Towards automation security research and training environment

Jari Seppälä, Mikko Salmenperä and Hannu Koivisto*
Tampere University of Technology, Department of Automation Science and Engineering,
P.O. Box 692, FI-33101 Tampere
Puh 040 767 4998*, firstname.lastname@tut.fi, http://www.tut.fi/ase/
Jarmo Harju
Tampere University of Technology, Department of Pervasive Computing, P.O. Box 533, FI-33101 Tampere
firstname.lastname@tut.fi
Sami Repo
Tampere University of Technology, Department of Electrical Engineering, P.O. Box 692, FI-33101 Tampere
firstname.lastname@tut.fi
John Holmström
Ajeco Oy, Arinatie 10, 00370 Helsinki
firstname.lastname@ajeco.fi
Pasi Ahonen
VTT Techical Research Centre Of Finland Ltd., P.O. Box 1000, FI-02044 VTT
firstname.lastname@vtt.fi

KEYWORDS Cyberlab, automation, information security, laboratory, cyber, security

ABSTRACT

An automation system is a networked software product in hardware intensive environment and requires more than normal IT security skills. Building an automation security research and training environment for automation requires knowledge on the internal workings of an automation system as well as creative approach on how to keep the system secure where needed, and broken when required for development and teaching purposes. The main challenges are to combine the amount of automation specific hardware and to create good practices which keep the need for maintenance, versatility and pedagogical aspects in balance. This paper presents a project called TUTCyberLabs, the learned lessons and the design decisions. The main focus is on Department of Automation Science and Engineering environment ASECyberLab.

1 INTRODUCTION

Cyberlab - everyone also in Finland is building one, but if everyone is building then how all of them can survive. A Cyberlab requires maintenance, updates, best practices and experts as do any laboratory environment, especially when the environment is related to security research and education. Cyberlabs that has been advertised in Finnish press are JYVSECTEC/RGCE in Jyväskylä [1], VTT Cyber War Room in Oulu [3] and Cybersecurity Learning Environment in Kymenlaakso University of Applied Sciences [4]. Why build another?

There is a clear need for co-operation in national level since there is not enough customer base in Finland to build commercially viable office-hour Cyberlab from research, teaching nor testing point of view. This challenged was acknowledged in Tampere University of Technology (TUT) already in early days of Cyber Hype in 2010. Therefore, the starting point for building a Cyberlab was selected as non-commercial day-to-day use of own organisation. "No rental" decision was made, all use is done in co-operation with participating departments.

The history of Cyberlab in Tampere University of Technology began from two different projects: networking laboratory at Department of Pervasive Computing (TIE) which has been running since 1996, and Control Systems Security Training course at Department of Automation Science and Engineering (ASE) started at 2010. The joint SmartGrid Security Research between ASE and Department of Electrical Engineering (DEE) in CLEEN SHOK project Smart Grids and Energy Market (SGEM 2010-2014) was the final spark for the idea of building TUT wide Cyberlab. The final enabler was The Finnish Academy which granted funding for *TUTCyberLabs - Research infrastructure for cyber security* in 2014 under the FIRI 2013 call for research infrastructures.

The joint environment of three departments inside TUT created the necessary skill set combining the deep knowledge required to build all the components required to tackle the modern critical infrastructure cybersecurity challenges. Department of Automation Science and Engineering's ASECyberLab contains various automation systems from batch processes to moving machines. Department of Electrical Engineering's

