A Mixed-Interaction Critical Infrastructure Honeypot

Marc-Oliver Pahl*, Alexandre Kabil*, Edwin Bourget*, Matthieu Gay†, Paul-Emmanuel Brun†
*IMT Atlantique/ Chaire Cybersecurity for Critical Networked Infrastructures (Cyber CNI), † Airbus CyberSecurity
firstname.lastname@{*imt-atlantique.fr, †airbus.com}

***Abstract*—Operational Technology (OT) plays an essential role in modern societies. It is pivotal for applications such as water or power supply, healthcare, or transportation. At the same time, OT is often connected to the Internet for enabling remote-control and collaboration. Its societal impact makes OT an attractive attack target. Its connectivity to the Internet significantly increases the attack probability.**

For protecting against attacks, it is important to identify and study them. Honeypots enable such studies. However, realistic honeypots are difficult and expensive to setup. They are also inflexible as their setting is typically static.

In collaboration with Airbus Cybersecurity, the chaire Cyber CNI currently develops a mixed-interaction honeypot for critical infrastructures. The targeted setup combines physical and virtualized elements that can flexibly be reconfigured. This allows running diverse settings distributed in time or space. The virtualized part allows scaling the experiments. The goal of the Cyber CNI honeypot is enabling the closer study of Information and Operational Technology (IT & OT).

***Index Terms*—honeypot, OT, IT, CPS, high-interaction, cyber-range, testbed, pilot**

I. Introduction

Operational Technology (OT) plays an essential role in modern societies. Networked sensors and actuators drive central processes in our infrastructures and industries, such as water or power supply, healthcare, or transportation [1].

At the same time, OT is often indirectly connected to the Internet for enabling remote-control and collaboration. All kinds of entities that surround us can be remotely accessed including connected cars, factory automation robots, water pumps, smart grid substations, or buses and private cars for transportation. One of the most prominent industrial paradigms of the past years, industry 4.0, is about digitization and collaboration of manufacturing processes through connectivity [2].

Its societal impact makes OT an attractive attack target. Its heterogeneity creates an increased attack vector. Its connectivity to the Internet significantly increases the attack probability. Connectivity to the Internet results in a high number of potential attackers that can hack from their homes. Attacking critical infrastructures promises revenues such as visibility, the potential of creating physical damage, creating expensive damage, and blackmailing. Consequently, protecting networked distributed infrastructures is important to protect our society [3].

For protecting against attacks, it is important to identify and study them [3]. Honeypots enable such studies [4]. In industrial settings, honeypots are designed to lure attackers targeting industrial equipment such as Programmable Logic Controllers (PLC) or Supervisory Control And Data Acquisition (SCADA) systems. However, realistic honeypots are difficult and expensive to setup. They are also inflexible as their setting is typically static.

In collaboration with Airbus Cybersecurity, the Chaire Cyber CNI currently develops a mixed-interaction honeypot for critical infrastructures. The targeted setup combines physical and virtualized elements that can flexibly be reconfigured, in order to face issues related to existing honeypots. This allows running diverse settings distributed in time or space, on physical or virtual fields. The physical parts offer real, fully-functional interaction. The virtual part is fully-flexible in emulated devices and configurations. It provides scalability and better control over the interactions. The goal of the Cyber CNI honeypot is enabling the closer study of real attacks on Information and Operational Technology (IT & OT).

Section II introduces typical industrial honeypots that can be found in the field today. Section III presents the Cyber CNI testbed and honeypot.

II. Related Work

Even though the literature is quite extensive concerning honeypots in a general way, the specific field of industrial honeypots is promising albeit fairly recent. A search for "Industrial honeypots" on the Web of Science database returns 34 results, with 22 being very recently published since 2018. The following are the most relevant representatives for this work.

HosTaGe ICS Honeypot is an adaptation of the HosTaGe honeypot as Industrial Control System (ICS). The honeypot was originally designed for mobile devices security. HosTaGe is a low-interaction honeypot that emulates several standard industrial protocols such as Modbus or S7. Different to our approach, HosTaGe does not contain a physical part.

Antonioli et al. [5] propose a high-interaction ICS honeypot that simulated the Secure Water Treatment (SWaT) [6] industrial testbed. The honeypot is completely virtualized.

CamouflageNet [7] is an industrial honeypot. It is fully virtual but aims for high-interaction clones of physical devices.

IoTPOT [8] is a honeypot focused on Telnet attacks on Internet Of Things (IoT) devices. Since the IoT and ICS share common characteristics including telnet access, this work is also relevant.

GridPot [9] is an open source tool that simulates electricity grids. It has not been updated since its creation in 2015. It has however been used in commercial solutions such as Q-GridPot [10].

