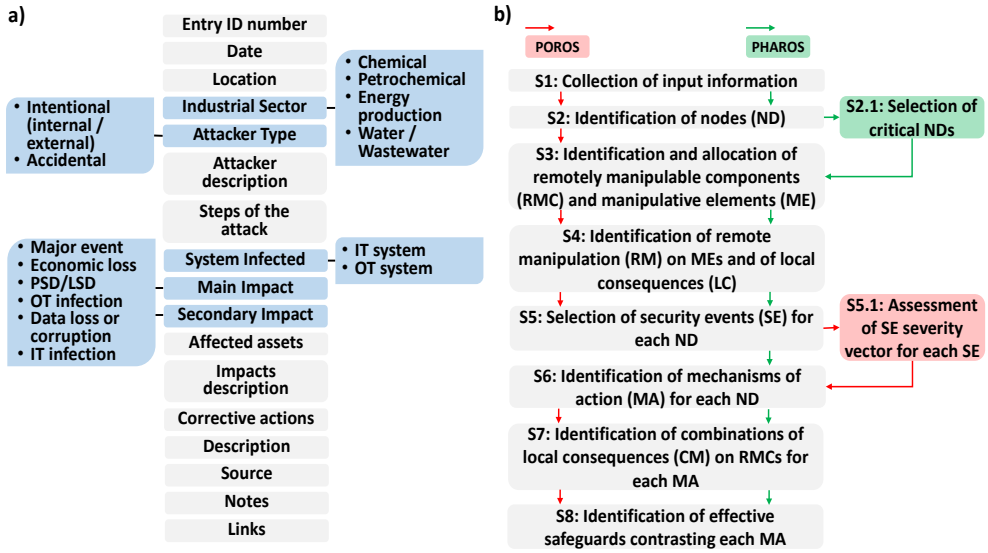

Figure 1: a) Structure of the developed database (grey boxes: free text fields; light blue boxes: itemized fields); b) Flowchart of POROS (red arrows) and PHAROS (green arrows)

The first tool consists in a Past Incident Analysis (PIA) of a dataset of 82 cybersecurity-related incidents (CSIs in the following) occurred worldwide in the process industry and similar sectors from which information of interest and lessons learnt (e.g. on attackers, impacts, cybersecurity countermeasures, etc.) was retrieved by applying Exploratory Data Analysis (EDA). The results of the PIA can be used to define generic cybersecurity-related scenarios that can be employed by authorities and practitioners as a reference starting point to undertake a case specific cybersecurity risk assessment (approach very consolidate in the safety management practice).
The second tool developed is a systematic and formally rigorous methodology, PHAROS (Process Hazard Analysis of Remote manipulations through the cOntrol System), aimed at the identification of the specific set of manipulations of the BPCS and the SIS which may lead to major accident scenarios (i.e. hazardous material and energy releases from plant equipment). Similarly, the third tool developed is POROS (Process Operability analysis of Remote manipulations through the cOntrol System), a methodology with the same core-mechanism of PHAROS, but also aimed at addressing operability issues. Overall, the results from PHAROS and POROS application can be used by a team of experts to perform a case-specific cyber risk identification, to define protection requirements for the safeguards in place (inherent/passive and procedural/active), and to support the design of the network systems (division into zones and conduits) as suggested by ISA/IEC 62443.
Overall, a more complete cyber risk identification is deemed to be can be performed by complementing the results from PIA to the ones that can be obtained through PHAROS and/or POROS assessments. In fact, information regarding potential attackers, their motivations, type of attacks, and IT countermeasures can be retrieved from PIA, while the case-specific plant/process related impacts, the set of manipulations through which they can be generated, the effective physical and automated safeguards, as well as the potential consequences in terms of loss human, economic, influence, and environmental values can be obtained from PHAROS and/or POROS application. In the following sub-sections, the three tools are briefly described.

