inter-eng 2012
The 6th edition of the
Interdisciplinarity in Engineering International Conference
"Petru Maior" University of Tîrgu Mureş, Romania, 2012

CYBER-PHYSICAL ATTACKS: THE ROLE OF NETWORK PARAMETERS

Béla GENGE and Christos SIATERLIS
Institute for the Protection and Security of the Citizen
Joint Research Centre, European Commission
Via E. Fermi, 2749, Ispra (VA), Italy, 21027
E-mail: {bela.genge,christos.siaterlis}@jrc.ec.europa.eu

ABSTRACT

The fact that modern Networked Industrial Control Systems (NICS) depend on Information and Communications Technologies (ICT) is well known. Although many studies have focused on the security of NICS, today we still lack a proper understanding of the impact that network parameters, e.g. network delays, packet losses, background traffic, and network design decisions, have on cyber attacks targeting NICS. In this paper we investigate the impact of network parameters on cyber attacks targeting industrial processes. Our analysis is based on the Tennessee-Eastman chemical process and proves that network parameters have a limited effect on remote cyber attacks.

Keywords: Cyber-physical, attack, network parameters, security, resilience.

1 Introduction

Modern Critical Infrastructures (CI), e.g. power plants, water plants and smart grids, rely on Information and Communications Technologies (ICT) for their operation since ICT can lead to cost optimization as well as greater efficiency, flexibility and interoperability between components. In the past CIs were isolated environments and used proprietary hardware and protocols, limiting thus the threats that could affect them. Nowadays CIs, or more specifically Networked Industrial Control Systems (NICS), are exposed to significant cyber-threats; a fact that has been highlighted by many studies on the security of Supervisory Control And Data Acquisition (SCADA) systems [1, 2]. The recently reported Stuxnet worm [3] is the first malware specifically designed to attack NICS. Its ability to reprogram the logic of control hardware in order to alter the operation of industrial processes demonstrated how powerful such threats can be.

In this paper we investigate the relationship between network parameters and cyber attacks targeting industrial processes. The main goal of our study is to evaluate the impact of network communication parameters on the outcome of remote cyber attacks. The network parameters included in our study are communications delays, packet losses and background traffic, that are typical to Internet communications. The adversary model included in the analysis is capable to communicate with control hardware through legitimate packets. As a physical process we used the Tennessee-Eastman chemical process [4] and the associated multi-loop control system [5].

The rest of the paper is structured as follows. Related work is presented in Section 2, while Section 3 discusses the investigation methodology. Then, Section 4 presents the results of our investigations and the paper concludes in Section 5.

2 Related Work

We start with approaches that assume an adversary that is capable to interact with control hardware using legitimate packets, but is not able to reprogram the control hardware. In this context we find the work of Zhu, *et al.* [6], that focused on securing communications protocols and proposed a secure routing protocol to increase the resilience of Smart Grids. In their work, Nai Fovino, *et al.* [7] proposed a *K-resilient* system together with lightweight cryptography to ensure that running one single command on a control hardware would require the confirmation from K nodes. The importance of cryptography to secure communications was also highlighted in several other approaches [8, 9, 10]. However, these techniques, together with [6] and [7], do not address more sophisticated attacks that manage to com-

promise secure communications protocols and finally reprogram the logic of control hardware.

In the context of the same adversary model are placed the work of Germanus, *et al.* [11] and the work of Avallone, *et al.* [12]. Instead of focusing on cryptographic measures, the two approaches proposed network architectures to increase the resilience of SCADA systems. The work of Germanus, *et al.* [11] employed a peer-to-peer (P2P) overlay network in which P2P communications between redundant nodes were used to implement path redundancy and data replication. On the other hand, Avallone, *et al.* [12] proposed to split packets and send them on two node-disjoint paths in order to limit the adversary's capability to reconstruct the entire information flow.

