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/CET1977152

An overview of Cyber Attack to Industrial Control System

Roberto Setola[a], Luca Faramondi[a], Ernesto Salzano[b], Valerio Cozzani[b,*]

[a]Complex System & Security Lab – University UCBM, Via A. del Portillo, 21, 00128 Roma (Italy
[b]Department of Civil, Chemical, Environmental and Materials Engineering – University of Bologna, Via Terracini 28, 40131 Bologna (Italy)
valerio.cozzani@unibo.it

The relevance of OT (Operational Technology) in Seveso plats has largely increased in recent years thanks to several benefits related to the improvement of efficiency, quality of the production, and cost reduction. Unfortunately, the use of these technologies exposes the plants to cyber threats. Indeed, a cyber-attack may cause the interruption of the production, and, at worst, could manipulate the control process in order to induce a catastrophic event. In recent years, several cyber-attacks have been performed against Industrial Control Systems. In this paper, we provide a process-engineering oriented overview of those attacks with the aim of illustrating their behavior. Particular attention is payed to Triton attack, being the first worm specifically designed to attack a Safety Instrumented System. The paper concludes with some consideration about a relevant approach that might be useful to increase the protection of the Seveso ICS.

1. Introduction

The acronym **OT** (somehow in contrast to the initials **IT**) refers to Operational Technology, i.e. that set of technologies, software and hardware, directly connected with the production, transportation and transformation of assets. Actually, it refers to everything that concerns the monitoring and control systems of the production system that are also specified with other acronyms as ICS, SCADA o PLC.
Over the last few years, the OT has complaint massively the IT Technologies, littering gradually property ones in favour of solutions based on off-the-shelf products. As much as, analogous to the undeniable benefits that we have observed in our daily lives in terms of improving the quality, the production and cost-effectiveness of the different manufacturing, has introduced in the OT domain the vulnerability and the threats inherent in the IT sector.
The problem is that the OT has several peculiarities that doesn't make it easy to transpose the protection measures that are usually adopted for the IT systems.
In fact, the OT is characterized in first place by the type of information exchanged on the network: extremely high quantities of information packets with limited dimensions (of the order of a few byte), coming from a large number of sources. This means that mechanism such as encryption (usually used to avoid the disclosure of information) or digital signature (used to avoid the alteration of the data) result difficult to adopt because they could introduce an elevated overhead and an inacceptable delay in the data-processing.
That's why another aspect to consider is the restriction of the hard real-time, in other words the requirement to guarantee the maximum execution time for every task. This constraint, essential for controlling most of the industrial processes hence to avoid that the very same behave in a critical or/and dangerous situation, along with the fact that these processes operate in a continues loop 24x365, makes it difficult to use the anti-virus systems and the activities of patching. Everything is even more complex because these systems have an extremely wide set up and a lifespan layout of more than ten years.
However, the most critical aspect related to the OT systems is that cyber-attack could create a potential impact not only in economic order, but also in kinetic order, i.e. the potential to damage physical objects. In other words, it's possible through a cyber-attack to modify conveniently the functioning of a process to the point of bringing it to a mechanical break point.

Paper Received: 5 February 2019; Revised: 26 April 2019; Accepted: 10 July 2019

Please cite this article as: Setola R., Faramondi L., Salzano E., Cozzani V., 2019, An overview of Cyber Attack to Industrial Control System, Chemical Engineering Transactions, 77, 907-912 DOI:10.3303/CET1977152

