CHEMICAL ENGINEERING TRANSACTIONS
VOL. 77, 2019
A publication of AIDIC
The Italian Association of Chemical Engineering
Online at www.cetjournal.it
Guest Editors: Genserik Reniers, Bruno Fabiano

ISBN 978-88-95608-74-7; **ISSN** 2283-9216
DOI: 10.3303/CET1977151

Plant Security – Public Awareness and Mitigation of Third Party Attacks as a new Layer of Protection in the Safety Concept

Jürgen Schmidt

CSE Center of Safety Excellence gGmbH (CSE-Institute), Pfinztal, Joseph-von-Fraunhofer Str. 9, 76237 Pfinztal, Germany
juergen.schmidt@cse-institut.de

Technical Safety has been improved to a significant extent during the last thirty years. This holds for chemical and petrochemical plants as well as for oil and gas pipelines - international and national statistics show a decrease in the number of events. Nevertheless, catastrophic incidents can't be fully excluded in future. Third party activities like cybercrime attacks on operational technology, excavation and drilling into pipelines, or accidents during maintenance and service are main reasons for these incidents. With today's State of Safety Technology, a wider protection of the infrastructure would lead to a non-acceptable effort. However, especially in Germany population density increases while public acceptance of incidents decreases continuously.
The CSE Center of Safety Excellence initiated a center for safety integrity and security "**CeSIS**" with the intention to develop new security measures for safety related control systems of plants integrated into today´s OT environment and to combine latest navigation and detection technologies for a development of a new anti-collision system to avoid third party incidents on pipelines. In addition, an innovative communication concept should encourage the motivation of the general public to secure actively the protection of plants and pipelines.
In the presentation, several new measures to mitigate third party attacks and incidents are proposed to define a new barrier in the Layer of Protection Concept for plants and pipelines and to integrate security as part of the overall safety concept.

1. Introduction

International and national statistics [EGIG, 2011; Dietsch et.al., 2016] show a continuous decrease in the number of events at process plants and per 1000 km pipeline length as a result of a permanent increase in Technical Safety during the last thirty years. Nevertheless, catastrophic incidents like explosions in the harbour of Tianjin and Ludwigshafen or gas explosions in Ghislenghien [Gis2014, 2018], Gräveneck [Gräv2008, 2018] or Oppau [Lu2016, 2018] can't be fully excluded. The reason for these incidents are mainly third party activities of one of the following types: (1) mechanical damage, e.g. by excavators and drilling machines, on a safe pipeline (2) cyber criminals e.g. on industrial control and safety systems and (3) human error, e.g. accidents during inspection, repair or maintenance in a wrong part of a plant. All types are external interference of safe plants or pipelines. Different research and development activities are needed to effectively enhance the current safety standard of process plants and gas transmission pipelines against third part impacts. An innovative plant security concept is needed - it is time for a paradigm shift: control and safety systems must be checked on new types of vulnerabilities and effectively managed by means of a specific Plant Security Management System (PSMs). This is the task of the **Ce**nter for **S**afety and **I**ntegrity **S**ystems (**CeSIS**) [CESIS, 2019] and its cyber crime prevention project PSM2x [PSM2x, 2019]. Additionally, pipelines shall be protected by (1) a **Th**ird party **an**ti-**c**ollision **s**ystem (**THANCS**) based on latest Industry 4.0 opportunities and (2) an active role of the population to ensure pipeline security. This initiatives and projects are latest parts of the prevention of third party interference activities and the start to introduce a new layer of protection in current safety concepts

Paper Received: 24 February 2019; Revised: 28 May 2019; Accepted: 15 July 2019

Please cite this article as: Schmidt J., 2019, Plant Security – Public Awareness and Mitigation of Third Party Attacks as a new Layer of Protection in the Safety Concept, Chemical Engineering Transactions, 77, 901-906 DOI:10.3303/CET1977151

2. New Layer of Protection for Plant Security

Safety concepts are used in industry to systematically protect people and the environment from hazards of technical plants. The protection of humans and the environment is particularly high if it is ensured by several independent measures. The measures can be combined in layers of protection, Figure. 1. Every single layer is part of the concept and helps prevent disruptions or at least limit the effects of disruptions. Not every measure can be implemented in the same high quality. For this reason, a distinction is made between preventive safety measures and primary and secondary protective measures within the safety concept. Every protective measure is subject to particularly stringent requirements, so that it can be safely applied even in the case of a rare malfunction. The effectiveness (safety integrity), accuracy and availability of the protective measure must be proven.