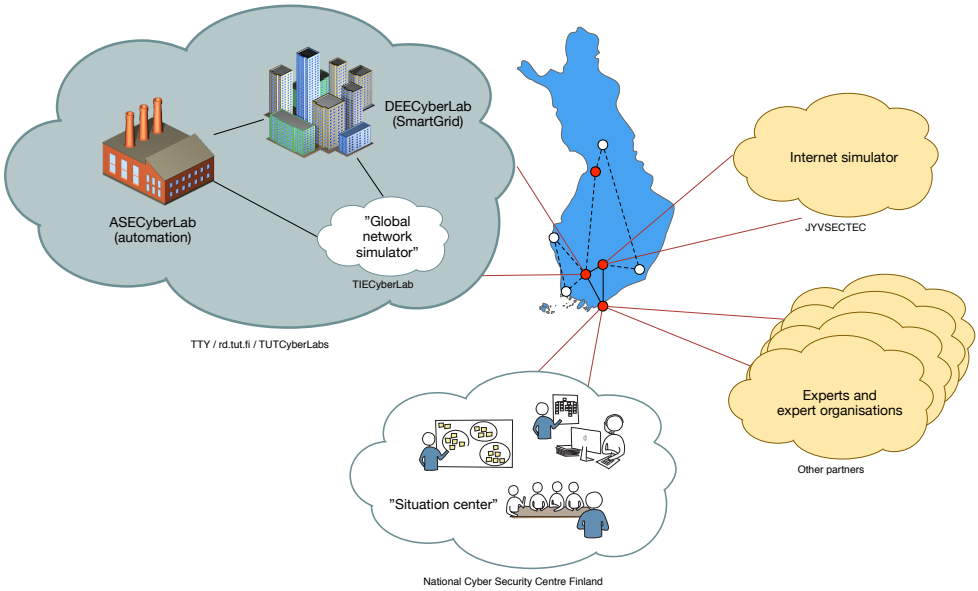

Figure 1: TUTCyberLabs and national co-operation.

DEECyberLab contains the Smart Grid infrastructure and consumer environments. Department of Pervasive Computing's TIECyberLab is the glue which binds all into TUTCyberLabs and provides the external connection point and practices during future national and international cyber security trainings as well as the office of our virtual city. The roles can be simplified as follows

- ASECyberLab - energy production, process automation, moving machines
- DEECyberLab - energy consumption, energy transfer, Smart Grids, energy storage
- TIECyberLab - network security, general IT infrastructure, office, co-operation solutions with external parties

The national co-operation can be summarised as work on progress. There exists tested and active remote solutions between research and commercial partners but much work is still needed to enable the vision in Figure 1. The challenge is not in technology but finding the first externally funded project where national collaboration is needed.

2 BUILDING A CYBERLAB

What is required from CyberLab? First of all, a CyberLab must work as integrated part of day-to-day operations. In Tampere University of Technology this means education and research. It must not contain heavy bureaucracy, nor should it require special organisation just to keep everything running. From this starting point TUTCyberLabs emerged and it was the first lesson from the project - keep the administrative overhead as minimal as possible.

Building a general cyberlab for security research is easy. Almost any kind of separate IT network segment and related software and hardware is sufficient since research environments are usually tuned around a specific research task. Building a cyberlab for security education is more challenging. Anything can happen during teaching. This is even more obvious when you are teaching students to break, or audit networked software systems. The inclusion of critical infrastructure, that is production and consumption, makes the challenge even harder by introducing the cyber-physical processes into the environment.

The Control System Security Training course at ASE created a different challenge. It needed a portable Industrial Control Systems (ICS) security training environment. The scientific decision on the size of the system was based on the volume of Volkswagen Golf Variant internals. All the equipment must fit into the trunk of author's car in addition to two instructors in the front. The result was training environment which today contains four different automation systems, 17 virtual machines, network monitoring and situational awareness solution. Starting from January 2015 the environment is integrated into ASECyberLab and into TUTCyberLabs. The military grade protocol agnostic remote connection solution [Error! Reference source not found.] from Finnish company Ajeco, created the means to extend the portable environment via secure multichannel connection as remote process plant for TUTCyberLabs.

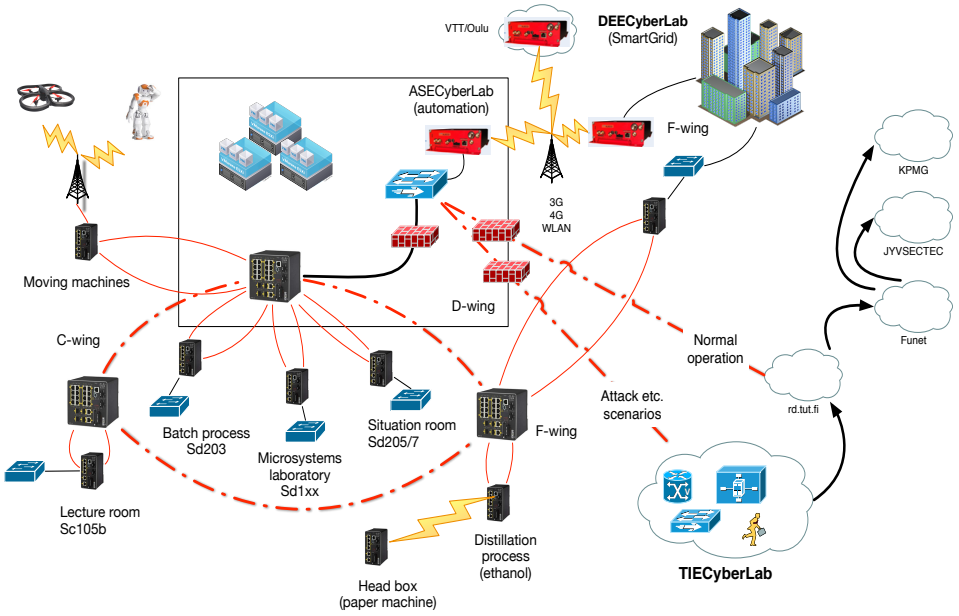

Figure 2: ASECyberLab. The red wireless boxes are used to enable secure co-operation and integration to other national parties as well as withing TUT.

