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/CET2290058

Methodology for a combined Safety and Security Analysis based on Classic HAZOPs for Operational Technology Insert

Johannes Biernath*, Jürgen Dürrwang, Jürgen Schmidt, Jens Denecke

CSE Center of Safety Excellence (CSE-Institut), Joseph-von-Fraunhofer-Str. 9, 76327 Pfinztal, Germany
johannes.biernath@cse-institut.de

The continuous increase in digitalization and automation in the chemical industry leads to more interconnected systems via internal and external networks. These systems are vulnerable to cyber-physical attacks and can affect safety. To protect chemical plants against safety-related failures and security-related attacks, a comprehensive and combined safety and security analysis is required. This article presents a uniform methodology, which includes safety hazards and security vulnerabilities as well as an analysis of potential hazards due to interaction between both. A strong focus is placed on the easy applicability of the method by integrating well-known safety procedures like HAZOP into the methodology. The article summarizes research results submitted for publication in (Biernath, 2022).

1. Introduction

Digitalization and automation lead to significantly more interconnected systems in the chemical industry. This trend will continue over the next years with more sensors, final elements, and control systems, like Basic Process Control Systems (BPCS) or Safety Instrumented Systems (SIS), to be deployed according to Bryzek (2013). Isolated systems that are not connected to other information technology (IT) or operational technology (OT) systems will successively be removed and replaced by networked structures to allow for smart protection systems with the aim of zero incidents and zero emission.
These structures are already opened up to the external world of a plant, to increase the efficiency of chemical plants through process data analysis or to be able to use machine learning tools for maintenance prediction or operational performance improvement as described by Patel (2016). As a consequence of this openness, cyber-attacks are now feasible and have already been taken place, see Hemsley (2018), Cherepanov (2016), or Pinto (2018). Therefore, the protection of chemical plants against cyber-attacks is an essential task.
The relevance of this aspect is well known and standards for safety instrumented systems in the chemical industry like DIN EN 61511/08 or leaderships groups like CeSIS (2022) already address this subject. Unfortunately, these standards do not present in detail any guidance for risk assessment or the selection of security countermeasures. To meet security requirements for OT-Systems, the German industrial regulation NA 163 and the guideline KAS 51 have been developed in the last few years. Both represent the current state of the art and serve as security guidelines for the chemical industry. Essential points, such as the development of an information security management system, are based on the standard ISO 27001 or IEC 62443. However, even in these guidelines, there are no uniform methods for conducting threat and risk analyses when developing chemical systems. The guides are also lacking in clarity on how dependencies between safety countermeasures and security countermeasures can be identified and resolved. Therefore, a combined safety & security analysis is required, to prevent conflicts between safety and security measures. Conflicting or reinforcing effects between safety and security countermeasures should be identified to give a prioritization of security and safety countermeasures on basis of different evaluations within the methodology.

2. State of knowledge

The Failure Mode, Vulnerabilities and Effect Analysis method is based on Failure Mode and Effects Analysis by the International Electrotechnical Commission et al. (2006), which is a structured technique for investigating

Paper Received: 14 January 2022; Revised: 25 March 2022; Accepted: 28 April 2022
Please cite this article as: Biernath J., Dürrwang J., Schmidt J., Denecke J., 2022, Methodology for a combined Safety and Security Analysis based on classic HAZOPs for Operational Technology Insert, Chemical Engineering Transactions, 90, 343-348 DOI:10.3303/CET2290058

system failures and their causes. FMVEA expands this concept by including weak points and attacks related to the security of a system and extends the catalogue of relevant security threats, see Strobl (2018). Since FMVEA is based on the FMEA methodology, see McDermott (1996), defects must be identified before the analysis can be performed. Therefore, the approach is not suitable for early development phases. According to Chockalingam et al. (2016), the approach requires detailed information about the system design. Furthermore, there is no exchange between the safety and security path when analyzing failures and threats. This can lead to a situation where safety and security interactions are overlooked, as it is described by Torkildson (2018). The link between safety and security is only established in the combined evaluation of the damage for the failure and threat modes. Furthermore, FMVEA also has the limitation that only individual causes of an effect are considered, whereas multi-stage attacks are not considered according to Verma (2019). Another critical point is that no procedure is shown for identifying failures and threats, which makes the initial application of the methodology more difficult, see Macher (2016).