2.1 Past Incident Analysis

The first step of PIA was the retrieving of the past cybersecurity-related incidents (CSIs). Two criteria were applied: i) the CSI shall originate as a result of an intentional or accidental infection of the network system; and ii) the CSI involves a facility belonging to one of the following industrial sectors: chemical (including pesticides production and pharmaceutical industry), petrochemical (including refineries and Oil&Gas transportation via pipeline), energy production (including nuclear power plants), water/wastewater treatment (including water supply systems). Data were gathered from different sources: scientific literature, the web, and open-source databases on industrial accidents/incidents such as ARIA database, RISI database, Global Terrorism Database, and CSIS proprietary database. Each entry in the database is structured into fields (see Panel-a of Figure 1). Ten "free text fields" allow retaining general details concerning the incident: entry ID number, date, location, description of attacker, steps of the attack, affected assets, description of impacts, corrective actions,

description, source, notes, and links. Four "itemized fields" allow to introduce an unambiguous classification of the CSIs: industrial sector (chemical, petrochemical, energy production, water/wastewater), attacker type (intentional internal, intentional external, accidental); system infected (IT system, OT system), impact (major event, economic loss, PSD/LSD, OT infection, data loss or corruption, IT infection).
The second step of PIA was the analysis of the overall dataset which contains a total of 82 CSIs. In particular, Exploratory Data Analysis (EDA) was used to obtain statistical data regarding the time trend of CSIs, the geographical distribution, the distribution among the industrial sectors, type of attacker and system infected, the impacts of the cyber-attacks, and the most common cybersecurity countermeasures in contrasting an attack. These categorical variables were investigated both singularly and in couples in order to investigate the degree of correlations between them. The detailed method and results obtained from PIA are provided in Iaiani et al. (2021a).

2.2 PHAROS and POROS

PHAROS and POROS, based on a reverse-HazOp concept, require the application of 9 steps (see Panel-b of Figure 1) to be performed by a team with knowledge of the process plant system, the logics of the BPCS and SIS systems, and the loss prevention system. No specific IT-OT skills in the team are required. The input information for the application of the methodologies are: 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 operating conditions of each process unit, the logics of the BPCS and the SIS, and the data sheets of each process unit. The procedure is intended for application to front-end design phase as well as to the security review of operating plants. The core mechanism of both PHAROS and POROS methodologies is graphically show in Figure 2. In particular, an attacker is intended to generate a Security Event (SE, e.g. release) through specific Mechanism of Actions (MAs, e.g. give rise to internal overpressure). In order to do this, he/she has to carrying out Remote Manipulations (RMs, e.g. setpoint change) of the Manipulative Elements (MEs, e.g. controllers and their logics) so that Local Consequences (LCs, e.g. closing/opening) on the Remotely Manipulable Components (RMCs, e.g. automatic valves, pumps, compressors) of the physical plant take place, and to overcome the Inherent/Passive safeguards (IPSs, e.g. PSVs) and the Active/Procedural (APSs, e.g. PSD activation logics) safeguards present.
In the following, each step is briefly described, pointing out the differences between the two methodologies when present. However, more details and application cases regarding are provided in Iaiani et al. (2021a) for PHAROS analysis, and in Iaiani et al. (2021b) for POROS analysis.
In step 1 (S1) the input information is collected.