Q-GridPot is an appliance that comes with two honeypots, GridPot and Conpot, and several analysis tools. Conpot is a low-interaction server-side ICS honeypot. Like the other honeypots, it benefits from standardized interaction protocols, in case of the smart grid IEC 61850. It targets simple deployment, modification, and extension. Q-GridPot is a hardware developed by the HoneyNet Project to run honeypods such as Gridpot or Conpot.

The SCADA HoneyNet Project [11] is a software-based framework to simulate a variety of industrial networks such as SCADA, Distributed Control System (DCS), and PLC architectures. It is actively maintained since 1999.

GasPot is another industrial honeypot [12] that simulates a Veeder Root Guardian AST, consisting of a tank gauge. Created in 2015 by Trend Micro, it is not updated since 2016 [13]. When deployed in different countries, GasPot allows identifying hackers with links to the Iranian and the Syrian Electronic Army.

All presented honeypots use a simulated virtualized versions of the industrial hardware. They provide different forms of interaction. In contrast, this paper proposes the hybrid use of physical and virtual components. This results in a real setting and scalability with flexible reconfiguration possibilities, resulting in more flexibility and realism.

The closest related work is [14]. The authors ran a production honeypot for over a year.

III. The Cyber CNI Honeypot

The Cyber CNI mixed-interaction honeypot consists of eight parts as shown in fig. 1:

1) Section III-A Field Devices: This part consists of the actual managed hardware such as conveyor belts, robot arms, camera, or thermometers.
2) Section III-B Programmable Logic Controllers (PLCs): The controllers locally manage the operation of the field devices.
3) Section III-C Connectivity: The distributed components are connected over a physical or virtualized network.
4) Section III-D Management: High-level management logic of the components, e.g. SCADA.
5) Section III-E Visualization: A mixed reality interface gives intuitive access to the current state of the testbed as well as to the measured data.
6) Section III-F Honeypot Interface: This is the connection to the Internet.
7) Section III-G Measurement Infrastructure: This part contains all functionality for collecting and analysing the measured data.
8) Section III-H Testbed Management: Functionality to configure the testbed, manage user, data, and much more related to the experimentation.

It is implemented as a mix of physical components (section III-A-section III-C) and virtualized components (section III-I). It provides innovative user interfaces (section III-E), and automation for obtaining, collecting, and evaluating data (section III-G), as well as managing the testbed itself (section III-H). Finally, as honeypot it is obviously connected to the Internet (section III-F).

A. Field Devices

The Operational Technologies (OT) parts of the testbed comprise different *physical components*. The central platforms are Fischertechnik Industry 4.0 miniature factories [15].

Using miniaturized components saves costs, and mitigates potential safety-impacts on the platform without making concessions on its representativeness of a real-life industrial system, which is essential for a honeypot. As fig. 2 shows, they consist of miniaturized sensors and actuators. That makes the emulation especially interesting for our honeypot is that the miniaturized factory is controlled by industrial PLCs. Consequently, it is indistinguishable from a full-size factory under remote-control.

The physical industrial processes that are currently implemented are the *Fischertechnik Industry 4.0 setup* [15] and another factory setup created for a hackathon in the past [16]. Depending on the identified use cases, other physical settings might be added to the honeypot. Several physical copies of the platform exist so that the resources can be allocated to several scenarios or research projects at the same time. Different configurations can be anticipated such as using all of the platforms at the same time for load balancing or having a production platform for data generation while other research platforms are being modified and tested.

In addition, full-size hardware including Siemens motors, pumps, valves, and Schneider heating circuits can be connected to the honeypot for extending the settings.

Complementing to the physical entities, different *virtualized* entities exist. Multiple Diateam factory simulations that are again controlled by PLCs become part of the platform. Due to the PLC control, those are again different to distinguish from real hardware.

Finally, the Airbus CyberRange (section III-I) enables simulating a variety of hardware. The simulation has the advantage that it can be reconfigured and measured easily. By simulating components on all presented layers, the virtualized part of the Cyber CNI testbed becomes highly realistic.

B. Programmable Logic Controllers (PLCs)

The hardware components from section III-A connect to so-called Programmable Logic Controllers (PLCs). The PLCs run local control workflows and can be remotely configured. For representing different settings, and for evaluating differences, the Cyber CNI testbed contains different PLCs from the vendors Crouzet, IndustrialShield, Siemens (see fig. 3), and Schneider.

