CHEMICAL ENGINEERING TRANSACTIONS
VOL. 82, 2020
A publication of AIDIC
The Italian Association of Chemical Engineering
Online at www.cetjournal.it
Guest Editors: Bruno Fabiano, Valerio Cozzani, Genserik Reniers

ISBN 978-88-95608-80-8; **ISSN** 2283-9216
DOI: 10.3303/CET2082054

A Systematic Methodology for the Identification of Major Accidents Induced by Malicious Manipulation of the BPCS and the SIS in a Process Plant

Matteo Iaiani[a], Alessandro Tugnoli[a,*], Gabriele Landucci[b], Valerio Cozzani[a]

[a]LISES – Dipartimento di Ingegneria Civile, Chimica, Ambientale e dei Materiali, Alma Mater Studiorum – Università di Bologna, Italy
[b]DICI – Dipartimento di Ingegneria Civile e Industriale, Università di Pisa, Italy
a.tugnoli@unibo.it

Cyber-attacks aimed to interfere with the Basic Process Control System (BPCS) and the SIS (Safety Instrumented System) of industrial facilities where large quantities of hazardous substances are stored or handled may have consequences comparable to those of conventional major accidents due to internal causes.
While consolidated approaches exist to manage and control the cybersecurity of IT (Information Technology) and OT (Operational Technology) systems of a plant, there is an evident lack of operating procedures for assessing the actual link between malicious manipulations of the BPCS and the SIS (OT system) and the major accidents that can be induced.
In the present study a specific operating systematic methodology, PHAROS, was developed to address the identification of major accident scenarios achievable by remote manipulation of the physical components of the plant (e.g. automatic valves, pumps, compressors, etc.). The methodology exploits a reverse-HazOp concept and it also supports the definition of the specifications for the design and management of barriers aimed at the prevention and mitigation of such scenarios. The application of PHAROS to a demonstrative case study evidenced first that both the BPCS and the SIS typically need to be attacked in order to induce major accidents, and second, that passive/inherent safeguards have a key role with respect to the success of the considered malicious attack in case they are properly designed.

1. Introduction

The process industry is currently undergoing a digital transition towards higher levels of automation (e.g. digital sensors, improved network protocols, increased interconnection with external networks, etc.). This ensures advantages such as efficient process control, quick and safe response to abnormal conditions, improvement of product quality, but also exposes the process sites to security threats.
The consequences of malicious manipulations on the Basic Process Control System (BPCS) and the Safety Instrumented System (SIS) of plants handling hazardous materials may potentially be comparable to accidents due to internal failures (Tugnoli at al., 2019). For example, in 2008, attackers intentionally shut down alarm systems, cut off communications with the control room and over-pressurized a section of the BTC (Baku -Tbilisi-Ceyhan) crude oil pipeline. This resulted in an explosion, in the release of more than 30,000 barrels of oil in an area above a water aquifer, in a fire lasting more than two days, and in outage losses of $5 million per day (Department of Homeland Security).
In this panorama, major accidents triggered by attacks to the OT system (BPCS plus the SIS) are becoming an issue that process industry can no longer disregard (Thomas and Day 2015). Due to the particular nature of this industrial sector, a complete security analysis requires the assessment of two parts (see Figure 1a): the IT/OT network (first part) and the process system (second part). The ISO/IEC 27000 series of standards on information security management (ISO-IEC, 2018), the standard IEC 61511 on functional safety of safety instrumented systems for the process industry sector (IEC, 2017) and the ISA/IEC 62443 series of standards