This was, for more, the purpose of the AURORA project, led by the Idaho National Lab (USA): using a cyber-attack to destroy a power plant of 27 tons (Cárdenas et al., 2008). This is the demonstration that a cyberattack can lead to a mechanical damage, comparable to what is achievable with an explosive charge, with the advantage that this action could be launched from thousands of miles away, and the possibility to date back to the author is extremely reduced.
This means that a cyber-attack against these systems, besides the economic damage due to a failure and a damaged reputation (as for a normal cyber-attack against IT systems) can create problems for the environment and to people's health. Such an aspect can be dramatically emphasised inside a SEVESO plant due to the intrinsic hazard of the plant.
Another important aspect are the recovery times. In fact, while the replacement of a component of a computer system is an operation that can take place in an estimable time within hours or at most days, the maintenance of a mechanical element (like the power plant that has been destroyed during the AURORA experiment) can take months or even years of time.
It must be said, however, that until the year 2010 only a small amount of people thought that it was possible to realize an action like (it has been done by) the AURORA project. This was because till this action could really damage an OT system it cannot limit itself to paralyze/block the system (something that even can be made in principle with a simple DoS\DDoS attack) but must be able to "conduct" the physical process in a critical state. To do this we need to, besides a proper knowledge about information technology (both proper expertise of the IT elements and the connection of the peculiarities of the ICS systems in terms of protocols, languages and systems) but even a specific knowledge of the physical processes, and not least, a detailed comprehension of the semantics of the different variables. In fact, not only should the cyber-attack be able to send legitimate commands (syntactical correct) but must also be able to know which commands to send and to which objects.
For a long time, it was considered that the complexity of the OT systems represented an adequate barrier: a security by obscurity strengthened by the peculiarities of these systems. As a matter of fact, the only accomplished attack we know was against the water control system in the small city of Maroochy Shire (Australia), but in this case the attacker was one of the developers of the system, who tried to set up an extorsion (Slay & Miller, 2007). Indeed, several experts assumed that the AURORA experiment was possible because the attacker has significant a priori knowledge about the plant and adequate access to it in order to manipulate some of the "mechanical" protection elements.
In 2010, the scenario changed radically thanks, or better due to the Stuxnet worm (Langner, 2011). This worm is still considered as one of the most complex software programs ever made with an estimated development cost about over 20M$. It's the first of his kind specifically designed to attack a PLC, and precisely a Siemens'PLC. In particular, it seems that the "real" target of Stuxnet was to alter the rotational speed of some motors if specific conditions could be proved. Very briefly, as a first step the worm scans the infected computer to check if there is the Siemes PLC suit installed. If so, it substitutes a legitimate .DLL file with a modified one able to send a specific "challenge" to the connected PLC. In case of a positive answer from the PLC, the worm updates the value of the speed rotation. Nobody knows who the creators of this worm are, or even what are their real target(s). Some rumour suggest that the primary target of Stuxnet was the atomic site of Natanz (Iran) and specifically the destruction of the centrifuges for the uranium enrichment; suggesting that the worm could have been designed by nations that are historically opposed to the Iranian atomic program. Regardless of the creators and the targets, one thing is clear: Stuxnet was the very first cyber-weapon realised to create "focused" damage to mechanical infrastructures taking advantage of the cyber vulnerability of the OT systems.
Moreover, Stuxnet shows that it is possible to perform a cyber attack against an OT system and that such an attack can induce kinetic consequences.

2. Operational Technologies

The acronym **OT** (somehow, in contrast with the acronym IT) underlying the set of technologies, software and hardware, directly connected with the production, the transport and the transformation of assets. Therefore, besides the physical elements that represent the production system, also untouchable tools like network and communication protocols are a part of the set. These tools are necessary to guarantee the safety of the information flow which regulates and controls the plant. There is therefore a strong relation between such technologies and everything related to the monitoring systems and the control of the manufacturing systems.
The industrial systems that we analyse, often specified with the acronym **ICS** *(Industrial Control System)*, include well-known systems as **SCADA** *(Supervisor Control and Data Acquisition),* and have been introduced since the 1960's for monitoring the production lines inside the manufacturing companies. Today they are very often associated to large-scale infrastructures. Further the **DCS** *(Distributed Control System)* are widely employed in the process industry, particularly the petrochemical industry, for the management of plants,