The miniaturised factory has been divided into three subsystems each controlled by one PLC. The PLC models are interchangeable and communicate with each other and the SCADA

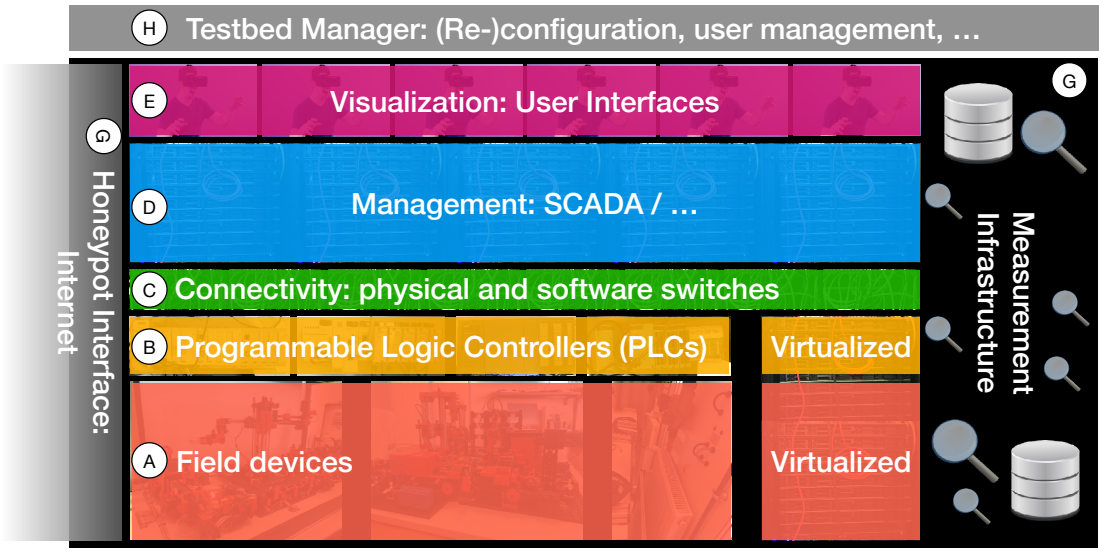

Fig. 1. The Cyber CNI Honeypot Architecture.

through OLE for Process Control Unified Architecture (OPC UA). OPC UA provides the interoperability layer that enables the higher-level SCADA processes to seamlessly interact with PLCs from different vendors.

Despite the interface compatibility, the PLCs have to be programmed in different languages. It will be interesting to see if different attacks specialize on certain controllers.

Again, in the CyberRange PLC functionality is virtualizes to introduce additional scale for realism and attack potential.

C. Connectivity

The different PLCs get interconnected via managed switches. They allow reconfiguring topologies according to the test scenarios. In addition, they allow traffic inspection.

In addition, virtual switches connect the virtualized system parts. Finally, software defined switches (SDN) may become an interesting attack target in the future.

D. Management

For high-level management of the industrial processes including their interplay, so called Supervisory control and data acquisition (SCADA) comes into play. In the testbed, anything above and starting from the SCADA is virtualized, running in software on the CyberRange.

As detailed before, this brings great flexibility in terms of reconfigurability, introspection, and scale. It also enables the intended inclusion of co-simulation by replaying communication traffic, and by instantiating different settings. Via the Cyber CNI testbed manager the whole infrastructure can be reconfigured in software, enabling time-sharing by running different settings at different times, and space sharing by running different settings in parallel on different platform parts.

The plan is also to include new management paradigms such as information-centric component management [17]. It will be interesting to see, if such architectures will also be attacked. Overall, we expect them to increase the reliability of our infrastructures under attack.

E. Visualization

Having a hybrid physical/virtual testbed brings opportunities but also another layer of complexity, due to the interconnectivity of its parts. Visualization is therefore central as observing what happens in the honeypot is the goal. Therefore, the Chaire will extend its Augmented Reality interface activities to include the Cyber CNI testbed.

Using 3D headsets, multiple interfaces and dashboards that help monitoring and controlling different aspects of the platform will be provided. A special focus will be on Mixed Reality (MR) interfaces for displaying information on the real hardware [18].

Operators will be able to access contextual information and interactions according to their needs, devices and tasks. MR Interfaces offer communication and cooperation capabilities that allow users to exchange information into one application, limiting the tool pivoting tasks that are time consuming and complex to manage. Three-dimensional visualizations promise new insights.

Virtual Reality (VR) interfaces allow immersing users into environments. In the described testbed, virtual machines, network topology and real-time data regarding several aspects of the honeypot could be represented in a more intuitive way [19].

Developing 3D interfaces is more difficult than providing 2D dashboards, but it can increase the User Experience (UX) and in the long term could be beneficial, as all developments are made in one platform for several devices. They are particularly useful for monitoring and control of Cyber-Physical Systems (CPS) [20], as they can provide adapted interfaces for specific supports.

Mixed-Reality interfaces are relatively new. Compared to traditional 2D Visual Analytics tools [21] they promise over-

coming limitations such as screen space, lack of natural interactivity, and collaboration issues. This will be part of our research [22], [23].