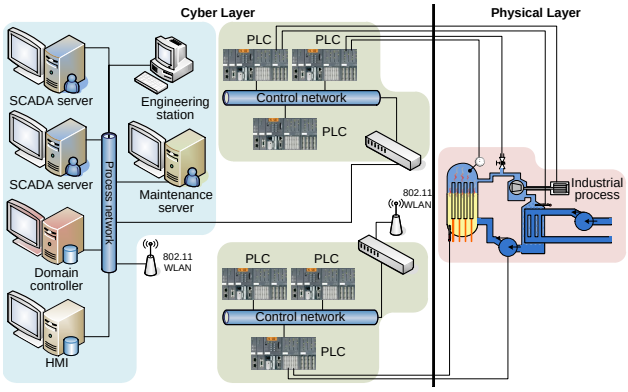

Fig. 1: Process control architecture

3 Investigation Methodology

As already stated, our investigation focuses on identifying network parameters that affect cyber attacks targeting industrial processes. For this purpose one could employ experimentation with real systems, software simulators or emulators. Unfortunately, experimentation with production systems suffers from the inability to control the experiment environment in order to reproduce the results. Furthermore, if the study intends to test the resilience or security of a system, there are obvious concerns about the potential side effects (faults and disruptions) to mission critical services. Software based simulation has always been considered an efficient approach to study physical systems, mainly because it can offer low-cost, fast and accurate analysis. Nevertheless, it has limited applicability in the context of cyber security due to the diversity and complexity of computer networks. Software simulators can effectively model normal operations, but fail to capture the way computer systems fail.

Based on these facts in our study we have chosen a hybrid approach in between the two extremes of pure simulation and experimentation with only real components. That is, we employed an Emulab-based testbed [13, 14] to recreate the control and process network of NICS, including control hardware and servers, and a software simulation to reproduce the industrial processes. For the industrial process we used the Tennessee-Eastman (TE) chemical process model [4] and the associated multi-loop control system developed by Sozio [5].

3.1 Process Control Architecture Overview

Modern process control architectures have two different control layers: (i) the physical layer, which comprises actuators, sensors and hardware devices that physically perform the actions on the system (e.g. open a valve, measure the voltage, etc.); and (ii) the cyber layer, which comprises all the information and communications devices and software that acquire data, elaborate low-level process strategies and deliver the commands to the physical layer. The cyber layer typically uses SCADA (Supervisory Control And Data Acquisition) protocols to control and manage an industrial installation. The entire architecture can be viewed as a "distributed control system" spread among two networks: the control network and the process network. The process network usually hosts the SCADA servers (also known as SCADA masters), human-machine interfaces (HMIs), domain controllers and other installation-specific nodes, e.g. engineering stations, maintenance servers. The control network hosts all the devices that on one side control the actuators and sensors of the physical layer and on the other side provide the control interface to the process network. A typical control network is composed of a mesh of PLCs (Programmable Logic Controllers), as shown in Fig. 1.

3.2 Experimentation Framework Architecture

The experimentation framework developed in our previous work [15, 16] follows a hybrid approach, where the Emulab-based testbed recreates the control and process network of NICS, including PLCs and SCADA servers, and a software simulation reproduces the industrial processes. The architecture, as shown in Fig. 2, clearly distinguishes 3 layers: the cyber layer, the physical layer and a link layer in between. The cyber layer includes regular ICT components used in SCADA systems, while the physical layer provides the simulation of physical devices. The link layer (i.e. cyber-physical layer) provides the "glue" between the two layers through the use of a shared memory region.

The physical layer is recreated through a soft real-time simulator that runs within the SC (Simulation Core) unit and executes a model of the industrial process. The cyber layer