refinery and holder. The last ones differ from SCADA systems in numerous features: control techniques, application areas, size of the system, interaction with the worker, etc…
In the control systems mentioned above, the task to supervise the process is entrusted to devises like **PLC** *(Programmable Logic Controller)* with the purpose to manage the supervision activities of the measures of the different plants, to elaborate a control strategy of the process and to implement (or rather to modify the behaviour effectively intended).
Notice that while IT systems that has been designed to interface with a human operator, the OT systems must anyway interface with “physical systems”, such as chemical reactions, a liquid flow, warming and cooling processes, a motion of an object, etc. It follows that the time and methods of interaction between the process and the control system can’t be “dictated” by the OT system as it happens in IT systems where the human operator (being a smarter element) understands and learns how to use the IT tool and its interfaces, but an OT system has to adapt and operate with the times and methods induced by the underlying process. Specifically, this implies that, in order to guarantee high process levels, the OT systems are characterised by a high level of determinism whether for what concerns the input data and the execution times of the individual tasks. In other words, the OT systems must be in the presence of a certain sequence of inputs, whereas the output is always the same after a certain time interval (requirement of **hard-real time**), an aspect that isn’t neither expected nor required in normal IT systems.
A direct implication is the extreme complexity connected to the introduction of classical tools of cyber security, such as anti-virus and firewall, in industrial systems since the mode of operation of these tools is poorly combined with the characteristics of SCADA and ICS because it inhibits, for a unmeasurable period of time, the normal operation of the system and therefore violates the fundamental requirement on the duration of the single task (which could also have dramatic consequences on a production process, for example an OT system that controls an exothermic chemical reaction). In most industrial systems, the precision with which the operations necessary for the correct process of the system are carried out is a fundamental requirement. For this reason, the operating systems dedicated to OT systems differ from the classical operating systems, especially in the management of task priorities. The inclusion of classic cyber threat identification techniques means to include control routines that modify the smooth running of activities generating delays that, although they may be quantitatively unimportant, makes the control system less ready and far from the precision for which it was designed.
The other key aspect to consider when analysing OT systems is that it must operate continuously until the underlying physical process is active (i.e. until it is replaced by another monitoring and control system). The period of activity of these systems can range from a few hours up to several decades, for example in the case of a blast furnace. This element brings out two significant consequences. In the first place, the life time of these systems is much higher than the average life time of an IT system, which implies the use of **"legacy"** software hardware, which often results in a system that is necessarily "out-of-date" and therefore with possible difficulties in finding updates and potential incompatibilities with the latest generation tools. The motivation lies in the impossibility to suspend the monitoring and control of this type of systems, even for limited time horizons, with the aim of making updates. Consequently, the other aspect is the extreme difficulty, and in some cases the impossibility of suspending the operation of the OT system to proceed with the installation of software updates. All this clarifies, as illustrated in a research by the Red Tiger Security, in latency for the installation of security patches of about a year (with peaks that reach even 3 years).
This delay, which may seem anomalous, derives not so much from a lack of interest of the operators who deal with detecting bugs related to cyber security, whose level of awareness has grown a lot in recent years, but from the need to prevent that installing patches can create problems for the underlying production process. It must be considered, in fact, that these systems are born primarily to ensure adequate levels of safety and, therefore, any intervention (including software updates) must be achieved and realized only in conditions of process security that cannot always be guaranteed in absence, even for a few fractions of a second, of the OT monitoring and control system.

3. Evolution of the scenario

In recent years, cyber attacks to Seveso sites emerged as another possible initiator of malicious accident chains. Cyber security threats are becoming a growing concern for all those industrial sectors in which automation is high, which includes the chemical and petrochemical industry. The study by Casson Moreno et al. (2018) concluded that, currently, cyber threats hold the fourth position among those related to security, following terrorism, vandalism and physical theft. According to some estimates, the percentage of cyber attacks is bound to increase in the coming decades.
Such an increment has been evident since 2001 and was related both to the increasing relevance of chemical and petrochemical plants as possible targets but also due to the large adoption in such plants of off-the-shelf

products due to the strategies adopted to manage the Y2K bug, i.e. dismission of legacy and proprietary system in favor of commercial platform (e.g. Windows, Linux, ecc).
As mentioned before, until Stuxnet there hasn't been no evidence about the feasibility of an effective cyber attack against OT. Indeed, even if some episodes affected some OT (see for example (Bologna & Setola 2005)) they were generally unplanned "side effects" related to the saturation of communication channels.
After Stuxnet there has been an increased attention to cyber security of OT systems and several scholars published research on possible cyber attack strategies and vulnerabilities, see among others(Ten et al., 2008), (Bernieri et al. , 2017), (Creery &., & Byres, 2005), (Cherdantseva et al. 2016).
Moreover, there have been also several real cyber attacks against infrastructures and plants. These attacks adopt different strategies and tools but all of them appear as proof of concept, i.e. as tests to validate the methodologies and to emphasize the potentiality of these class of attacks. There is no evidence that such attacks have been performed by the same group or by linked group, but they appear as steps of a single strategy as schematically illustrated in Figure 1.