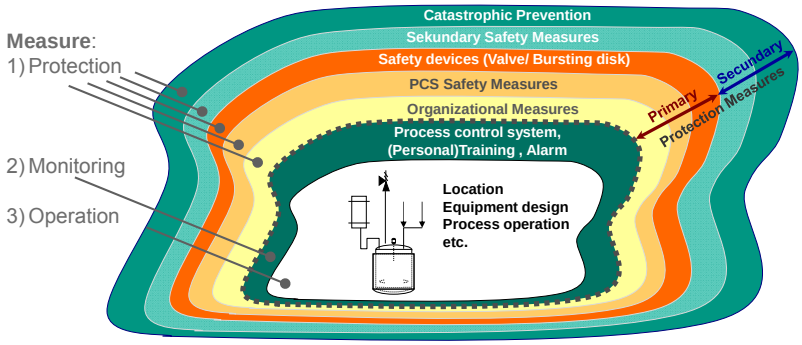

Figure. 1: Layer of protection in a safety concept for technical plants

Security shall be a topic in almost all layers of protection. The typical physical fence of a plant or site is not sufficient anymore – in addition, a cyber fence for all electronic devices is needed. Unfortunately, security is most often not a topic within a safety analysis. At least a high level of awareness is needed to protect the safety devices, process controller, communication networks and safety related interlock systems. Security is in the response of the operational technology (OT) departments, safety engineers are not trained and not responsible for this technology. And the typical OT strategy is to protect the environment (network) around the safety systems instead of closing the gaps of the systems itself. Is this the most effective way to prevent third party interference by means of hacking attacks? At least an additional layer of protection in the safety concept is needed to sharpen the awareness of this important topic – this layer is called Plant Security, Figure. 2.
Considering pipeline safety technology, third party interference caused by caterpillars, drilling machines, agriculture and forestry machines are the main hazard but protection measure are only organizational. Human errors are the main cause for more than a billion Euro damage costs only in Germany each year. Third party interference on pipelines shall be also part of the plant security concept and integrated into the proposed new layer of protection.

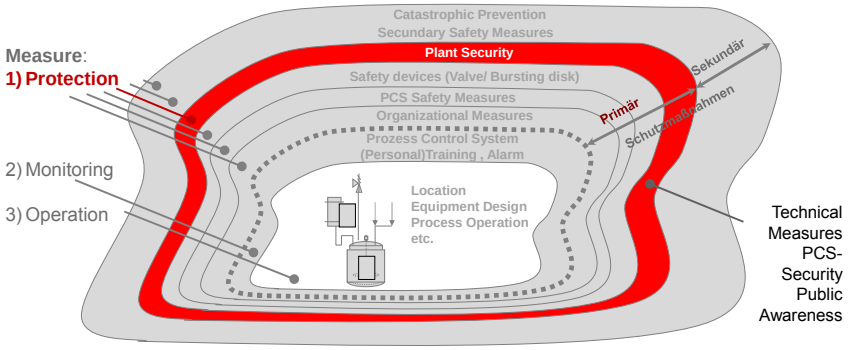

Figure 2: – New layer of protection called Plant Security in a safety concept. The CSE Center of Safety Excellence initiated CeSIS [CESIS, 2019] and PipeSecure2020 [Secure2020, 2019] to define specific measures for Plant Security.

3. Center of Safety Integrity and Security (CeSIS)

CeSIS is an innovation center for plant security founded in 2018 by a cooperation of the company's CSE-Engineering (safety) and 8com (IT security). The objectives are to protect safe plants and pipelines against:

- attacks by unauthorized persons (e.g. cyber-attacks) and
- third-party incidents (e.g. excavators, drills, human error etc.) in technical systems (e.g. chemistry, petro-chemistry, pharmacy, power plants, and critical infrastructure)
- human error during maintenance and service.

PSM2x [PSM2x, 2019] is a cooperation project within CeSIS for industry partners for the implementation of plant security guidelines at two plants each from the area of chemistry/petro chemistry and gas transportation is. The objectives of the project are:

- Analysis of plant security risks with the latest detection techniques in a realistic plant environment
- Simulation of attacks on PCS and SSPS plant networks to visualize vulnerabilities
- Planning, selection and definition of measures for prevention, detection, response of cyber attacks
- Cyber environment monitoring with test environment for sensors, PCS and SSPS