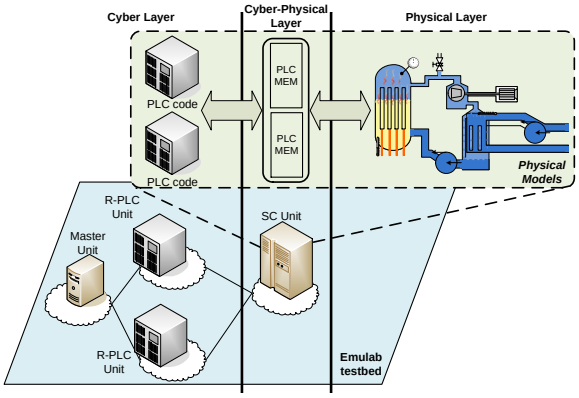

Fig. 2: Experimentation framework overview

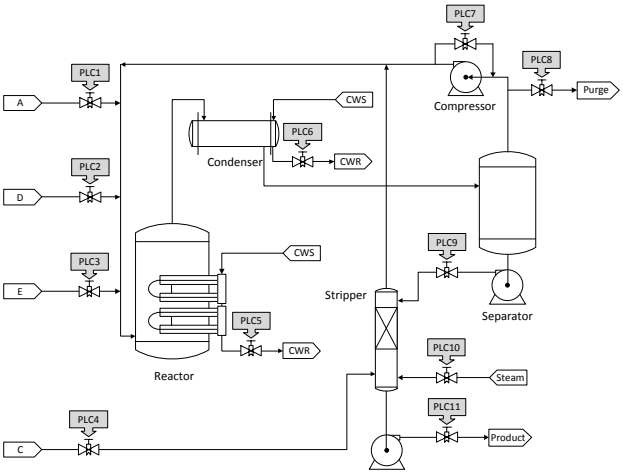

Fig. 3: Architecture of the Tennessee-Eastman process

is recreated by an emulation testbed that uses the Emulab architecture and software [13, 14] to automatically and dynamically map physical components (e.g. servers, switches) to a virtual topology. Besides the process network, the cyber layer also includes the control logic code that in the real world is run by PLCs. The control code can be run sequentially or in parallel to the physical model.

3.3 The Tennessee-Eastman Chemical Process

As pointed out by other authors as well [4, 17, 18], the complexity of the Tennessee-Eastman (TE) chemical process makes it suitable for a wide range of topics, such as process-wide control strategy, non-linear control or multivariable control. Recently, the TE process was also used in several security-related studies [19, 20], that add another important topic to the previous list.

The TE chemical plant is a process with 41 measured parameters and 12 manipulated variables. Out of the 12 variables throughout the literature we find control loops defined for 11 variables only, as for the last one (i.e. agitator speed control valve) it is not desirable to close the loop (McAvoy and Ye [17]). We briefly describe the process architecture and PLCs in Fig. 3.

3.4 Adversary Model and Attack Scenarios

The conducted experiment included a powerful adversary model and the TE industrial process . The main goal of the adversary was to cause the process parameters to reach their shut down limits (SDLs). As pointed out by Cárdenas, *et al.* [19] attacks targeting the minimum/maximum value of parameters/control variables are the ones that can damage the process in relatively short time periods. Such attacks cause the accumulation of products (e.g. steam, water, fuel) by completely opening valves (feed-valves) that feed products into process units and completely closing valves (free-valves) that free products from the process units. In both our models the adversary followed the same procedure to force the industrial process to shut down. More specifically, based on the documentation provided by Downs and Vogel [4] we identified the feed-valves and free-valves of the TE process and we employed OPEN commands for PLCs controlling feed-valves and CLOSE commands for PLCs controlling free-valves.

3.5 Experiment Implementation

The experiments were implemented in the Joint Research Centre's (JRC) Experimental Platform for Internet Contingencies (EPIC) laboratory. The Emulab testbed included nodes with the following configuration: FreeBSD OS 8, AMD Athlon Dual Core CPU at 2.3GHz and 4GB of RAM.

4 Experimental Results

We start our presentation with the normal operation of the TE process. Then, we move on to the results from the attack scenario described in the previous section.

4.1 Normal Operation of the Tennessee-Eastman Process

The operation of the TE process for 40h without any disturbances is shown in Fig. 4, where the target set-points are