Paper Received: 18 December 2019; Revised: 15 May 2020; Accepted: 8 August 2020
Please cite this article as: Iaiani M., Tugnoli A., Landucci G., Cozzani V., 2020, A Systematic Methodology for the Identification of Major Accidents Induced by Malicious Manipulation of the Bpcs and the Sis in a Process Plant, Chemical Engineering Transactions, 82, 319-324 DOI:10.3303/CET2082054

on security for industrial automation and control systems (ISA-IEC, 2018) provide approaches for the assessment of the IT/OT network (firs part of the assessment, see Figure 1a), requiring the evaluation of all the impacts that can result from attacks to the IT/OT system, including those on physical process plant.
Nevertheless, there is an evident lack of operating procedures for assessing the actual link between malicious manipulations of the BPCS and the SIS (OT system) and the major accidents that can be induced.
The methodologies dedicated to process plant security vulnerability assessment (e.g. the VAM-CF methodology (Jaeger, 2002), the CCPS methodology (AIChE-CCPS, 2003) and API RP 780 methodology (Moore, 2013)) 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). In spite of the recognized relation between safety and security (Brewer, 1993; Eames and Moffett, 1999; Kriaa et al., 2015), the hazard assessment techniques used in the field of process safety to analyse the hazards in the process systems (HazOp, LOPA, fault tree analysis, etc.) do not account for these aspects.
The present study aims at filling the gap in the availability of systematic operating procedures for security assessment of the link between malicious manipulations of the BPCS and the SIS (OT system) and major accidents in a process plant. To this aim, a rigorous methodology for hazard identification was developed (PHAROS: Process Hazard Analysis of Remote manipulations through the cOntrol System). The procedure exploits a reverse-HazOp concept: starting from the possible critical events of concern (e.g. major accidents as loss of containment of hazardous substances), the remote manipulations achievable through an attack to the BPCS and the SIS, and leading to such critical events, are identified by a systematic procedure. Physical safeguards preventing or mitigating the critical event are considered and rated for their effectiveness.
In the following, the different steps of PHAROS are described. A case study on an Oil&Gas upstream plant is also described, to demonstrate the application of the methodology and the typical results obtained.

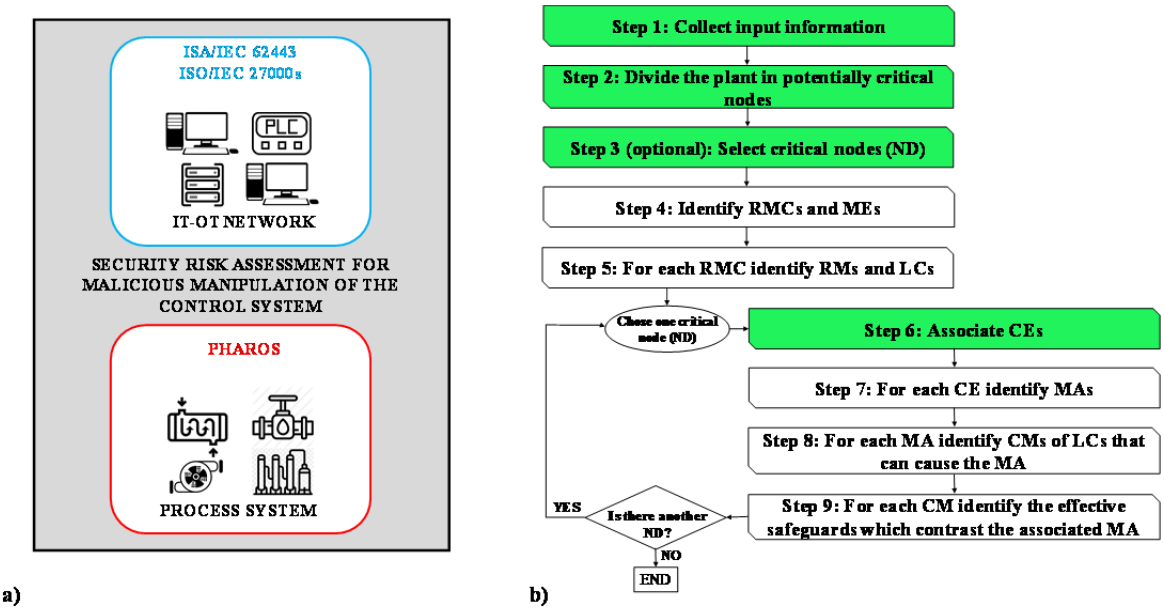

Figure 1: a) Schematization of the security risk assessment for malicious manipulations of the control system of a process plant; b) Flowchart of the PHAROS procedure. Shaded steps can be integrated with conventional safety studies. Acronyms are described in section 2.2.