By means of the project **PSM2x** guidelines, rules, regulations and the latest protection concepts are to be put into practice in detail using examples of real plants. So far, many companies differentiate between safety and security. A security culture is often not established (yet), security management systems don't cover all relevant risks and security measures aren't managed centrally. In several applications an asset monitoring for the current state of security in operation is missing. With **PSM2x** the vulnerabilities of security and safety measures are to be uncovered systematically and the necessary systems and documents as well as measures are to be developed in detail. It is key important for the PSM2x project partner to involve all parties necessary to realize safety functions in process plants and pipeline networks – sensor, PCS and SSPS manufacturer as well as plant operators, safety and security specialists and authorities. The project is outlined for 2 years, where three major topics are investigated:

(1) Development of the CeSIS Plant Security Management System (PSM):
- Recommendations for the protection of technical systems against cyber attacks
- Plant security guidelines, safety goals, security monitoring
- Requirements for personnel structures and processes
- Concretization of directives like NAMUR I KAS I BSI I Seveso III I ISO
- Plant security asset management
- Plant security detection & reaction

(2) Plant Security Awareness & Culture
Implementation of plant security management for technical facilities within a company for the following areas: people, technology, operation, maintenance, inspection, auditing

(3) CeSIS Plant Security Training
- Training for security culture and implementation of protection measurements against cyber-attacks
- Integration of plant security into the risk management of plants

In detail, vulnerabilities of safety channels consisting of sensors, PCS and/or SSPS devices and actuators are investigated to protect the **Pr**otection & **I**nterlock **S**ystem for **O**perational **N**etworks (PrISON Zone). This includes standard and latest safety technology like model-based safety related PCS systems, Figure. 3, as developed at the CSE Center of Safety Excellence.

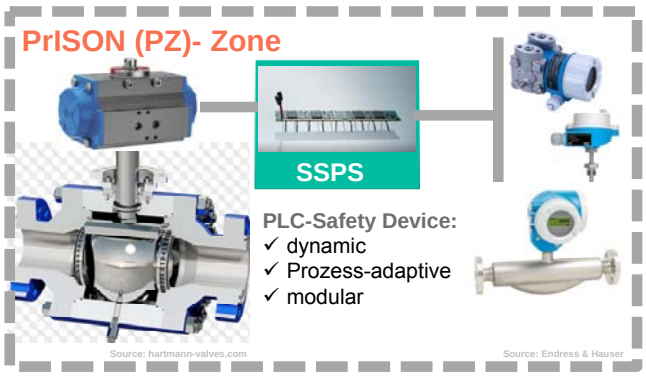

Figure. 3: Protection zone around a smart high integrity protection system (SmartHIP)

4. PipeSecure2020

PipeSeucre2020 is another initiative to improve the safety of technical plants – in that case pipeline systems – and to define measure for the new layer of protection Plant Security. The critical infrastructure gas is at least in Germany considered more and more sensitive in the overall energy mix. Renewable Energy is very popular in Germany and seem to be available limitless and with less potential hazards compared to natural gas. For a major part of the German society the need for natural gas is not obligatory. Any incident and especially a catastrophic incident may strengthen the public demand to further increase the security of natural gas pipelines. Hence, a continuous improvement of the existing technical safety concept for gas pipelines by means of adaptation to the current State of Safety Technology is necessary. A major impact on the concept is to prevent external interference.

The CSE Center of Safety Excellence initiated the "**THANCS**" program (**Th**ird party **An**ti-**C**ollision **S**ystem) with the intention to combine latest navigation and detection technologies for a development of a new excavator anti-collision system to avoid third party incidents. In addition, an innovative communication concept should encourage the motivation of the general public to secure actively the protection of pipelines. Based on the **Nudging-Principle**, people's behaviour should be altered in a predictable way without prohibitions, instructions or significant changes in economic incentives [Thaler et.al. 2008]. Present types of communication are used mostly for an information transfer to strengthen the public perception of safety, but do not encourage the public awareness. To introduce a new awareness and mitigation concept, latest findings of risk acceptance and communication shall be applied to parties living within a zone of potential consequences of natural gas pipelines. Risk shall be understood, accepted as part of a life, but no fear shall be inspired. In many cases, engineering and objective argumentations, which are dominated by numbers, are insufficient to encourage the necessary trust in the communication. The situational circumstances of those communications have to be suited to the typical application procedure (heuristics) of nontechnical people.