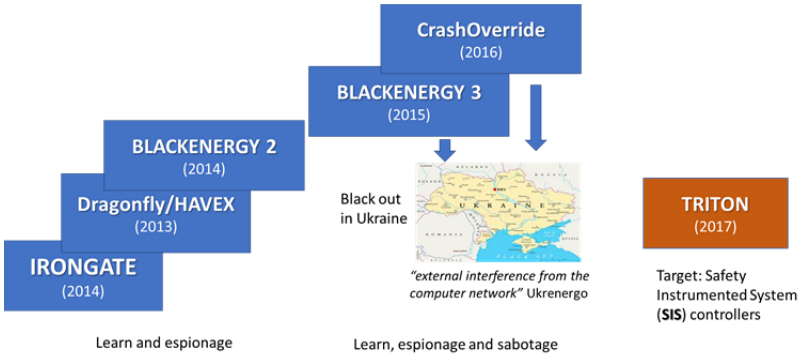

Figure 1: Evolution of cyber attacks against OT after Stuxnet.

One if the first malware specifically designed for OT system discovered after Stuxnet has been **Irongate** (2014) (Homan et al. 2016). As Stuxnet, it operates against Siemens' PLC environment performing a man-in-the-middle attack. Specifically, the malware replaces a DLL with a malicious one, that is able to record five seconds of 'normal' traffic from a PLC to the user interface and replays it, while sending different data back to the PLC. Notice that Irongate operates only inside a simulation environment PLCSIM. Hence Irongate is able to perform an active masking strategy to hide the manipulation activities in order to avoid of being discovered (for the same reason the malware does not run if VMware or Cuckoo Sandbox environments were employed in order to avoid triggering sandbox evasion).
In 2013 it has been discovered a large espionage campaign performed via **Dragonfly**. It has been estimates that over 2,000 sites were compromised, with a large emphasis on electric power and petrochemical asset owners. Dragonfly used HAVEX malware to create a map of devices within the OT network. To this end HAVEX uses legitimate functionality in the OPC protocol to identify the different equipment and devices presentin the network with their addresses.
The malware **Blackenergy 2** adopts a different strategie to learn the industrial process. Specifically, the malware monitors the Human-Machine Interface (HMI) to extract relevant information from the graphical representation of the plant and on the base of the activities performed by the human operators. The malware contained exploits for specific types of HMI applications including Siemens SIMATIC, GE CIMPLICITY, and Advantech WebAccess.
Blackenergy 3 is considered the cause of the electric blackout in Ukraine in December 2015 (Case, 2016). The malware, after assimilating the correct functioning of the system learned the operations via analysis of HMI, used legitimate functionalities of distribution management systems to disconnect substations from the grid. Moreover, it uses the KillDisk malware deleting some system files (specifically to cancel serial-to-Ethernet devices) in order to delay restoration activities.
It's interesting to underline the fact that CERT USA has highlighted that this malware has been rediscovered in several control systems of American utilities and that the very same was present in these systems for some time, in some cases even more than 5 years.
One year later, in December 2016, a second black-out hit the Ukraine and this time the electricity operator Ukrenergo clearly declared that the cause of the damage lies in an "external interference from the computer network". The attack was performed using the **CrashOverride** malware (Dragos). This malware, like Blackenergy 3, can introduce "legitimate" commands, managing to manipulate the behaviour of the electricity