The Six-Step Model, described by Adepu (2016) and Sabaliauskaite (2017), is one of the combined safety and security approaches, where both study fields, in the first instance, are analyzed separately. For this purpose, the model uses six dimensions of the Cyber-Physical System (CPS): functions, structures, failures, safety countermeasures, cyber-attacks, and security countermeasures. Relationships between the individual dimensions are represented by relationship matrices. The approach requires an integration step to combine the two study areas. This can lead to a high number of iterations to resolve conflicts in safety and security requirements, see Lisova (2018). Furthermore, the approach does not show a method to perform the threats analysis and does not provide any risk assessment procedure, so the prioritization of attacks or threats is unclear.

The Security Guideword Method (SGM) from Durrwang (2017) is a threat analysis that combines safety and security in such a way that security threats are identified that may violate safety objectives. Therefore, the SGM extends the safety analysis with security causal factors to identify security threats that violate operational security. The procedure is based on the recognized Hazard and Operability Study (HAZOP) technology as described by Eriscon (2005) and enables safety categories to be taken over in a structured and guided manner so that security threats can be identified. But the analysis results highly depend on the experience of the experts. Therefore, the selection of the analysis team is elementary, as it is with HAZOP. In addition, SGM is developed for the vehicle domain and uses artifacts of the ISO 26262 for risk assessment which does not entirely fit to the OT domain in the chemical industry.

Besides the shown methodologies, risk and hazard analysis for a chemical plant is also required to identify safety-related hazards, their risks and the required safety countermeasures, like organisational measures, mechanical devices or safety instrumented systems (SIS). A widely used analysis are hereby the Hazard and operability studies (HAZOPs).

In general, the technique of a HAZOP is based on breaking a complex structure of a chemical plant piping and instrumentation diagram (P\&ID) into several nodes. Each node should include information about its description, functions, boundaries, design conditions, and substances. The next step is the analysis of each node concerning potential deviations, their causes, and consequences as well as their risks and required safeguards, see Guiochet (2016). The analysis procedure follows these defined orders, which can be considered in Table 1 from the left to the right. Most recently promising developments have been made to automatically perform the HAZOP analysis based on artificial intelligent approaches as can be seen in Single (2020a, 2020b, 2020c)

Table 1: Structure of a HAZOP-Template for a specific node

Deviation	Cause	Consequence	Risk	Safeguards
<Pressure too high, Temperature too low, ...>	<leakage, rupture, malfunction,...>	<material loss, fire damage, shock wave,...>	<Class A,B, C,D,...>	<organization, mechanical, process control,...>

3. Methodology

A new approach called Safety-Cyber-Security-Evaluation (SCSE) is presented in this section. It is based on a matrix framework with simple expandability and requires five steps, which are shown in Figure 1

In the first step, the results of an already carried out risk and hazard analysis are transferred into the first matrices in one step. That is possible since in the chemical industry a risk assessment, such as HAZOP, must be carried out for many safety-relevant systems. In these risk assessments the same categories as in the matrices, like nodes (N), deviation (D), causes (Ca), consequences (C) or safety countermeasures (SaC), are identified and can be transferred into the blue matrices of Figure 1