2. Methodology

2.1 Overview

The PHAROS methodology is a systematic and formally rigorous procedure for the analysis of process schemes. As the methodology is concerned with the “process system” part of the security risk assessment (Figure 1a), it starts from the assumption that the attacker successfully managed to gain full control the BPCS and SIS systems (either remotely or by direct access to the site) by overcoming any possible IT-OT defense barrier (e.g. authentication, firewalls). Therefore, the attacker is supposed to be able to impart any instruction, potentially eluding alarms and active safeguards controlled by the IT-OT system.

The procedure should be performed by a team: the minimum technical knowledge that is required concerns 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 procedure 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.

2.2 Detailed description of the methodology

PHAROS consists in nine steps, all shown in the flowchart of the procedure reported in Figure 1b.
In Step 1 the input information is collected.
In Step 2 the plant is divided into process nodes. Only the nodes in which hazardous substances are processed or stored (called potentially critical nodes) are of concern in the assessment. The division in process nodes may be carried out by a procedure similar to that applied in the HazOp study, as described by the standard IEC 61882 standard (IEC, 2016).
Step 3 consists in identifying the critical nodes (ND) among the process nodes. This step is aimed at reducing the number of nodes to be analyzed, focusing on those from which the more severe consequences can originate. Hence, the critical nodes shall be selected on the basis of the inherent hazard. Mannan (Mannan, 2012) and Tugnoli et al. (Tugnoli et al., 2007; Tugnoli et al., 2012) provide reviews of procedures for hazard ranking of process units and their application for inherent safety scoring.
The selection of the most critical nodes can be based either on absolute terms or on relative terms. Clearly enough, all the potential critical nodes can be selected as critical nodes if deemed necessary, making step 3 an optional step.
Step 4 consists in the identification, based on a review of process documentation, of the remotely manipulable components (RMCs), of their manipulative elements (MEs), and in the allocation of RMCs to the critical nodes. RMCs are the physical components in the plant whose operation is regulated by the BPCS and the SIS (e.g. automatic valves, pumps, compressors, etc.). The MEs are the elements of the BPCS and the SIS by which the manipulation action is carried out (e.g. controllers and their logics).
The allocation of each RMC to one or more critical 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:

- if a RMC is located on a stream that directly connects process units belonging to two different NDs, it is allocated to both nodes;
- if a RMC is located on a stream internal to a critical node, it is allocated only to that node.

Step 5 consists in identifying, for each ME, all the possible remote manipulations (RMs) that can be carried out through an attack to the OT system (e.g. a set-point change or signal shutdown). Next, for each ME, the local consequences (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 pump).
Step 6 consists in associating to each critical node the compatible critical events (CEs). A CE is a loss of containment (LOC) or a loss of physical integrity (LPI) which “unleashes” the material or physical hazards normally present in the system (Delvosalle et al., 2006). HazOp analysis, what-if-analysis, failure modes and effect analysis (FMEA), MIMAH, HazId, DyPASI are well-known techniques that can be used to identify CEs.
Step 7 consists in identifying all the mechanisms of action (MAs) by means of which each CE can be initiated through an attack to the OT system. The MAs are the physical mechanisms that the attackers may use to initiate the CE (e.g. increase the internal pressure of a vessel). 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 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 9 consists in identifying, for each CM, the effective safeguards (i.e. safety devices) which are present in the node being analyzed. “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 CEs. 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).
Safeguards can be classified in active/procedural safeguards (APSs) and inherent/passive safeguards (PSs) (Kletz, 1998). The first ones are automated or human-mediated actions, which involve response by the same