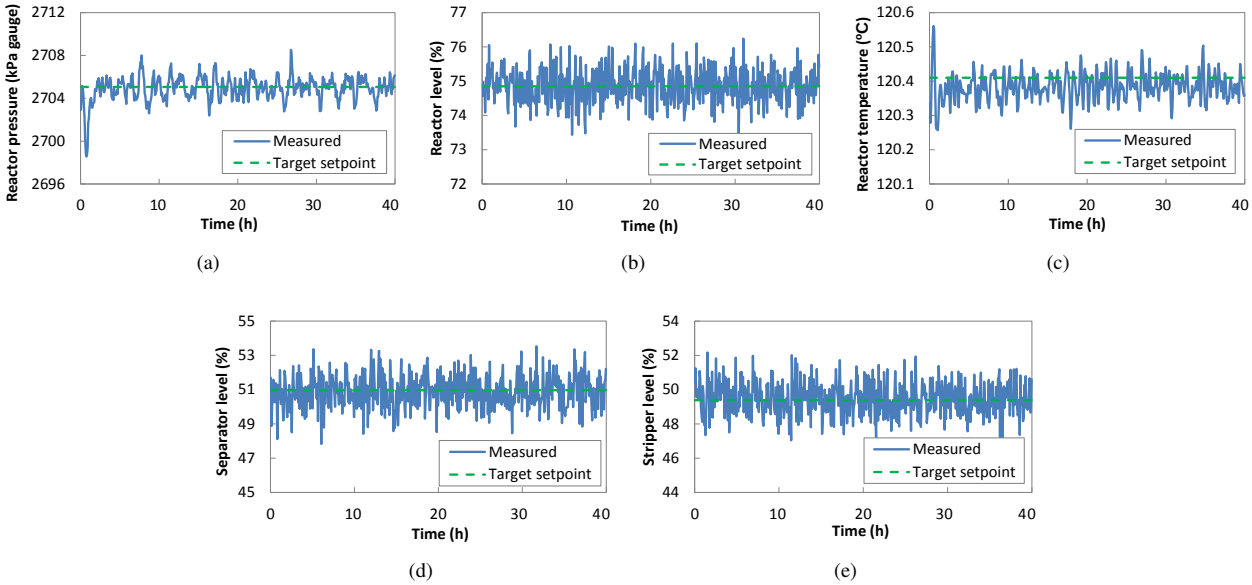

Fig. 4: Normal operation of the Tennessee-Eastman process for 40h without any disturbances: *Reactor* pressure (a), *Reactor* level (b), *Reactor* temperature (c), *Separator* level (d), and *Stripper* level (e).

illustrated with a dashed line. With the implemented control loops the process is able to run in a steady-state, as shown by the five sub-figures depicting the behavior of the parameters that could trigger a shut down of the process. Without these control loops, process parameters would reach their shut down limits (SDLs) after approximately 3.6h [5].

4.2 Effect of Network Delays

Next, we measured the effect of network delays on the process SDT. For the full network setting, the effect of delays is insignificant, as up to 0.5s the SDT does not show any changes. On the other hand, for network delays of 1s the value of the SDT increased to 4.83min, while for delays of 3s the SDT increased to 5.51min. However, such extreme delays can rarely be measured over the Internet, and even in such cases the impact on the attack is minimal. The effect of network delays on the cyber attack targeting the TE process is shown in Figure 5.

4.3 Effect of Packet Losses

In the next step we analyzed the effect of packet losses. Packet loss rates of 5% increased the SDT of the full network setting to 5.16min. However, extreme packet losses of 10% had an insignificant effect on the SDT and increased it to only 5.58min in the same setting. Similarly to the study of network delays, we can conclude that significant effects are measured only for extreme packet losses that can rarely be found in real settings. The effect of packet losses on the cyber attack targeting the TE process is shown in Figure 6

4.4 Effect of Background Traffic

Finally, we analyzed the effect of background traffic. In this case the increase in the background traffic to 5Mbit/s did not produce significant changes in most of the implemented settings. However, by increasing the traffic to 10Mbit/s, i.e. the maximum capacity of the external network, the SDT showed major changes. Starting with the full network setting, the SDT increased to almost twice its initial value, i.e. 7.91min. Such change is mainly caused by the excessive background traffic that lead to network congestions and finally to packet losses and additional delays. The behavior of the TE process for the two background traffic parameters was illustrated in Fig. 7.

4.5 Discussion

The main goal of this study was not to be exhaustive in the choice of network parameters, but to show that these might play an important role in the outcome of cyber attacks, given that specific conditions are met. The results from this section showed that the studied parameters have a significant effect on the outcome of cyber attacks only in case of extreme network conditions.