3 TUTCYBERLABS

The purpose of the TUTCyberLabs research infrastructure was to create a versatile environment, focused on industry automation and electricity distribution platforms, which would facilitate research and education of cyber security. The use cases vary from normal automation education to attack and defense exercises and testing of security features of various devices and software. Particularly, it concentrated on creating an environment, which can be used to tackle the cyber challenges of critical infrastructure now and in the Future. The novel aspect of the platform was that it consists of automation system components and Smart Grid components in addition to a set of standard computing devices (PCs, TVs, gateways, mobile devices and servers). The environment must support teaching and research in each participating department, and should not have critical dependencies which can cause distruption in any of the sublaboratories. The design principle was classic "divide-and-conquer".

3.1 ASECYBERLAB

To meet the presented challenges with automation systems, ASECyberLab illustrated in Figure 2 was constructed. The core network structure is based on a process automation plant. The core is fault tolerant fiber optic ring commonly used in automation environments. The subprocesses can be integrated into the core with ease using fault tolerant copper rings. The situation room, a necessity in any Cyberlab must support various scenarios and the audio-video equipment should include the state-of-the-art display technologies for both computer as well as mobile use. The subprocesses, or automation subsystems, are allowed to be physically where their installation is meaningful. The automation may require water, air, waste water disposal, multiple floors, moving parts etc. and best way to teach is not always done next to process automation rather in classroom. The automation must be delivered with ease to the classroom - teachers are no different from automation operators, their expertise is somewhere else than in building remote communication solutions.

From the start it was decided that heart of the ASECyberLab will be virtualisation. Virtualisation makes possible fast recovery times, and enables quick scenario changes. It should be emphasised that it ”makes possible”. To enable it in practice requires careful planning and testing. However, even with modest virtualisation cluster and couple of desktop virtualisation clients it is possible to construct fault tolerant automation system. The virtualisation technology selected during the first steps of ASECyberLab in 2009 is currently in operational use also in industrial controls systems around the world. It should be noted that although virtualisation can be used to build fault tolerant automation solutions, it also presents yet another complexity layer which requires also security patching and resource planning. These challenges can also be studied in ASECyberLab. The possibility to evaluate solutions using virtual machines simplifies research and education scenarios and at the same time creates interesting research topic for Industrial Control Systems.

The requirements for ASECyberLab situation room came from the education and training perspective. The room must be as versatile as possible and support not only the security education but also working in small groups and with modern equipment. The result is illustrated in Figure 3.

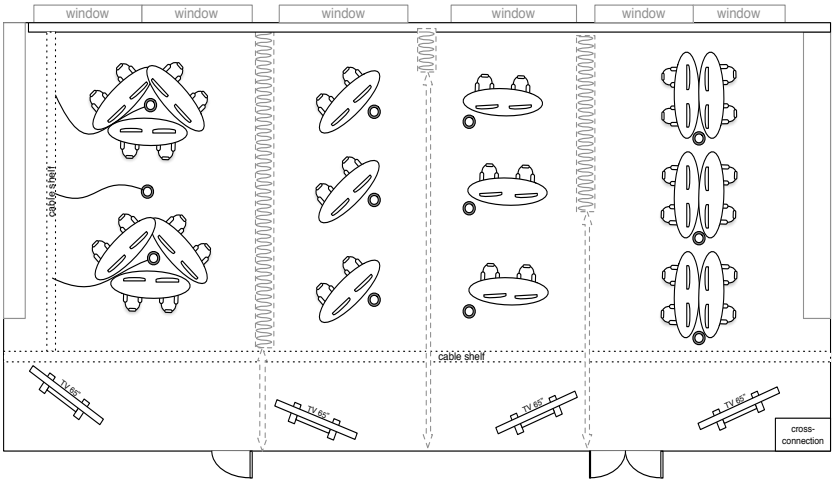

Figure 3: Situation room.

The situation room can be used in various scenarios. For example, in red-blue exercises the teams can be in the opposite ends and the management in the middle. This is enabled by noise absorbing walls between table segments. In normal classroom studies the group can be divided into any number or subgroups between 2-4. The monitor system supports presenting from any table into any combination of displays. Separate displays can different sources. The displays can also be used separately with wireless and wired display technologies.