IT-OT system under attack; while the second ones are devices that provide their safety action independently of the IT-OT system (e.g. PSVs, rupture disks, vent systems, emergency hatches, etc.).
Similarly to an HazOp study, once all the steps have been performed, a completeness check is required. It consists in verifying that all the critical nodes have been analyzed, and that all the MAs, by which the associated CE can be originated have been developed as combinations of LCs on the relevant RMCs. Moreover, for the CEs (and corresponding MAs) that require actions from a nearby ND to occur, it must be verified that the additional CEs have been fully developed in the relevant nodes.

3. Case Study

3.1 Set up of the Case Study

An onshore upstream Oil&Gas plant for the preliminary treatment of crude oil was considered as a Case Study for the application of the PHAROS procedure. The main goals of the plant are the separation of the production water and the oil and gas processing up to specification for transport via pipeline.
In the following, the application of the PHAROS methodology is demonstrated on the critical process node featuring the Slug Catcher SC001 and the Gas KO Drum GKD001.
Both process equipment are under pressure (65 barg) and contain both liquid and gas phases. Figure 2 reports a simplified P&ID of the considered node (named ND01 in the following).

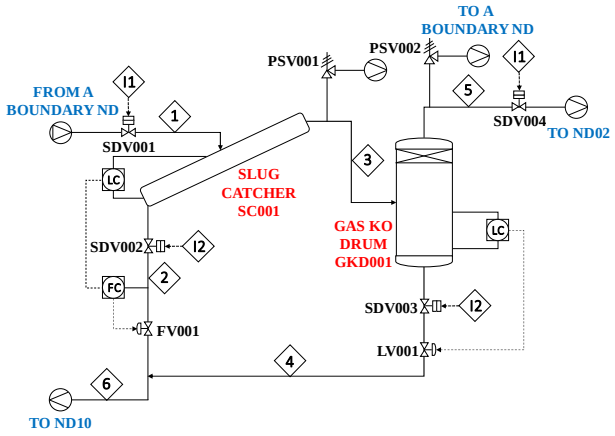

Figure 2: Simplified P&ID of the critical process node ND01. I1: PSD logic; I2: LSD logic; SDV: shutdown valves; PSV: pressure safety valves; FC: flow controller; LC: level controller; FV, LV: control valves.

3.2 Application and results

The total results obtained from the application of PHAROS methodology to the node ND01 are summarized in Figure 3. The second row (yellow shaded) shows the critical events associated to ND01: the parallel assessment of nearby nodes and the available HazOp study for the plant under investigation suggested for the addition of the additional critical events aCE01 and aCE02. In the third and fourth rows (green shaded) are reported the mechanisms of action that can be carried out by the attackers in order to initiate the identified CEs. The sets of local consequences (called combinations, CMs) on the relevant RMCs allocated to the node ND01 (red shaded on the left side of the table), through which each MA can be carried out, are reported in the body (grey shaded). Finally, the last two rows (light blue shaded) report the APSs and IPSs for each CM that are present in the node under assessment.
Some general conclusions may be drawn from the analysis of the results obtained from the application of PHAROS methodology on the Case Study.
The first thing to underline is that it is possible to initiate critical events by tampering with only one system between the BPCS and the SIS. For example, the increase in the liquid level (see Table 1) can be carried out by the attackers either by manipulating the BPCS only (i.e. closing the control valves FV001 and LV001 controlled by the BPCS controllers FC and LC), or by manipulating the SIS only (i.e. by closing the shutdown valves SDV002 and SDV003 controlled by the programmable logic controllers of the SIS). Only the over-pressurization of the slug catcher SC001 and the gas KO drum GKD001 (MA01) can not be carried out by manipulating the BPCS only. However, in order to successfully conduct an attack resulting in a major event on the process equipment of the target system, attackers have also to bypass the safeguards in place. If active