The development of new layer of protection in a security concept for the gas infrastructure to protect pipelines from external interferences is the aim of the initiative "PipeSecure2020" at the CSE Center of Safety Excellence. The CSE is a non-profit competence center for research and education in the field of process and plant safety. The center is guided by an industrial advisory board in the areas of chemicals, petrochemicals, oil and gas and has special knowledge and decades of experience in handling and protecting risks of technical plants. The CSE Society includes about 50 renowned companies and institutions. The CSE has the challenge to develop innovative safety concepts in order to increase the global and cross-industry safety of critical infrastructures. A world-scale plant to perform flow measurement and type testing of safety device with pressures up to 3400 bar (~ 50 000 psi) is under construction, *Figure 4*. The plant is built on the site of the Fraunhofer Institute for Chemical Technology in Pfinztal near Karlsruhe, Germany. Research is embedded in an interdisciplinary education of young academics in the field of process and plant safety at Karlsruhe Institute of Technology, the Technical University of Kaiserslautern and the University of Applied Science in Karlsruhe.

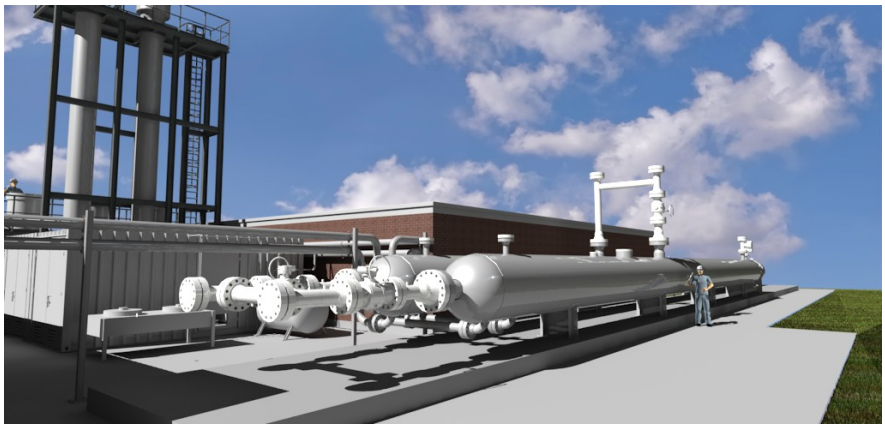

Figure 4: CSE High pressure loop for flow measurements and type testing at pressures up to 3400 bar

5. THANCS Program

The CSE-Institute aims to develop an innovative alarm system to automatically warn the operator of an excavating machine when approaching a gas pipeline and switches off the construction or agricultural machinery before an actual contact happens. On the one side, these Technical Security measure increase the

protection of gas pipelines for the construction industry. On the other side, potentially affected persons in the vicinity of gas pipes are also better protected. As a first easy and inexpensive preventive security measure, a warning system embedded in a mobile device is planned. Machine operators of excavators and drilling machines will be warned of a damage to gas pipelines optically and acoustically from their mobile device. Gas network operators will be identified and informed about the actual risk situation evaluated on the basis of e.g. the population density in the surrounding of the pipeline. To enable the availability in rural areas (gaps in the mobile device network) or urban building situations, in a subsequent step this alarm system will be enhanced to a local autonomous system. An appropriate detection system for gas pipelines must be found in addition to the mobile device warning system. Measuring systems from other branches like the archaeology and the measuring principle of the geomagnetism offer a good source base for that purpose. On the basis of the autonomous alarm system, a prototype of an automatic anti-collision system in a construction machine that switches off the machine before a contact with a gas pipeline happens (Industry 4.0 Device) can be developed.
For the conversion of these technical security measures precise geodata are necessary for the spatial position of all pipelines. Present offers for pipeline network information like the nationwide management system of pipeline net data information (BIL) are currently based on available two-dimensional geographical data. These data are received from responsible gas net operators with a certain degree of incompleteness and exactness, for instance, of the depth of a pipeline. The European guideline **IN**frastructure for **SP**atial **I**nfo**R**mation in **E**urope (INSPIRE) may lead on a long term basis to more precise electronically available data of critical infrastructures but may involve further potential security weak points. The digitization and the comparison of data from the information of gas net operators and public sources is a challenge within the project. Suitable measuring methods, for instance, GPS detection or ultrasonic measurements, must be further optimized to allow the integration of these data from inspection devices.