3.2 DEECYBERLAB

The modern society depends on energy distribution. Smart Grids are seen as the Future electrical energy distribution. They are a tool to provide more dependable infrastucture, an energy-efficient way to control energy consumption and production, and a means to integrate new energy solutions to the critical infrastucture.

The DEECyberLab illustrated in Figure 4 provides the research and teaching environment where not only the traditional electricity engineering can be studied but also the challenges the Smart Grids bring into the equation. The security challenges rise mainly from the information integration needed to build a Smart Grid and the expansion of participants creating, owning and sharing the information.

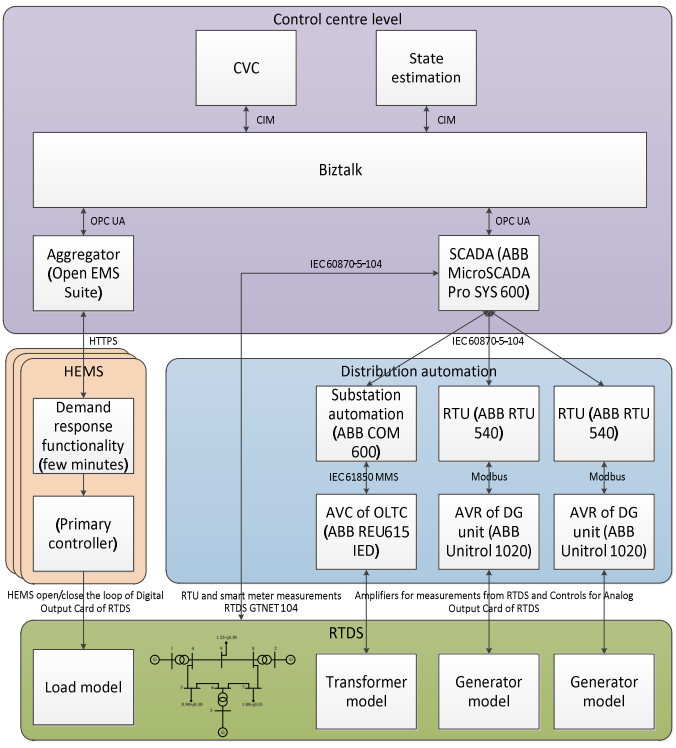

Figure 4: DEECyberLab. The HEMS is Home Energy Management System and RTDS is Real Time Digital Simulator for electrical grid.

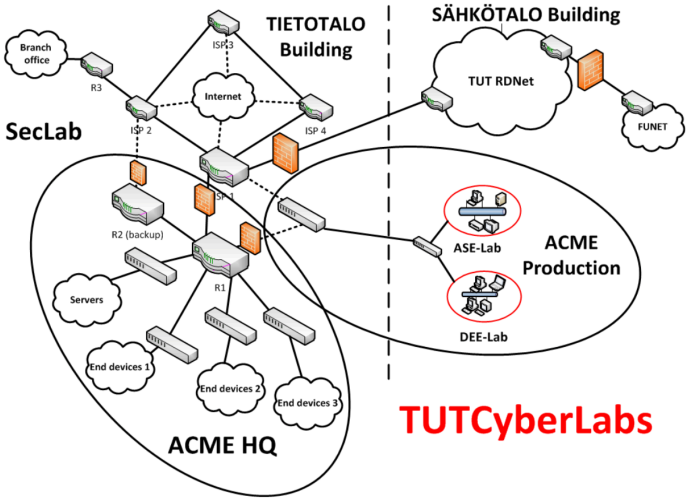

Figure 5: TIECyberLab is illustrated on the left hand side. It is internally called SecLab.

3.3 TIECYBERLAB

The TIECyberLab in Figure 5 can be considered as traditional Security Laboratory. It consist of routers, switches, firewalls and office equipment. The infrastructure is therefore combination of operator class devices as well as company office IT. The IT part is built on top of virtualisation as is typical in modern IT infrastructure. Tampere University of Technology has had separate research network called RDNet since 2009 [5]. This network provides the safe and secure connection from TUTCyberLabs to the Internet.

4 EXAMPLE USE CASES

The presented use cases are from ASECyberLab. DEECyberLab and TIECyberLab have similar use cases with the exception of different audience. These examples illustrate the vision in the beginning of the project. How it can be used and how it must be used. The 4.1. is an example of the "can be done" and the 4.2-4.3 are examples of "must be able to".