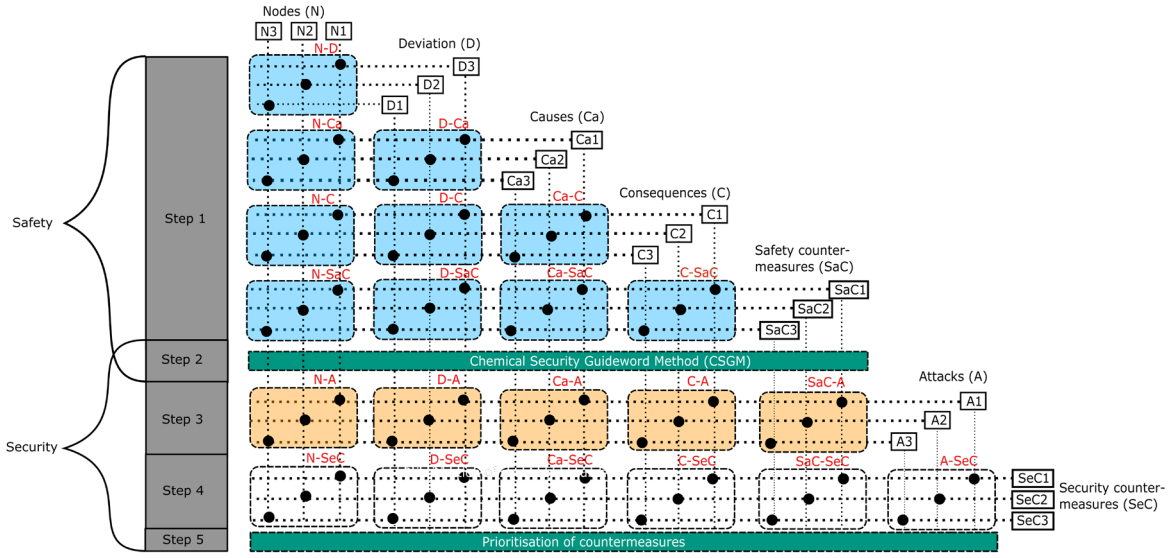

Figure 1: Five-step concept of the Safety-Security analysis (SCSE) Step 1: Transfer hazard analysis; Step 2: Execution of Chemical Security Guideword Method (CSGM}; Step 3: Integration of CSGM results; Step 4: Derivation of countermeasures; Step 5: Prioritization of countermeasures

The risk category is fused with the category consequences because a cyber security attack will not attack the risk directly. Due to using the same categories, the transmission of the results of a HAZOP is quite easy and can be done automatically. It should be emphasized, that for an automated application the text within the categories in a HAZOP must follow a specific systematic. Otherwise, a transferring of the results wouldn't be successful. A possible systematic is defined in Single (2020a, 2020b, 2020c).
By transferring the results into the matrices, the following different cyber-physical attack related scenarios may be considered:

1) Attacks on safety instrumented systems leading to a non-performance of the safety instrumented function
2) Simultaneous attacks on different non-safety relevant units, which can cause a security-relevant scenario to the same plant unit
3) Simultaneously triggering of different safety scenarios, which are covered by the same safety countermeasure in case of a single-failure consideration in the HAZOP
4) Attacks on essential functions and their availability based on the IEC-TR63069

In this second step, the results of the former step will be analyzed under the aspects of possible threats and attack vectors. For this purpose, the start is similar to the typical beginning of a HAZOP with summarizing the relevant information. Here, it is the case number of the HAZOP, the involved components, like sensors, logic controller and final elements, their manufacturers, and interfaces. It ends with the defined cyber-physical attack-related scenario, which is relevant for this case number. An example is shown in Table 2.

Table 2: Involved components for an example

Category	Descrption		
Case	1		
Component	Temperature sensor	Failsafe Logic controller	Valve
Manufacter	Endress+Hauser	Siemens	Samson
Interfaces	4-20mA HART	Industrial Ethernet; Profisafe	Profisafe
Scenario	Attack on safety instrumented systems, which leads to a non-performance of the safety instrumented function		

Based on this information the CSGM method can be applied, which is comparable to the HAZOP method and based on guidewords, which reflect a possible threat comparable to a deviation in the HAZOP, see Table 3.

Table 3: Description of some CSGM guide words and the reference to the STRIDE guidewords

CSGM Guidewords	CSGM ID	Description	STRIDE
Delay	1	Unavailability of information due to a delay of data on a communication channel. Delaying an emergency message could result in a non-activating of relevant protection mechanisms and the risk of not preventing the situation.	DoS
Denial (of service)	2	The denial or blocking of a critical service leads to the unavailability of the service. For example, if the temperature measurement service is no longer available, high temperatures can no longer be detected.	DoS
Trigger	3	An unauthenticated execution or activation of a software function on the target component. This can be critical, for example, if the activated function causes an elementary change in the process. For instance, this could be the opening of a control element to maliciously inject an increased quantity of a hazardous fuel	Spoofing
Manipulation	4	The malicious modification of existing information is used to change the behaviour of the target component. A classic example of this is Man-in-the-Middle attacks, in which the attacker intercepts a message, manipulates the information contained and forwards the message to the destination. In particular, a wide variety of scenarios are feasible like the manipulation of sensor values or control signals, which can lead to a dangerous scenario.	Tampering
Resequencing	5	A maliciously manipulated bus device modifies the safety message sequence. For instance, if a safety function should at first reduce the velocity of a pump and then stop its pump function, a swapping of both orders leads to a still-running pump.	DoS

These guidewords are mapped onto the different components of each case, which are resulted from the first step. Similar to the causes in the HAZOP, in the CSGM the possible attacks are determined next, which can lead to the considered threat. For this purpose, well-known attack vectors, which are documented for instance by National Vulnerability Database (NVD) or manufacturer security advisories, can be directly implemented or an attack tree can be used to define relevant attack vectors and the risk can be defined by a well-known approach like Common Vulnerability Scoring System (CVSS). For the last case, the root of the tree always corresponds to the cyber-physical attack-related scenario. The results can be directly transferred to the orange matrices to fulfill the third step of the methodology.