Augmented Reality (AR) devices as the Microsoft Hololens headset or even classical tablets or smartphones will help monitoring the physical testbed status when being physically close to it. Proposing contextual information that will float above the testbed will be useful to understand specific issues or events which are tied to a specific hardware parts [24].

The planned works will be based on the Unity or Unreal Game Engines. The same environment will be used to monitor and control our platform. The interfaces will be adaptive to users and devices. For example, a user that will have to interact with the physical testbed will use a mobile or an AR interface, whereas a user who needs to visualize the whole network topology will use a VR one. Both of these interfaces will concern the same environment, and several users will be able to collaborate even if they are using different devices.

F. Honeypot Interface

To attract real attackers, the entire Cyber CNI testbed will be connected to the Internet. Different address ranges and country locations will be used for establishing an interesting attack surface. Separate networks will be used for this activity, not to endanger the regular operation of the IMT Atlantique.

G. Measurement Infrastructure

Since observation is key in a honeypot, measuring interactions and activities is also key. The Cyber CNI testbed will have probes on all layers. This includes obvious network interactions from the outgoing interfaces, over all local physical and virtualized networking traffic, down to the physical signals exchanged with the field devices. In addition, out-of band sensors such as cameras, microphones, and current meters will allow supervising the processes and detecting anomalies.

Processes for collecting, managing, and analyzing the data obtained will be provided in this layer. Machine-learning will play an important role to analyze and filter data. Semantics will play a central role here [25]. In addition, the testbed will be used to test own security mechanisms such as [26].

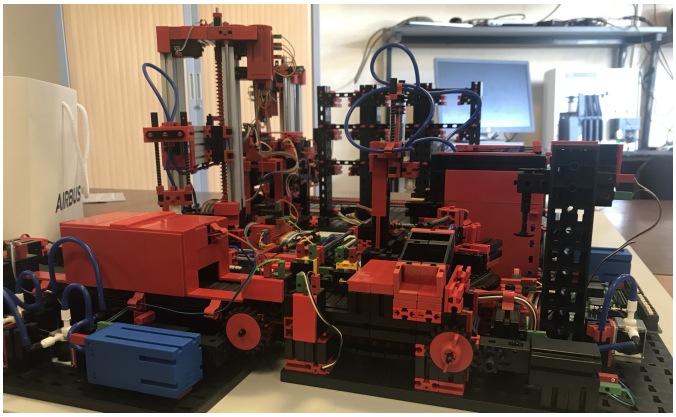

Fig. 2. Fischertechnik Industry 4.0 factory emulation.

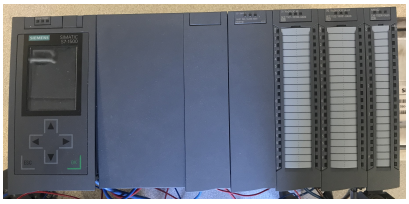

Fig. 3. Siemens SIMATIC S7-1500 PLC.

A goal is to make obtained data sets available to external researchers to reproduce our research, and to conduct additional research.

H. Testbed Manager

A central property of the Cyber CNI testbed is its reconfigurability. The testbed will run different setups distributed over space and time. Space sharing is possible due to the large extent of the platform. Different parts can be used for different honeypots at the same time. Time sharing is possible by running different configurations at different times.

The testbed manager takes care of the configurations, users, and also the data collection and access through those running the experiments. The current aim is opening the infrastructure also for experiments by externals. The testbed manager will be central for this as well.

Configurations will be stored as files. They will comprise everything from field devices over PLCS and connectivity to the SCADA processes, and the network interfaces.

Especially the security configurations will be interesting. A special focus will be on implementing state of the art security implementations such as those from ANSSI [27]–[29] or NIST [30]. Depending on the intended observations, they will only be partially implemented in certain configurations. In addition, research security mechanisms such as [31]–[34] will be deployed to observe their effect on the attack potential.

The testbed manager interface will allow calling configurations based on schedules. The previously described systems enable reinitializing them completely. This includes programming the PLCs. Consequently, the Cyber CNI testbed can be reconfigured, enabling reproducible experiments and honeypot settings.

A goal is to provide configurations for relevant standardized settings such as

- the Secure Water Treatment (SWAT) of Singapore University of Technology and Design (SUTD) [6]
- EPIC [35]
- Gugliemi [36]
- DETER project [37]

More interesting testbeds can be found in [38]. These settings will be interesting as they allow reproducing research experiments. This might be of interest for attackers as well since the settings were created for good reasons, often to correspond attacks.

For the Cyber CNI testbed real industrial settings will be especially interesting. The IT and OT scenarios will therefore

be developed with the partners of the Chaire Cyber CNI, Airbus, Amossys, BNP Paribas, EDF, and Nokia. In addition, other companies will be contacted and are invited to contact us, e.g. via the Ple d'Excellence Cyber (PEC).