4.1 Control Systems Security Training

"Seeing is believing" - this was the base assumption on top the Control Systems Security Training was built on [6]. The portable enviroment which can be packed into a car, driven to automation company's office and can be used to provide the hands-on experience of implications of poorly implementation of information security in automation. The target audience is everyone around automation systems for example managers, developers, subcontractors, IT support, and automation engineers. Although information security is discussed and hacking tools are used, the required skill level is normal office user. The course functions as start for company's internal automation security project, a place to start or even the place to find the first contacts for securing an automation enviroment. This course is also available as co-operation with ASECyberLab partner KPMG [7].

The course consists of two parts. The first part discusses of information security as a tool to create more dependable automation. What incidents have happened and why it happened. The role of monitoring and auditing in industrial control systems is debated. The instructors on the course are more facilitators than teachers and the provided material works as a base for discussions.

The second part is where ASECyberLab is used as target for hacking. During one day exercise the participants should find the way from Internet into their target automation system. The role of monitoring is presented during the rehearsal using tools like SecurityOnion, Codenomicon Clarified Analyzer and Cisco Sourcefire.

4.2 Network based automation

Department of Automation Science and Engineering integrated critical infrastructure security into the Information Systems in Automation degree program in 2005. The security aspects are discussed in all courses from the beginning and security analysis is one of the evaluation criteria in project reports.

The core of the course is the applications of TCP/IP in automation. The students are familiarised for example in short and long distance wireless networks, using web servers and web services in automation and various integration technologies commonly found in automation systems. ASECyberLab provides the virtualisation solution and automation network where students can safely install, build an automation application and study the security challenges with Microsoft Distributed Component Object Model based OLE for Process Control (OPC Classic). The OPC Classic is know of it's security problems but still widely used integration technology due to long lifecycles in automation environments.

4.3 KYBER-TEO

The KYBER-TEO (2014-2016) project is VTT managed project with an aim to develop cyber security services and practical implementations of information security solutions and practices in the industrial sector. The main sponsors are the National Emergency Supply Agency and participating companies. ASECyberLab is used in the project as platform for developing and evaluating viable monitoring solutions for Industrial Control Systems. The physical processes together with varying automation equipment and automation systems used in critical infrastucture enables analysis and development of real-life solutions in a safe environment.

5 CONCLUSIONS

This paper presented the TUTCyberLabs concept, a Cyberlab built with co-operation in mind and targeted for educational and research purposes for participating departments in Tampere University of Technology. The seven most important lessons from the project are 1) build the environment to support normal day-to-day operations, 2) avoid organisational overhead, 3) keep it always as simple as possible, 4) there must be a vision how to use it in practise, 5) be lazy that is automate as much as possible, 6) be realistic and remember that you are running a installation of actual industrial control system and 7) there must be a tested simple drop-in solution for co-operation between partners.

The creation of TUTCyberLabs concept has been an interesting challenge. It has proven to be an answer to the initial visions although some of the decisions might be different had the change to do the project again. The project has faced all the challenges of building something concrete based on a vision, combining the vision with 30 year old automation system and related courses, and upgrading a 30 year old process into the current state-of-the-art automation system.

6 REFERENCES

1. Rajamäki J., Holmström J. and Hult T., The future solutions and technologies of public safety communications - DSiP traffic engineering solution for secure multichannel communication. International Journal of Communications, Issue 3, Volume 5, 2011.
2. Realistic Global Cyber Environment, Jyväskylä Security Technology. [http://jyvsectec.fi/en/rgce/], accessed 23.2.2015.
3. Cyber War Room, VTT Technical Research Centre of Finland Ltd. [http://www.vttresearch.com/media/news/vtt-cyberlab-reliably-spots-security-vulnerabilities], accessed 23.2.2015.
4. Cybersecurity Learning Environment, Kymenlaakso University of Applied Sciences. [http://www.ictlab.kyamk.fi/index.php/fi/kyberturvallisuus/etusivu/oppimisymparisto/100-cyberlab-datakeskus], accessed 23.2.2015.
5. TUT Rearch Network. [https://wiki.tut.fi/TUTResearchNetwork/WebHome], accessed 23.2.2015.
6. Automaation tietoturva (omin käsin)-kurssi. Tampere University of Technology, Department of Automation Science and Engineering. In Finnish. [https://ae.ase.tut.fi/csst], accessed 23.2.2015.
7. Automaation tietoturva-kurssi. KPMG Oy. In Finnish. [https://events.kpmg.fi/Default.aspx?tabid=852&TapahtumaID=38825], accessed 23.2.2015.