and/or procedural safeguards are present, this requires the attackers to manipulate the SIS in any case. For this reason, the separation between the BPCS and the SIS in the IT-OT architecture is in favour of security, especially for those cases in which only the infection of the BPCS allows to initiate critical events.
Moreover, the manipulation of a single RMC (i.e. SDV004) can initiate a critical event potentially resulting in a major hazard. For this reason, the SIS controller (hardware and software) that manage the shutdown valve SDV004 requires a priority in its management at IT-OT system level.
In the other two cases (see MA02 and MA03 in Figure 3) the manipulation of two RMCs is required. Obviously, the greater the number of RMCs to be manipulated, the higher the complexity of the attack and the higher the security level.
It should also be remarked that a redundancy of active and procedural safeguards (APSs), is present for MA01 and MA03 (see Figure 3), while only a single procedural safeguard (i.e. high liquid level alarms) is present for MA02.
On the other hand, the identification of the inherent/passive safeguards (IPSs) is extremely important as they provide a layer of protection independent from the BPCS and the SIS, whose effectiveness and likelihood of failure are part of the cybersecurity risk assessment (e.g. ISA/IEC 62443). Since the PSVs are typically sized on the basis of the relieving rates that do not include scenarios of malicious manipulation (API 2014), their sizing may be revised taking into account the security cases identified by the present approach and introducing them in the sizing procedure of API 521 RP (API 2014).

ND01		**Slug Catcher SC001, Gas KO Drum GKD001, connected pipework**		
Critical events (CEs)		CE01: continuous release of a flammable substance (gas/liquid) CE02: instantaneous release of a flammable substance (gas/liquid)	aCE01: liquid fraction in stream 5	aCE02: gas fraction in stream 6
Categories of Mechanisms of action		Give rise to internal overpressure	Increase in the liquid level	Increase in the liquid level
Mechanisms of action (MAs)		MA01: Blocking of stream 5	MA02: Blocking of stream 2 + Blocking of stream 4	MA03: Maximum flow in stream 2 + Maximum flow in stream 4
Remotely manipulable components (RMCs)	SDV002	NM	Closed (or manipulation on FV001)	NM
	SDV003	NM	Closed (or manipulation on LV001)	NM
	SDV004	Closed	NM	NM
	FV001	NM	Increased closure (or manipulation on SDV002)	Increased opening
	LV001	NM	Increased closure (or manipulation on SDV003)	Increased opening
Active/Procedural safeguards (APSs)		High pressure alarms PSD logic I1	High liquid level alarms	Low liquid level alarms LSD logic I2
Inherent/Passive safeguards (IPSs)		PSV001, PSV002, catch basin	-	-

Figure 3: Worksheet containing the results obtained from the application of PHAROS methodology for the node ND01. NM: no manipulation of the RMC required.

4. Conclusions

The PHAROS methodology aims at complementing security risk assessment of a process plant addressing the remote manipulation of the control system. In particular, it allows for the identification of the combinations of remote manipulations which can lead to critical events (hazardous material and energy releases from plant equipment), and the definition of the specifications for the sizing and security management of the effective safeguards against such combinations of manipulations.
The application of the methodology to a representative case study highlighted that, a successful attack generally has to infect both the BPCS and the SIS in order to give rise to critical events. Actually, the attackers must not only tamper with the physical components of the plant (e.g. valves, pumps, compressors, etc.), but they must also bypass the active/procedural safeguards. For this reason, the separation (e.g. air gap) of the BPCS and the SIS in the IT-OT network architecture results to be an effective measure against cybersecurity risk. It has also been pointed out that it is possible to initiate major events with simple attack patterns, since the manipulation of a single component may be sufficient.
Passive/inherent safeguards have a key role in protecting the system from malicious manipulations of the control system whenever they are able to contrast the identified mechanisms of action. This derives from the

fact that they are not electronic devices and so they can not be remotely affected by the attackers. An appropriate sizing of such devices, considering the security cases and the critical events identified by the present procedure is therefore important to guarantee safeguard effectiveness in protecting the system.
The PHAROS methodology resulted an effective tool, contributing to the synergy among safety and security, and allowing the identification of security issues related to remote malicious manipulation of the control system.