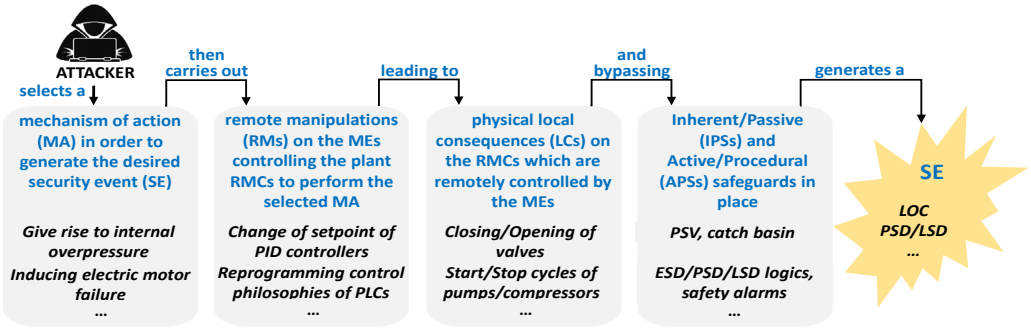

Figure 2: Core mechanism of PHAROS and POROS methodologies

In step 2 (S2) the plant is divided into nodes. In case of POROS, all the nodes are considered in the analysis (including the utilities), while only the ones in which hazardous substances are processed or stored are of concern in the PHAROS assessment (called critical nodes, step S2.1). The division in process nodes may be carried out by a procedure similar to that applied in the HazOp study, as described by the IEC 61882 standard.
Step 3 (S3) consists in the identification, based on a review of process documentation, of the RMCs, of the corresponding MEs, and in the allocation of RMCs to the selected nodes. The allocation of each RMC to one or more nodes is carried out on the basis of the influence it can have on that node (ND). The following guidelines can support the allocation of RMCs: i) if a RMC is located on a stream that directly connects process units belonging to two different nodes, it is allocated to both nodes; ii) if a RMC is located on a stream internal to a node, it is allocated only to that node.
Step 4 (S4) consists in identifying, for each ME, all the possible RMs that can be carried out through an attack (e.g. the set-point change and the signal shutdown for a BPCS controller, or the function reprogramming for

a SIS controller such as a PLC). Next, for each ME, the LCs on the corresponding RMC are identified (e.g. the increase/decrease in the opening degree of the controlled valve, the increase/decrease in the rotational speed of the controlled operating machine).
Step 5 (S5) consists in associating to each selected node the compatible SEs. In case of POROS assessment, a SE is intended as any event which affect the operability and/or system integrity of the system analysed (e.g. arrest/blockage of a piece of equipment/item or product out of specification), while in case of PHAROS assessment, the SEs are only hazardous material and/or energy releases (i.e. major events). Given the high number of SEs identified with POROS, a cut-off criterion based on severity vectors is suggested in order to focus the efforts in improvement of preventive and mitigation measures on the worst-case SEs (step S5.1). Several well-known techniques can be used to identify SEs: HazOp analysis, what-if-analysis, failure modes and effect analysis (FMEA), MIMAH, HazId, DyPASI, etc.
Step 6 (S6) consists in identifying all the MAs by means of which each SE can be initiated through an attack to the BPCS and SIS. 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 7 (S7) consists in identifying the combinations (CMs) of LCs from the allocated RMCs by means of which each MA in a node can be carried out. In general, not all the RMCs present in a node need to be manipulated in order to carry out a MA: to limit the number of CMs to the essential ones, a CM should be selected on the basis of the minimum set of manipulations required.
Step 8 (S8) consists in identifying, for each CM, the effective safeguards (i.e. safety devices) which are present in the node being analysed (both IPSs and APSs). “Effective” means that the safeguard is able to contrast, directly or indirectly, the MA associated to a particular CM, avoiding the occurrence of the corresponding SEs. Effectiveness shall be checked case by case, as it also depends on design specifications of the barrier (e.g. matching or not the requirements from physical scenarios deriving from the attack).
Similarly to an HazOp study, once all the steps have been performed, a completeness check is required. It consists in verifying that all the nodes have been analysed, and that all the MAs, by which the associated SE can be originated were developed as combinations of LCs on the relevant RMCs. Moreover, for the SEs (and corresponding MAs) that require actions from a nearby ND to occur, it must be verified that the additional SEs have been fully developed in the relevant nodes.

3. Case study

A Slug Catcher (double vessel type) and connecting pipework was taken as the System Under Consideration (SUC) for the case study in order to demonstrate the potential use of the toolbox previously described in performing a cyber risk identification. The Process Flow Diagram (PFD) of the SUC is shown in Panel-a of Figure 3: the inlet stream from the sealine is separate by the Slug Catcher SC100; the liquid phase is sent to the liquid treatment section (out of the boundaries of the analysis), while the gas phase is sent to a two-stage compression; discharges from PSV are sent to a flare system.