I. Airbus CyberRange

The virtualized part of the Cyber CNI testbed is implemented in strong collaboration with Airbus Cybersecurity. An Airbus CyberRange physical platform is currently used. If required, it can be extended with a cloud instance.

The Airbus CyberRange is an advanced simulation platform that can be used to model IT / OT systems composed of tens or hundreds of machines and play realistic scenarios including real cyber-attacks. The platform manages several environments, isolated ones from the others, as well as from the legacy IT / OT from the organization.

By means of these capabilities, users can immerse themselves in an environment customized to look like their system in operation. This support several use cases including operational qualification, testing, and training. For the hardware, the tool exists in 2 main forms:

- Physical platform: High performance servers stored in a mobile box, on site, switches, hosting VMware, vSphere Infrastructure.
- Cloud Platform: the CyberRange platform is also available in the Cloud, allowing a flexible and multisite collaborative experience.

In the CyberCNI testbed both could be used. The physical platform will be used for sure.

On top of that, Airbus CyberSecurity has developed a software LADE: set of web and micro services simplifying the deployment of virtualized infrastructures, running cyber-attacks, tests and scenarios. LADE allows hybrid infrastructure management. This management software significantly reduces the delay between designing the simulation and having it deployed.

Regarding the hardware, the CyberRange uses high efficiency servers to host and run one or more virtualized networks with thousands of Virtual Machines and Containers. By default, the platform provides 16 working environments (named workzones), each workzone offers a capacity of 25 VMs and 100 containers. thus, offering a potential virtualisation, combined of 400 VMware and 1600 Dockers. The division in 16 workzones is configurable and it is possible to limit the number of workzones to maximize the capacity of a workzone.

In terms of scalability, the CyberRange platform can be scaled up at different levels: Network Servers VMware - LADE It is possible to add switches to be able to interconnect more than 24 physical devices. At a switch level, the concept of stack can be used, allowing administration at the same time. Network capacity expansion requires switches that can address VLANs greater than 1024 as well as switches that can declare a large number of VLANs (for example 4096). It is possible to add several servers running the VMware ESXi operating system in the VMware Cluster. LADE software acts at the cluster level, which means that the number of servers underlying the cluster is completely transparent meaning that the limits of the software LADE are those of VMware.

In addition, physical equipment can be connected to the physical platform making a hybrid platform through the ports of the switch and integrated into a virtualized network hosted on CyberRange. The CyberRange comes with a switch in order:

- To connect physical equipment, IT or OT
- To connect hardware traffic generators
- To be inter-connected with other existing platforms or systems
- To be inter-connected with storage systems
- To accept connections of remote maintenance and remote access in web mode
- To inter-connect several CyberRange environments together

In some use-cases, it is necessary or simpler to be able to access the different tools available in the CyberRange. Using cloud services, Airbus CyberSecurity has developed the features to have CyberRange as SaaS.

Regarding the simulation capabilities, the CyberRange enables virtualization of complex networks including (most of them come out of the box):

- Operating Systems (OS): Debian, CentOS, Ubuntu, Windows, etc.
- Servers: Windows Server, File sharing (FTP), Web Servers (apache, nginx), Databases (MariaDB, Postgres), etc.
- Security equipment: firewall, Intrusion Detection System (IDS), etc.
- Sub-networkzones: DMZ, User LAN, etc.
- Network architectures: Virtual switch, Virtual routers, VLAN, AS, BGP, OSPF, RIP VRRP, Network operators, Backbone, etc…

From the software perspective, the network frames are managed by the virtual component of VMware by a VMware Distributed Virtual Switch (DVS). This component creates virtual networks associated with a VLAN number, and from which the virtual machines are connected. LADE ensures storage consumption limits both per group of users and per workzone. VMware ensures computing limits (CPU usage, RAM usage). Those limits guarantee dedicated performances in all workzones. Resource limitation mechanisms are customizable in VMware for virtual machines and in LADE for Docker containers. LADE has a library of architectures, limited by the allocated disk space.

Extending this space is easy by connecting the platform with external storage systems such as a NAS. In addition to computing capacity, each workzone can have up to 32 networks, completely independent and isolated from the other spaces using VLANs. Deploying a virtual machine or container is done by drag-and-drop to the workspace. The user can change the configuration settings before creating the component in his workspace.

The creation of Networks is carried out via a Drag-And-Drop mechanism by selecting a component from the Network section. The control panel proposes to set the network addressing the default gateway for all the machines that connect to it. Once deployed, the context menu allows the removal or the configuration of the selected network such as the network description, name, address and the default gateway.

To connect a host to the network, simply click on it, then click on the network to which you want to connect it. A control panel opens to define the network settings. In the same way, a user can modify or delete the network connection of a machine via the context menu.