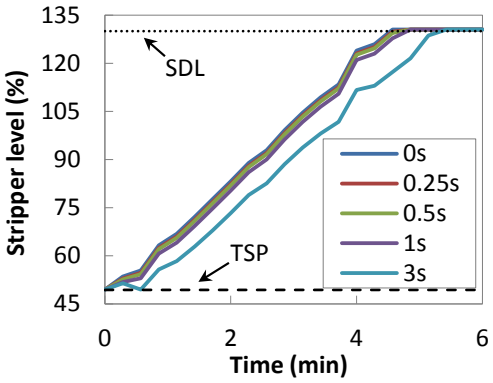

Fig. 5: Effect of network delays on the cyber attack and the operation of the Tennessee-Eastman process (SDL- Shut Down Limit, TSP - Target SetPoint)

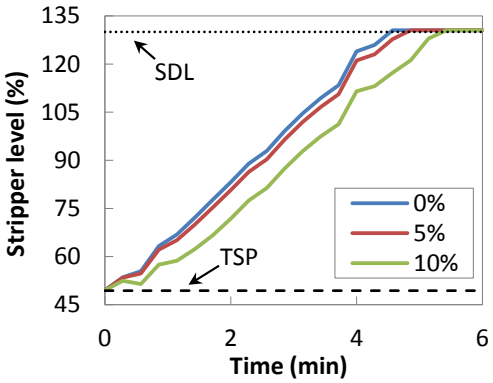

Fig. 6: Effect of packet losses on the cyber attack and the operation of the Tennessee-Eastman process (SDL- Shut Down Limit, TSP - Target SetPoint)

Throughout our study we found that network delays have the least effect on cyber attacks. This is mainly because packets are not lost, but only delayed and at the end are able to reach their target. On the other hand, the effect of packet losses is more obvious and in extreme cases can even double the value of the SDT. The main cause of this is that packet losses lead to major delays caused by timeouts in the transport layer. It is a well-known fact that network timeouts cause the retransmission of packets, which might occur more than once for each loosed packet. However, out of the three communications-related parameters, the most significant effect was recorded for network congestions. These were caused by a background traffic equal to the network capacity. In some cases this setting increased the value of the SDT by three or even four times. Nevertheless, such highly congestioned networks can rarely be found in practice and even so, the adversary could launch the attack from several locations in order to ensure the successful outcome of the attack.

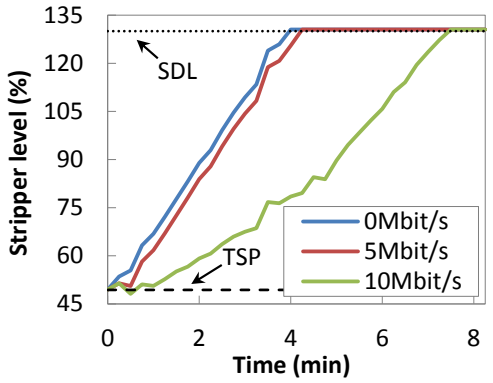

Fig. 7: Effect of background traffic on the cyber attack and the operation of the Tennessee-Eastman process (SDL- Shut Down Limit, TSP - Target SetPoint)

5 Conclusions

The study conducted in this paper employed an experimental approach to show that network communication parameters have a significant effect on the outcome of cyber attacks targeting CIs only in extreme cases. The studied parameters illustrated that communications-related parameters such as network delays, packet losses and background traffic can cause a significant impact only in case of extreme values that are rarely measured in practice. Nevertheless, it is also worth mentioning that if the attack is extremely time-dependent than even moderate changes in the network traffic can affect the cyber attack. As future work we intend to investigate other network parameters and develop novel countermeasure or techniques for designing more resilient CIs.

References

[1] S. East, J. Butts, M. Papa, and S. Shenoi, "A taxonomy of attacks on the dnp3 protocol," *IFIP Advances in Information and Communication Technology*, vol. 311, pp. 67–81, 2009.

[2] I. Nai Fovino, A. Carcano, M. Masera, and A. Trombetta, "An experimental investigation of malware attacks on scada systems," *International Journal of Critical Infrastructure Protection*, vol. 2, no. 4, pp. 139–145, 2009.