3.1 Cyber risk identification using results from PIA

According to the categories of industrial sectors considered in the developed database (see Panel-a of Figure 1), the SUC can be classified under the industrial sector “Petrochemical”. The analysis of the distribution of the CSIs among sectors shows that petrochemical installations are the most affected by cyber-attacks (Iaiani et al., 2021a), and thus the cyber threat shall be considered in the context of a security assessment of the SUC (e.g. SVA/SRA methodologies, cybersecurity risk assessment of ISA/IEC 62443). Three different types of attacker with different motivations were found credible (Iaiani et al., 2021a): accidental attacker (i.e. non aimed at specifically targeting the SUC, but any vulnerable host) motivated by challenge, intentional internal attacker (i.e. insider aimed at specifically targeting the SUC) motivated by revenge or gaining personal advantage, and intentional external attacker (i.e. outsider aimed at specifically targeting the SUC) motivated by compromising, stealing, changing, or destroying information, as well as by interfering with plant normal operations.
The share of the categories of impact vs the industrial sectors reported in Panel-b of Figure 3, shows that there is historical evidence for petrochemical installations of both OT infections leading to major events, and of IT infections leading to data loss or corruption. Therefore, combining types of attackers, and impacts, the following cybersecurity-related scenarios can be considered: a) accidental attacker infecting the IT system and compromising sensitive data; b) intentional internal attacker infecting the OT system and activating a LSD/PSD; c) intentional external attacker infecting the OT system and generating a major event.
The effective possibility of generating scenarios b) and c) and the specific set of manipulations through which they can be generated in the SUC, as well as the definition of the effective safeguards in place, can be assessed by applying POROS. In case the only concern is that of major accidents (e.g. in the context of integrated

management of safety and security risks in a Safety Report), only scenario c) is relevant end its credibility and in-depth analysis can be investiagated using PHAROS.

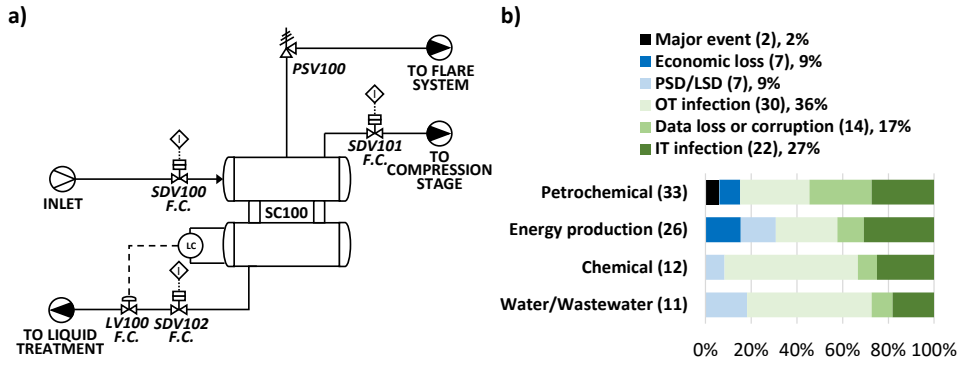

Figure 3: a) Process Flow Diagram (PFD) of the SUC; b) (results from PIA) Share of the impacts of the CSIs recorded vs the industrial sectors

Overall, this information coming from PIA can support the steps of adversary identification, adversary characterization, and hazards identification of SRA/SVA methodologies and of the cybersecurity risk assessment proposed by ISA/IEC 62443.