The CyberRange offers the possibility to register an External Host. This feature enables the user to connect a physical device to the switch of the CyberRange and configure the host directly from LADE.

In the LADE, a user can perform group of actions on machines, such as backing up part of the infrastructure as a topology. Once built, the user can select all or part of the system to save it as a new component. It is then directly inserted into the library and can be reused at will, either in the same workzone or in a different workzone.

The copy becomes accessible by simple drag-and-drop. It is possible to modify and save this component again, while keeping the previous version. This makes it possible to obtain several versions of the component, and to use the one that is most appropriate when needed. Once the topology is saved, it appears in the Topologies section of the navigation panel. This feature offers the possibility to test different configurations and to redeploy a whole topology (or a part of it) in case of misconfiguration or to restore a complete infrastructure after a cyber-attack.

By default, each workzone is isolated from the others but it is possible to route the traffic between them. Regarding data collection and supervision, this possibility could be used to deploy a SOC in a workzone to supervise another one. In that case, all the traffic can be monitored and event logs of each VM can be collected to follow the activity of a workzone.

To make the simulation more real, the software LADE offers the possibility to run traffic generators on a virtualized topology. The CyberRange platform integrates a set of network traffic generators able to generate random flows and reproduce traffic recorded in virtualized infrastructure. Execution conditions of the traffic generators (source, destination, frequency) can be set by the user. The administrator can add/modify traffic generators from the administration interface. They can also export/import generators to make them available to users.

The CyberRange platform offers the possibility to replay recorded traffic in virtual infrastructures, via LADE interface, in the same way as the other items of the catalog (network and life traffic, attacks, etc.). During the execution of the generator, the user can view the operations performed by the traffic generator.

IV. Conclusion

Honeypots allow observing and investigating real attacks. Such observations can significantly help understanding weaknesses of a system. This paper described the Cyber CNI testbed that acts as a mixed-interaction honeypot. The testbed combines physical and virtualized components.

The honeypot is called mixed-interaction as it is reconfigurable and therefore allows different levels of honeypot interaction, from low-level interaction through replay to high-interaction virtualized and real interaction. The physical parts of the honeypot allow full interaction. The virtualized parts can offer different interaction levels. The chosen approach with simulating the entire processing chain can offer full-interaction.

While the physical components comprise Fischertechnik, heater, or motors that are managed via industrial PLCs, the Airbus CyberRange allows a wide range of virtualized experimentation. This adds high flexibility and scalability for configuring different settings.

After motivating the approach (section I) and existing testbeds (section II), the testbed and honeypot architecture were introduced in detail in section III. Highlights were:

- the real settings with minituarized components that enable full observation of effects of attacks (section III-A)
- innovative ways of visualizing and analyzing data with 3D interfaces (section III-A)
- full monitoring and automation via the measurement infrastructure (section III-G) and testbed manager (section III-H)
- full reconfigurability for diverse settings enabling relevant experimentation in space and time sharing (section III-H)

The proposed honeypot is to the best of our knowledge unique in its flexibility and reconfigurability. It promises gaining highly-relevant insights on current cyber-attacks. These insights promise being helpful for protecting real (critical) infrastructures. In addition, they promise enabling better research for making future IT and OT systems more secure.

We are looking forward to collaborating with companies and researchers all over the globe on this big endeavor.

References

[1] I. F. Mikhalevich and V. A. Trapeznikov, "Critical Infrastructure Security: Alignment of Views," *2019 Systems of Signals Generating and Processing in the Field of on Board Communications, SOSG 2019*, 2019.

[2] E. Oztemel and S. Gursev, "Literature review of Industry 4.0 and related technologies," *Journal of Intelligent Manufacturing*, vol. 31, no. 1, pp. 127–182, 2020. [Online]. Available: https://doi.org/10.1007/s10845-018-1433-8

[3] S. W. Smith, "Securing the Internet of Things: An Ongoing Challenge," *Computer*, vol. 53, no. 6, pp. 62–66, 2020.

[4] I. Barak, "Critical infrastructure under attack: lessons from a honeypot," *Network Security*, vol. 2020, no. 9, pp. 16–17, 2020.

[5] D. Antonioli, A. Agrawal, and N. O. Tippenhauer, "Towards high-interaction virtual ICS honeypots-in-a-box," in *CPS-SPC 2016 - Proceedings of the 2nd ACM Workshop on Cyber-Physical Systems Security and PrivaCy, co-located with CCS 2016*. Association for Computing Machinery, Inc, oct 2016, pp. 13–22.