network with the aim to create a black-out. However, it adopts a more sophisticated strategy. Indeed, it leverage the OPC protocol to map the industrial network environment and to select its targets; it learns from monitoring HMI the legitimate commands to open closed breakers. Specifically, once the malware identifies the target, it begins an infinite loop and continues to set addresses to this value effectively opening closed breakers. Moreover, it prevents to be discovered creating a Denial of Visibility, i.e. override in the OPC module the legitimate value with the value 0x01 which represents a “Primary Variable Out of Limits” misdirecting operators from understanding protective relay status.
Several scholars stressed that CrashOverride learned through past attacks, indeed it exploits functionalities adopted by Havex (i.e. the use of OPC protocols to map the network) and Blackenergy 2 and 3 (i.e. the use of HMI to learn the functionalities of the system and to generate legitimate commands)
In chronological order the last attack has been discovered in December 2017 with the name **Triton** (Johnson et al. 2017**)**. The peculiarity of this malware is that its targets are the SIS systems (Safety Instrumental System), i.e. the part of the ICS systems, generally separated from the normal systems of process controlling, that are used to prevent catastrophic events. It’s obvious that an alteration/manipulation of a SIS system, in conjunction with another type of event can create extremely dangerous situations. Specifically, the malware attacked the SIS of the Triconex which entered a failed safe state, which automatically shut down the industrial process.
TRITON is also designed to communicate, using the proprietary TriStation protocol, which is not publicly documented suggesting the adversary independently reverse engineered this protocol.
Some scholars suppose that the attacker inadvertently shutdown operations while developing the ability to access to the system.
Notice that a cyber attack to a SIS system could create more dramatic impact, especially if combined with an attack to the SCADA/DCS system, where the last one moves the plant into a critical operational region and the attack to the SIS avoids triggering the emergency procedure. But also, a “simple” attack to SIS could have severe consequences due to the possibility, as shown by the TRITON attack, to showdown the plant.

4. Defence strategies

Therefore, how should the cyber security of an OT system be set up? Surely the strategy of **security by obscurity** based on the use of protocols and proprietary systems (also called legacy) that has lasted for over twenty years does not seem more reasonable, especially considering the wide use of off-the-shelf solutions.
The best way is to adopt a strategy of defence in depth (i.e. with a so-called "onion" approach) able to recognize the presence of a hierarchy of relevance of threats in the various OT systems, introducing barriers and filters that make it extremely difficult for an attacker (but also to prevent the spread of viruses and malware) to access to critical levels, i.e. those levels of the system that supervise and manage the functions that directly guarantee the safety of the process.
This strategy, as illustrated also in the ANSI/ISA 99 standard (ISA99), invites to segment the OT network into **zones**, or gather logical or physical resources that share common security requirements based on factors such as critical issues and consequences. All the operating units within an area are considered trust, while the exchange of information and data with entities belonging to different areas is carefully monitored. It is essential, therefore, that the areas dialogue through a small and well-monitored number of joints (called **conduit**, or conduits). In correspondence of a conduit it is advisable to insert systems able to verify the correctness of the flow using a firewall or similar systems.
In the presence of an "onion" architecture, in which the most sensitive levels are the internal ones, a propagation approach for the commands and information, related to the functioning of the system comparable to a flow that can be oriented from the internal levels to the more external, i.e. from the layers characterized by a higher level of safety towards those considered less sensitive, is preferred. From this perspective, solutions based on devices that allow an information flow only in a unidirectional way are interesting. These systems, generally referred to as data diode, are capable to allow, in analogy to a diode, the flow of data in a one-way mode. Unfortunately, it is almost impossible to limit the flow of information in a single direction, as it is necessary both to receive information from the field and to define set-points, strategies and maintenance activities. This imposes the presence of by-pass systems of the date diode with consequent limitations of the efficiency of this last, making the adoption not very useful in all those cases in which the control activities are in a comparable volume to the monitoring flow.
Other elements to be considered are the presence of mechanisms able to identify incorrect flow (e.g. introduce an Intrusion Detection System – IDS) and/or incoherent data (e.g. via an Anomaly Detection System ADS) so as the capabilities for a strong authentication.
All these activities can be achieved complementing the actual centralised model with solution where smartness is distributed in the edge as suggested in (Bologna & Setola, 2005)