6. EURIC: European Risk Communication Platform

A comprehensive protection from external interferences on gas pipelines may be attained if in addition to the construction industry the society or at least potentially affected people are integrated. This new concept of protection does not yet exist in any European country, neither in Germany nor in another European land. The population will be involved actively into the protection of critical infrastructure and promote the awareness in public. Analogous to the behavioural employment protection in companies that demand a personal responsibility of their employees for their own safety, the CSE Center of Safety Excellence aims to develop a suitable communication concept and public education program.
For this purpose, the risk perception of the population has to be examined regarding the hazards of the critical infrastructure. The risk perception and acceptance of the population shall be investigated for different risk-based and deterministic concepts of technical safety. On this basis, the behavioral pattern of the population in present public information events, can be directed. Risks have to be appointed openly and target-audience-oriented, civil reliance has to be built and converted into a positive attention. To date, the public discussion on technical risks, for example, in project approval procedures, is mostly only based on a mediation of information that strengthens the security feeling of the citizens, indeed, but does not promote general attention in the public. Potential hazards are often not addressed but faded-out. The high level of technical safety may lead to an “emotion of zero-risk” in the society with the consequence of zero awareness even to obviously risky situations. Instead of acting towards hazard mitigation or following an escape reflex a minority of the society tend to fully fade-out hazardous situations. Hence, an innovative communication draft should be compiled outgoing by current citizen's information and integrated in new media and topical results of risk perception. For this, qualitative customer surveys will be carried out on the basis of morphological effects and communication research. A major aspect is to develop a communication strategy. The aim of the new communication strategy is to train people’s awareness on risks and to motivate them to report potential hazards to a central information system. In this context, the term mindfulness of the public means to understand, detect and report potential hazards or abnormalities in construction areas. This concept is based on the Nudging Principle and should influence the civil behavior without giving orders or imposing bans. For this, it is essential that a respectable trust base is created between the population and the gas net operator or a third party (e.g., the CSE Center of Safety Excellence). The strategy should motivate the population to announce potential hazards to a central information system from their point of view, which initiates safety relevant measures according to a risk judgement and informs gas net operators and authorities if necessary. The situational circumstances of those communications must be suited to the typical application procedure (heuristics) of nontechnical people.
At the same time, an assessment matrix for the classification of the hazard potential, which is based on simple, automated risk assessment methods, should be developed. In this way, measures can be defined in a

catalog, which may be activated depending on the respective hazard message. Thereby, a determination of the necessary information for the evaluation of potential hazards is essential.

7. Conclusion

The CSE Center of Safety Excellence founded the Center of Safety Integrity and Security (CeSIS) and initiated the PipeSecure2020 program with the objective to improve the security of technical plants against cyber-attacks and the critical infrastructure gas by protecting the pipeline from external interferences. A new Plant Security Layer is recommended for the LOPA safety concept to enhance the awareness and to define appropriate safety measures for a safer operation of plants and pipelines. For that, CeSIS will define a specific Plant Security Management System based on research and experience from two different plants to be investigated during the following two years in the PSM2x industry project. Secondly, PipeSecure2020 is initiated to develop (1) an innovative alarm system for machine operators of excavators and drilling machines and by a further development to an automatic anti-collision system for such devices. For that, precise local geo-data of gas pipelines are needed. The development of (2) risk-based communication measures has the aim of encouraging not only machine operators, but also the population according to the principle of Nudging, so that any impermissible approach to a gas pipeline is preventively avoided. The new program aim to result in a comprehensive new protection approach to pipeline security for critical gas infrastructure.

References

CESIS: Center of Safety Integrity and Security CeSIS to investigate and define measures to avoid third party attacks, https://cse-engineering.de/cesis/, 03 February 2019

Dietzsch: Frank Dietzsch (DVGW), Ronny Lange (inetz GmbH), Jonas Schmidinger (bnNETZE GmbH) & Dr. Michael Steiner (Open Grid Europe GmbH). Bestands- und Ereignisdatenerfassung Gas – Ergebnisse aus den Jahren 2011 bis 2014; Energie | wasser-praxis 1/2016

EGIG: European Gas Pipeline Incident Data Group (EGIG): 8th EGIG-report 1970-2010, gas pipeline incidents, N.V. Nederlandse Gasunie, Groningen, 2011.

Gis2014: http://www.stern.de/panorama/weltgeschehen/belgien-15-tote-bei-gasexplosion-3072720.html, 05. October 2018

Grä2008: http://www.spiegel.de/panorama/gasexplosion-in-hessen-100-meter-flamme-schoss-auf-dorf-zu-a-502565.html,

Lu2016: http://www.spiegel.de/panorama/ludwigshafen-gasexplosion-hinterlaesst-ein-truemmerfeld-a-999175.html, 05. October 2018

PSM2x: Project of the CeSIS Group to define Plant Security Measurements explored by 12 companies and applied at current technical plants. https://cse-engineering.de/cesis/psm2x/, 03 February 2019

Seucre2020: Pipeline security project to mitigate third party attacks from gas transmission lines. https://cse-institut.de/pipesecure2020/, 03 February 2019

Thaler: Richard Thaler und Cass Sunstein: Improving decisions about health, wealth and happiness; 2008