[6] "Secure Water Treatment - iTrust." [Online]. Available: https://itrust.sutd.edu.sg/testbeds/secure-water-treatment-swat/

[7] H. Naruoka, M. Matsuta, W. Machii, T. Aoyama, M. Koike, I. Koshijima, and Y. Hashimoto, "Ics honeypot system (camouflagenet) based on attacker's human factors," *Procedia Manufacturing*, vol. 3, pp. 1074 – 1081, 2015, 6th International Conference on Applied Human Factors and Ergonomics (AHFE 2015) and the Affiliated Conferences, AHFE 2015. [Online]. Available: http://www.sciencedirect.com/science/article/pii/S2351978915001766

[8] Y. M. P. Pa, S. Suzuki, K. Yoshioka, T. Matsumoto, T. Kasama, and C. Rossow, "Iotpot: Analysing the rise of iot compromises," in *9th USENIX Workshop on Offensive Technologies (WOOT 15)*. Washington, D.C.: USENIX Association, Aug. 2015. [Online]. Available: https://www.usenix.org/conference/woot15/workshop-program/presentation/pa

[9] "GitHub - sk4ld/gridpot: Open source tools for realistic-behaving electric grid honeynets." [Online]. Available: https://github.com/sk4ld/gridpot

[10] "Q Gridpot Quantalytics." [Online]. Available: https://www.quantalytics.com/q-gridpot/

[11] "The Honeynet Project Honeypot research." [Online]. Available: https://www.honeynet.org/

[12] "GitHub - sjhilt/GasPot: GasPot Released at Blackhat 2015." [Online]. Available: https://github.com/sjhilt/GasPot

[13] "The Gaspot Experiment: How Gas-Tank-Monitoring Systems Could Make Perfect Targets for Attackers - Security News - Trend Micro USA." [Online]. Available: https://www.trendmicro.com/vinfo/us/security/news/cybercrime-and-digital-threats/the-gaspot-experiment?utm_source=social&utm_medium=smk&utm_campaign=gaspot2015-11

[14] S. Hilt, F. Maggi, C. Perine, L. Remorin, M. Rösler, and R. Vosseler, "Caught in the Act : Running a Realistic Factory Honeypot to Capture Real Threats," pp. 1–63, 2020. [Online]. Available: https://www.trendmicro.com/vinfo/it/security/news/internet-of-things/fake-company-real-threats-logs-from-a-smart-factory-honeypot

[15] "Industry 4.0 / IoT - fischertechnik." [Online]. Available: https://www.fischertechnik.de/en/simulating/industry-4-0

[16] S. N. Foley, F. Autrel, E. Bourget, T. Clédel, S. Grunenwald, J. Rubio Hernan, A. Kabil, R. Larsen, V. M. Rooney, and K. Vanhulst, "Science hackathons for cyberphysical system security research: Putting cps testbed platforms to good use," in *Proceedings of the 2018 Workshop on Cyber-Physical Systems Security and PrivaCy*, 2018, pp. 102–107.

[17] M.-O. Pahl and S. Liebald, "Designing a Data-Centric Internet of Things: VSL," in *Int. Conference on Networked Systems (NetSys)*, 2019.

[18] R. Skarbez, N. F. Polys, J. T. Ogle, C. North, and D. A. Bowman, "Immersive Analytics: Theory and Research Agenda," *Frontiers in Robotics and AI*, vol. 6, p. 82, 2019.

[19] K. Kullman, J. Cowley, and N. Ben-Asher, "Enhancing cyber defense situational awareness using 3D visualizations," in *Proceedings of the 13th International Conference on Cyber Warfare and Security, ICCWS 2018*, vol. 2018-March, 2018, pp. 369–378.

[20] R. Seiger, M. Gohlke, M. Korzetz, and U. Aßmann, "Mixed reality cyber-physical systems control and workflow composition," in *ACM International Conference Proceeding Series*. Association for Computing Machinery, nov 2017, pp. 495–500.

[21] R. Damaševičius, J. Toldinas, A. Venčkauskas, Š. Grigalinas, N. Morkevičius, and V. Jukavičius, "Visual analytics for cyber security domain: State-of-the-art and challenges," in *Communications in Computer and Information Science*, vol. 1078 CCIS, 2019, pp. 256–270.

[22] A. Kabil, T. Duval, and N. Cuppens, "Alert characterization by non-expert users in a cybersecurity virtual environment: A usability study," in *Lecture Notes in Computer Science (including subseries Lecture Notes in Artificial Intelligence and Lecture Notes in Bioinformatics)*, vol. 12242 LNCS, 2020, pp. 82–101.

[23] K. Kaneko, Y. Tsutsumi, S. Sharma, and Y. Okada, "PACKUARIUM: Network Packet Visualization Using Mixed Reality for Detecting Bot IoT Device of DDoS Attack," in *Lecture Notes on Data Engineering and Communications Technologies*, 2020, vol. 47, pp. 361–372.