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

AIChE-CCPS, 2003, Guidelines for Analyzing and Managing the Security Vulnerabilities of Fixed Chemical Sites, American Institute of Chemical Engineers - Center of Chemical Process Safety (AIChE-CCPS).
Brewer D., 1993, Applying Security Techniques to Achieving Safety, Directions in Safety-Critical Systems, 246–256.
Delvosalle C., Fievez C., Pipart A., Debray B., 2006, ARAMIS Project: A Comprehensive Methodology for the Identification of Reference Accident Scenarios in Process Industries, Journal of Hazardous Materials, 130(3), 200–219.
Department of Homeland Security, RISI - The Repository of Industrial Security Incidents, Accessed April 2, 2019, https://www.risidata.com/Database.
Eames D.P., Moffett J., 1999, The Integration of Safety and Security Requirements, Computer Safety, Reliability and Security, 1698, 468-480.
IEC, 2016, Hazard and Operability Studies (HAZOP Studies) - Application Guide (IEC 61882 standard), International Electrotechnical Commission (IEC).
IEC, 2017, Functional Safety - Safety Instrumented Systems for the Process Industry Sector (IEC 61511 standard), International Electrotechnical Commission (IEC).
ISO-IEC, 2018, ISO/IEC 27000 Series of Standards: Information Technology - Security Techniques - Information Security Management Systems, International Organization for Standardization (ISO) and International Electrotechnical Commission (IEC).
ISA-IEC, 2018, ISA/IEC 62443 Series of Standards: Industrial Automation and Control Systems Security, International Society of Automation (ISA) and International Electrotechnical Commission (IEC).
Jaeger C.D., 2002, Vulnerability Assessment Methodology for Chemical Facilities (VAM-CF), Chemical Health and Safety, 9(6), 15–19.
Kletz T.A., Amyotte P., 1998, Process Plants: A Handbook for Inherently Safer Design (2nd Ed.), Taylor & Francis.
Kriaa S., Pietre-Cambacedes L., Bouissou M., Halgand Y., A survey of approaches combining safety and security for industrial control systems, Reliability Engineering & System Safety, 139, 156-178.
Mannan S., 2012, Lees' Loss Prevention in the Process Industries: Hazard Identification, Assessment and Control (4th ed.), Butterworth-Heinemann.
Matteini A., Argenti F., Salzano E., Cozzani V., 2019, A Comparative Analysis of Security Risk Assessment Methodologies for the Chemical Industry, Reliability Engineering and System Safety, 191.
Moore D.A., 2013, Security Risk Assessment Methodology for the Petroleum and Petrochemical Industries, Journal of Loss Prevention in the Process Industries, 26(6), 1685–1689.
Thomas H.W., Day J., 2015, Integrating Cybersecurity Risk Assessments Into the Process Safety Management Work Process, In: 49th Annual Loss Prevention Symposium 2015, LPS 2015 - Topical Conference at the 2015 AIChE Spring Meeting and 11th Global Congress on Process Safety, 360–378.
Tugnoli A., Cozzani V., Landucci G., 2007, A Consequence Based Approach to the Quantitative Assessment of Inherent Safety, AIChE Journal, 53(12), 3171–3182.
Tugnoli A., Landucci G., Salzano E., Cozzani V., 2012, Supporting the Selection of Process and Plant Design Options by Inherent Safety KPIs, Journal of Loss Prevention in the Process Industries, 25, 830–842.
Tugnoli A., Iaiani M., Oliva G., Salzano E., Setola R., Cozzani V., 2019, Chemical Engineering Transactions, 77, 883–888.