Once the cyberattacks are assigned to the different cases, the next step is to consider security measures that can reduce the risk of cyberattacks. A good starting point for the selection of proper security measures are guidelines from the National Institute of Standards and Technology (NIST) like the SP 800-53 by NIST (2014) or SP 880-171 by Toth (2017). In addition, also manufacturers' security manuals are a useful source for possible security countermeasures. The defined safety and security countermeasures can be complementary or in conflict with each other. Therefore, it is useful to analyze these dependencies and to resolve possible conflicts by use of the SaC-SeC matrix. Within the SaC-SeC matrix, the safety countermeasures are compared with the security countermeasures, and their relationship is defined. There are four kinds of relationships, which are described in Table 4.

Table 4: Description of the different kinds of relationships between safety and security countermeasures

Relationships	Descrption
Reinforcement (+)	Strengthening impact between safety- and security countermeasures
Antagonism (-)	Weakening impact between safety- and security countermeasures
Conditional dependencies (&)	Security countermeasure is required for the safety countermeasure or vice versa
Independence (0)	No relationship between safety and security countermeasures

In the last step, the prioritisation of the security and safety countermeasures is considered, which is determined by different results during the execution of the SCSE approach.

The last step of the Safety-Cyber-Security-Evaluation (SCSE) is the prioritisation of the selected countermeasures. Therefore, the information generated over the previous steps can be taken over to support the prioritization procedure. In particular, various relationships for the four different cyber-physical attack-related scenarios are examined which can help to prioritize the identified measures. This is an important step since the implementation of security measures is often a trade-off between the increase of the security level and the available budget.

In the case of the first cyber-physical attack-related scenario, one factor for the prioritization are the results of the risk and hazard analysis and its risk assessment. The larger the risk, the higher the priority. A further factor for each scenario is the risk analysis within the second step. Especially with the attack vectors derived from the respective attack tree. Based on the individual attack steps in the tree (leaves), the corresponding vulnerabilities can be identified and assessed. For such a vulnerability assessment, existent vulnerability metrics like Common Vulnerability Scoring System (CVSS) or the Common Criteria for Information Technology Security Evaluation (CC) can be used.

A third factor is the relevance of the components. The more cases are defined per component, the higher is the impact of that component. In general, an FPLC is one of the most important components in a chemical plant and therefore it should get a high priority.

A fourth factor is the number of components, which are attacked by the same attack vector because this could lead to a large manipulation at the same time. For this point, the attack matrices should be considered. In the presented example, each attack vector has got just one affected component and therefore it doesn't make a difference.

The last factor for the prioritization is for the presented example the relation matrix SaC-SeC, which provides an overview of the strengthening or weakening influences between security and safety-relevant countermeasures. Thus, measures with strengthening influences or conditional dependencies should always be applied before measures with weakening influences.

4. Conclusion

In this paper, a uniform methodology called Safety-Cyber-Security-Evaluation (SCSE) for the combined assessment of safety and security in the OT domain is proposed. The approach focuses on an easy application for engineers in the chemical industry by use of guidewords and takes over safety categories to identify security problems. It enables to consider four cyber-physical attack related scenarios: attacks on safety instrumented systems leading to a non-performance,

simultaneous attacks on different units causing a security-relevant scenario, simultaneously triggering of different safety scenarios covered by the same safety countermeasure and attacks on essential functions and their availability based on the IEC-TR63069.

Furthermore, strengthening, weakening, conditional or independent interactions between safety and security countermeasures are identified and evaluated. At the end of the methodology, a prioritization of the implementation of each defined countermeasure is performed, based on the evaluations during the execution of this methodology.

References

Adept, S., Mathur, A, 2016, Distributed Detection of Single-StageMultipoint Cyber Attacks in Water Treatment Plant. Proceedings of the 11th ACM on Asia Conference on Computer and Communications Security - ASIA CCS ’16; Chen, X.; Wang, X.; Huang, X., Eds.; ACM Press: New York, New York, USA, pp. 449–460. doi:10.1145/2897845.2897855.

Bryzek, J. Roadmap for the trillion sensor universe. Berkeley, CA, April 2013.