[24] S. Beitzel, J. Dykstra, P. Toliver, and J. Youzwak, "Network anomaly analysis using the Microsoft HoloLens," in *Proceedings of the Human Factors and Ergonomics Society*, vol. 3, no. 1, 2018, pp. 2094–2098.

[25] M.-O. Pahl and G. Carle, "Crowdsourced Context-Modeling as Key to Future Smart Spaces," in *Network Operations and Management Symposium 2014 (NOMS 2014)*, May 2014, pp. 1–8.

[26] M.-O. Pahl and F.-X. Aubet, "All Eyes on You: Distributed Multi-Dimensional IoT Microservice Anomaly Detection," in *2018 14th International Conference on Network and Service Management (CNSM) (CNSM 2018)*, Rome, Italy, Nov. 2018.

[27] "GUIDE ANSSI," Tech. Rep. [Online]. Available: https://www.ssi.gouv.fr/uploads/2019/06/anssi-guide-passerelle_internet_securisee-v3.pdf

[28] "Cas pratique d'un tunnel routier Partie 1 : classification," Tech. Rep. [Online]. Available: https://www.ssi.gouv.fr/uploads/2016/10/systeme-indus_cas-pratique_tunnel_partie1_anssi.pdf

[29] "Cas pratique d'un tunnel routier Partie 2 : mesures," Tech. Rep. [Online]. Available: https://www.ssi.gouv.fr/uploads/2016/10/systeme-indus_cas-pratique_tunnel_partie2_anssi.pdf

[30] K. Stouffer, V. Pillitteri, S. Lightman, M. Abrams, and A. Hahn, "Guide to Industrial Control Systems (ICS) Security," National Institute of Standards and Technology, Gaithersburg, MD, Tech. Rep., jun 2015. [Online]. Available: https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-82r2.pdf

[31] A. Piccoli, M.-O. Pahl, S. Fries, and T. Sel, "Ensuring consistency for asynchronous Group-Key management in the industrial IoT," in *International Conference on Network and Service Management (CNSM 2020) (CNSM 2020)*, Izmir, Turkey, Nov. 2020.

[32] N. Mühlbauer, E. Kirdan, M. Pahl, and G. Carle, "Open-source OPC UA security and scalability," in *25th IEEE International Conference on Emerging Technologies and Factory Automation, ETFA 2020, Vienna, Austria, September 8-11, 2020*. IEEE, 2020, pp. 262–269. [Online]. Available: https://doi.org/10.1109/ETFA46521.2020.9212091

[33] J. Seeger, A. Bröring, M. Pahl, and E. Sakic, "Rule-based translation of application-level qos constraints into SDN configurations for the iot," in *European Conference on Networks and Communications, EuCNC 2019, Valencia, Spain, June 18-21, 2019*. IEEE, 2019, pp. 432–437. [Online]. Available: https://doi.org/10.1109/EuCNC.2019.8802018

[34] M. Pahl and L. Donini, "Giving iot services an identity and changeable attributes," in *IFIP/IEEE International Symposium on Integrated Network Management, IM 2019, Washington, DC, USA, April 09-11, 2019*, J. Betser, C. J. Fung, A. Clemm, J. François, and S. Ata, Eds. IFIP, 2019, pp. 455–461. [Online]. Available: http://ieeexplore.ieee.org/document/8717910

[35] Y. Soupionis and T. Benoist, "Cyber-physical testbed - The impact of cyber attacks and the human factor," in *2015 10th International Conference for Internet Technology and Secured Transactions, ICITST 2015*. Institute of Electrical and Electronics Engineers Inc., feb 2016, pp. 326–331.

[36] M. Guglielmi, I. Nai, A. Perez-Garcia, and C. Siaterlis, "A preliminary study of a wireless Process Control Network using emulation testbeds," in *Lecture Notes of the Institute for Computer Sciences, Social-Informatics and Telecommunications Engineering*, vol. 45 LNICST. Springer, Berlin, Heidelberg, 2010, pp. 268–279. [Online]. Available: https://link.springer.com/chapter/10.1007/978-3-642-16644-0_24

[37] T. Benzel, "The science of cyber security experimentation: the DETER project," in *ACSAC '11: Proceedings of the 27th Annual Computer Security Applications Conference*, 2010. [Online]. Available: https://dl.acm.org/doi/10.1145/2076732.2076752

[38] H. Holm, M. Karresand, A. Vidström, and E. Westring, "A survey of industrial control system testbeds," in *Lecture Notes in Computer Science (including subseries Lecture Notes in Artificial Intelligence and Lecture Notes in Bioinformatics)*, vol. 9417. Springer Verlag, oct 2015, pp. 11–26. [Online]. Available: https://link.springer.com/chapter/10.1007/978-3-319-26502-5_2