5. Conclusions

The number and the quality of cyber attacks against OT has increased in the last years. However, a large part of the scholars assume that almost all the attacks performed after Stuxnet have to be considered as “proof of concept”, i.e. like tests to verify the real potential and capacity of these cyber-weapons.
There is no reliable data who is behind these tests, but as stressed in the Global Risk Report 2018 (World Economic Forum, 2018) “*the cyber-attack capabilities are developing even more faster than the ability to manage hostile events*”, highlighting how there can be increased potential risks especially in the industrial sector.
The impression of the scholars is that actually behind these actions could “state sponsored organization” motived by geopolitical issue. Notice that recently the NATO recognised the cyberspace like an additional (defensive) domain of operations.
In this scenario it’s undeniable that the protection compared to this class of attacks cannot be entrusted only to private operators, but a strong synergy with public entities is essential.
However, the possibility that the attack capabilities could be gained also by criminal and/or terroristic entities is more and more concrete.
Hence it is mandatory for critical infrastructure operators, and specifically for Seveso operators, to start recognising the problem in order to deeply reconsider the cyber security approach to the OT system in order to adequately manage the actual (and the future) level of threats.

Reference

Bernieri, G., Miciolino, E. E., Pascucci, F., & Setola, R., 2017, Monitoring system reaction in cyber-physical testbed under cyber-attacks. Computers & Electrical Engineering, 59, 86-98.

Bologna, S., & Setola, R., 2005, The need to improve local self-awareness in CIP/CIIP. In Critical Infrastructure Protection, First IEEE International Workshop on(pp. 6-pp). IEEE.

Cardenas, A., Amin, S., Sinopoli, B., Giani, A., Perrig, A., & Sastry, S., 2009, Challenges for securing cyber physical systems. In Workshop on future directions in cyber-physical systems security (Vol. 5).

Case, D. U., 2016. Analysis of the cyber attack on the Ukrainian power grid. Electricity Information Sharing and Analysis Center (E-ISAC).

Casson Moreno V., Reniers G., Salzano E., Cozzani V., 2018, Analysis of physical and cyber security-related events in the chemical and process industry, Process Safety and Environmental Protection 116, 621-631

Cherdantseva, Y., Burnap, P., Blyth, A., Eden, P., Jones, K., Soulsby, H., & Stoddart, K., 2016, A review of cyber security risk assessment methods for SCADA systems. Computers & security, 56, 1-27.

Creery, A., & Byres, E. J., 2005, cybersecurity for power system and SCADA networks. In Petroleum and Chemical Industry Conference, 2005. Industry Applications Society 52nd Annual (pp. 303-309). IEEE.

Dragos, CRASHOVERRIDE Analysis of the Threat to Electric Grid Operations https://dragos.com/blog/crashoverride/CrashOverride-01.pdf

Homan J., S. McBride, R. Caldwell, 2016 IRONGATE ICS Malware: Nothing to See Here...Masking Malicious Activity on SCADA Systems, FireEye, www.fireeye.com/blog/threat-research/2016/06/irongate_ics_malware.html

ISA99, Industrial Automation and Control Systems Security https://www.isa.org/isa99/

Johnson B., D. Caban, M. Krotofil, D. Scali, N. Brubaker, C. Glyer, “Attackers Deploy New ICS Attack Framework, 2017, “TRITON” and Cause Operational Disruption to Critical Infrastructure”, FireEye https://www.fireeye.com/blog/threat-research/2017/12/attackers-deploy-new-ics-attack-framework-triton.html

Langner, R., 2011, Stuxnet: Dissecting a cyberwarfare weapon. IEEE Security & Privacy, 9(3), 49-51.

Macaulay, T., & Singer, B. L., 2016, Cybersecurity for industrial control systems: SCADA, DCS, PLC, HMI, and SIS. Auerbach Publications.

Slay, J., & Miller, M., 2007, Lessons learned from the maroochy water breach. In International Conference on Critical Infrastructure Protection (pp. 73-82). Springer, Boston, MA.

Ten, C. W., Liu, C. C., & Manimaran, G., 2008, Vulnerability assessment of cybersecurity for SCADA systems. IEEE Transactions on Power Systems, 23(4), 1836-1846.

World Economic Forum (2018), “The Global Risks Report 2018”, https://www.weforum.org/reports/the-global-risks-report-2018