CeSIS, Center for Safety Integrity & Security, 2022, www.cse-engineering.de/leadership/cesis/

Cherepanov, A., Lipovsky, R. BlackEnergy, 2016, what we really know about the notorious cyber attacks. Virus Bulletin Conference.

Chockalingam, S., Hadžiosmanovic´, D., Pieters, W., Teixeira, A., van Gelder, P, 2016, Integrated safety and security risk assessment methods: A survey of key characteristics and applications. International Conference on Critical Information Infrastructures Security, pp. 50–62.

Dürrwang, J., Beckers, K., Kriesten, R, 2017, A Lightweight Threat Analysis Approach Intertwining Safety and Security for the Automotive Domain. In Springer – International Conference on Computer Safety, Reliability, and Security; pp. 305–319. doi:10.1007/978-3-319-66266-420.

Di Pinto, A., Dragoni, Y., Carcano, A. TRITON, 2018, The first ICS cyber attack on safety instrument systems. Proc. Black Hat USA, 1–26.

Ericson, II., C.A, 2005, Hazard analysis techniques for system safety; Wiley-Interscience: Hoboken, NJ.

Erik Nilsen, T., Li, J., Johnsen, S.O., Glomsrud, J.A, 2018, Empirical studies of methods for safety and security co-analysis of autonomous boat. Safety and Reliability-Safe Societies in a Changing World

Jérémie, G, 2016 Hazard analysis of human-robot interactoin with HAZOP-UML. Safety science, 84, 225–237.

Hemsley, K.E., Fisher, E., others, 2018, History of industrial control system cyber incidents, Technical report, Idaho National Lab.(INL), Idaho Falls, ID (United States).

International Electrotechnical Commission, others, 2006, Analysis Techniques for System Reliability: Procedure for Failure Mode and Effects Analysis (FMEA); International Electrotechnical Commission.

Lisova, E., Sljivo, I., Causevic, A, 2018, Safety and Security Co-Analyses: A Systematic Literature Review. IEEE Systems Journal, pp. 1–12. doi:10.1109/JSYST.2018.2881017.

Macher, G., Armengaud, E., Brenner, E., Kreiner, C, 2016, A Review of Threat Analysis and Risk Assessment Methods in the Automotive Context. International Conference on Computer Safety, Reliability, and Security, pp. 130–141

McDermott, R., Mikulak, R.J., Beauregard, M, 1996, The basics of FMEA; SteinerBooks

NIST, E.A, 2014, NIST special publication 800-53 revision 4 recommended security controls for federal information systems and organizations. CreateSpace, Paramount, CA.

Patel, K.K., Patel, S.M., 2016, Internet of things-IOT: definition, characteristics, architecture, enabling technologies, application and future challenges, International journal of engineering science and computing, 6, 6123–6131.

Sabaliauskaite, G., Adepu, S., Mathur, A, 2017, A Six-Step Model for Safety and Security Analysis of Cyber-Physical Systems. In Critical information infrastructures security; Havarneanu, G.; Setola, R.; Nassopoulos, H.; Wolthusen, S., Eds.; Springer: Cham, Vol. 10242, Lecture Notes in Computer Science, pp. 189–200. doi:10.1007/978-3-319-71368-716.

Single, J., Schmidt, J., Denecke., J, 2020a Ontology-Based Support for Hazard and Operability Studies. International Journal of Safety and Security Engineering, 10, 311–319.

Single, J., Schmidt, J., Denecke., J, 2020b Knowledge acquisition from chemical accident databases using an ontology-based method and natural language processing. Safety Science, 129.

Single, J., Schmidt, J., Denecke., J, 2020c, Computer-Aided Hazop Ontologies and Ai for Hazard Identificationand Propagation. Computer Aided Chemical Engineering, 48, 1783–1788

Strobl, S., Hofbauer, D., Schmittner, C., Maksuti, S., Tauber, M.; Delsing, J, 2018, Connected cars — Threats, vulnerabilities and their impact. Proceedings 2018 IEEE Industrial Cyber-Physical Systems (ICPS); IEEE: Piscataway, NJ,375–380. doi:10.1109/ICPHYS.2018.8387687.

Toth, P, 2017, NIST MEP cybersecurity self-assessment handbook for assessing NIST SP 800-171 securityrequirements in response to DFARS cybersecurity requirements (Handbook No. NIST HB 162)(p. 170). Gaithersburg, MD: National Institute of Standards and Technology.

Verma, S., Gruber, T., Puschner, P., Schmittner, C, 2019, Combined Approach for Safety and Security. doi:10.13140/RG.2.2.15021.13283.