3.2 Cyber risk identification using PHAROS/POROS

In order to take into account also operability issues, POROS was applied to the SUC, which constitutes a single node. The results obtained are summarized in Table 1. Among the potential SEs considered applicable in step S5, the only two ones that were found possible are the direct activation of a ESD/LSD/PSD logic and the product out of specification, and in particular the presence of a liquid fraction in the gas outlet stream sent to the compression stage (the presence of liquid in that stream may lead to several damages in the compressors in the nearby node). In fact, no suitable MA was identified to exceed design specifications for the construction material with or without the creation of a breach (and consequent release of flammable gas and/or flammable liquid): therefore, no major event can be generated in the node analyzed by remote manipulations of the BPCS and the SIS. Since the direct activation of a ESD/LSD/PSD logic is deemed to cause not severe consequences (recovery from production outage follows normal start-up procedures with expected downtime of 6h, no damage to people and environment are expected), only the product out specification was selected as relevant SE for the SUC (cut-off criterion).In order to generate such SE, the attacker has to over-fill the Slug Catcher SC100 by closing the liquid outlet streams. Two alternative ways are possible: closing the shutdown valve SDV102 (see the PFD in Panel-a of Figure 3) or closing (partially or totally) the control valve LV100. In the first case the attacker has to access the OT system (in particular the SIS) and activate a signal shutdown to the PLC (Programmable Logic Controller) which act on SDV102 as it fails in the close position (FC) or to reprogram its functions so that the valve closes. In the second case, the attacker has to access the OT system (in particular the BPCS) and activate a signal shutdown to the PID (Proportional-Integral-Derivative) controller which act on LV100 (FC) or to increase the setpoint of the liquid level inside SC100. Clearly, the two described ways can also be performed together increasing the complexity of the attack pattern on one side, but also requiring greater efforts by the response measures in the other. The APSs that were identified through the revision of the P&IDs and relevant documentation are the PSD logic activated by LSHH on SC100, the high and very high level alarms LAHs and LAHHs, the hand switch (HS) for manual activation of ESD/PSD/LSD logics, and the position light for the closed position (ZLL) of SDV102. These safeguards have to be overcome by the attacker in order to generate the SE: therefore, efforts shall be spent in dividing these elements in different zones of the OT system (network segmentation) so that the attacker has to accomplish more complex attack patterns (security measure). No IPSs are instead present in SUC.Overall, this information coming from POROS application support step 5.3 (determine consequences and impact), step 5.4 (determine unmitigated likelihood), step 5.8 (identify and evaluate existing countermeasures), step 5.12 (identify additional cybersecurity countermeasures) of the detailed cybersecurity risk assessment proposed by ISA/IEC 62443, as well as the hazards and countermeasures identification steps of SVA/SRA methodologies. Moreover, the results obtained complement the ones achieved through PIA as regards process-related scenarios: in fact, the cybersecurity-related scenarios b) and c) (see sub-section 3.1) are replaced by the two chains of events identified though POROS, which are case-specific scenarios for the SUC.

Table 1: Results of the POROS assessment for the SUC

SE	MA	MEs	RMs	CMs on RMCs	IPSs	APSs
Product out of specification	Over-filling of SC100 by closing the liquid outlet	PLC (SIS)	Signal shutdown; Function reprogramming	i) SDV102 totally closed	None	PSD activated by LSHH on SC100 LAH and LAHH on SC100 + HS for manual ESD/PSD/LSD Position light ZLL for SDV102 + HS for manual reset of SDV102
		PID controller (BPCS)	Signal shutdown; Setpoint change (increase)	ii) LV100 partially or totally closed	None	PSD activated by LSHH on SC100 LAH and LAHH on SC100 + HS for manual ESD/PSD/LSD

4. Conclusions

A synergic toolbox was developed in order to support the cyber risk identification in the context of SVA/SRA methodologies and the cybersecurity risk assessment proposed by ISA/IEC 62443 on cybersecurity of Industrial Automation and Control Systems (IACS). It consists of three tools: a Past Incident Analysis (PIA) of 82 cybersecurity-related incidents occurred worldwide in process facilities and similar sectors, and two systematic and formally rigorous methodologies aimed at the identification of the specific set of manipulations of the BPCS and the SIS which may lead to security events of concern, PHAROS focused on major events, and POROS addressing also operability issues, pointing out the critical components of the plant and the effective physical and automated safeguards against such manipulations.

The potential synergic use of the toolbox in terms of cyber risk identification was shown in a case study addressing a slug catcher for gas/liquid separation. While PIA provides information on type of attackers and related motivations, as well as on generic impacts that can be generated by the cyber-attacks, PHAROS and POROS provide case-specific cybersecurity-related scenarios.

The toolbox developed paves the way to future developments in strategies for a more secure OT system architecture design and supports quantitative approaches for assessing the probability of success of a cyber-attack aiming at interfering with the operability and/or 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

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

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

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

Iaiani, M., Tugnoli, A., Bonvicini, S., Cozzani, V., 2021a. Analysis of Cybersecurity-related Incidents in the Process Industry. Reliab. Eng. Syst. Saf. 209, 107485. https://doi.org/10.1016/j.ress.2021.107485.

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

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

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

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

The Repository of Industrial Security Incidents (RISI) [WWW Document], 2015. URL https://www.risidata.com/Database (accessed 12.8.20).