[3] N. Falliere, L. O. Murchu, and E. Chien, "W32.stuxnet dossier," 2010.

[4] J. Downs and E. Vogel, "A plant-wide industrial process control problem," *Computers & Chemical Engineering*, vol. 17, no. 3, pp. 245–255, 1993.

[5] J. Sozio, "Intelligent parameter adaptation for chemical processes," Master's thesis, Virginia Polytechnic Institute and State University, USA, 1999.

[6] Q. Zhu, D. Wei, and T. Başar, "Secure routing in smart grids," *Workshop on Foundations of Dependable and Secure Cyber-Physical Systems*, 2011.

[7] I. Nai Fovino, A. Carcano, M. Guglielmi, and M. Masera, "A k/n attack-resilient ict shield for scada systems," *Proc. of the First Workshop on Secure Control Systems*, 2010.

[8] D. Choi, S. Lee, D. Won, and S. Kim, "Efficient secure group communications for scada," *IEEE Trans. Power Delivery*, vol. 25, no. 2, pp. 714–722, 2010.

[9] O. Pal, S. Saiwan, P. Jain, Z. Saquib, and D. Patel, "Cryptographic key management for scada system: An architectural framework," *Proc. of International Conference on Advances in Computing, Control, & Telecommunication Technologies*, pp. 169–174, 2009.

[10] I. dos Anjos, A. Brito, and P. M. Pires, "A model for security management of scada systems," *Proc. of IEEE International Conference on Emerging Technologies and Factory Automation*, pp. 448–451, 2008.

[11] D. Germanus, A. Khelil, and N. Suri, "Increasing the resilience of critical scada systems using peer-to-peer overlays," *Proc. of the 1st International Symposium on Architecting Critical Systems, Lecture Notes in Computer Science*, vol. 6150, pp. 161–178, 2010.

[12] S. Avallone, S. D'Antonio, F. Oliviero, and S. Romano, "Use of traffic engineering techniques to increase resilience of scada networks," *Proc. of 5th International Conference on Critical Infrastructure*, pp. 1–7, 2010.

[13] B. White, J. Lepreau, L. Stoller, R. Ricci, S. Guruprasad, M. Newbold, M. Hibler, C. Barb, and A. Joglekar, "An integrated experimental environment for distributed systems and networks," *Proc. of the 5th Symposium on Operating Systems Design and Implementation*, pp. 255–270, 2002.

[14] C. Siaterlis, A. Garcia, and B. Genge, "On the use of emulab testbeds for scientifically rigorous experiments," *Communications Surveys Tutorials, IEEE*, vol. PP, no. 99, pp. 1 –14, 2012.

[15] B. Genge, C. Siaterlis, I. N. Fovino, and M. Masera, "A cyber-physical experimentation environment for the security analysis of networked industrial control systems," *Computers & Electrical Engineering*, vol. 38, no. 5, pp. 1146–1161, 2012.

[16] B. Genge, C. Siaterlis, and M. Hohenadel, "Impact of network infrastructure parameters to the effectiveness of cyber attacks against industrial control systems," *International Journal of Computers, Communications & Control*, vol. 7, no. 4, pp. 673–686, 2012.

[17] T. McAvoy and N. Ye, "Base control for the tennessee eastman problem," *Computers & Chemical Engineering*, vol. 18, no. 5, pp. 383–413, 1994.

[18] N. Ricker, "Model predictive control of a continuous, nonlinear, two-phase reactor," *Journal of Process Control*, vol. 3, pp. 109–123, 1993.

[19] A. Cárdenas, S. Amin, Z. Lin, Y. Huang, C.-Y. Huang, and S. Sastry, "Attacks against process control systems: Risk assessment, detection, and response," *Proc. of the 6th ACM Symposium on Information, Computer and Communications Security*, pp. 355–366, 2011.

[20] R. Chabukswar, B. Sinopoli, B. Karsai, A. Giani, H. Neema, and A. Davis, "Simulation of network attacks on scada systems," *1st Workshop on Secure Control Systems, Cyber Physical Systems Week*, 2010.