EKSTERN RAPPORT

Nr. 25/2020

Tverrfaglig cyberfysisk lab for kraftforsyningen

NTNU

NVE Ekstern rapport nr. 25/2020
Tverrfaglig cyberfysisk lab for kraftforsyningen

Utgitt av:	Norges vassdrags- og energidirektorat
Redaktør:	Janne Hagen
Forfatter:	Stephen Wolthusen, Vasileios Gkioulos, Beatrice Giannini, Thomas Johansen, Lars Erik Pedersen, Tore Wist
Forsidefotograf:	Lars-Erik Smevold, KraftCERT

ISBN:	978-82-410-2092-6
ISSN:	2535-8235

Sammendrag: Rapporten dokumenterer NTNUs arbeid med å utvikle en tverrfaglig cyberfysisk lab til bruk i forsknings og undervisning i cybersikkerhet i kraftbransjen. NVE har støttet NTNU med dette arbeidet. Rapporten dokumenterer resultatet så langt og skisserer videre arbeid.

Emneord: IKT-sikkerhet, Driftskontrollsystemer, Maskinvare

Norges vassdrags- og energidirektorat
Middelthuns gate 29
Postboks 5091 Majorstuen
0301 Oslo

Telefon: 22 95 95 95
E-post: nve@nve.no
Internett: www.nve.no

desember, 2020

Forord

Kraftbransjen blir i økende grad avhengig av digital teknologi. Dette gjelder også i driftskontroll- og styringssystemene. Samtidig er trusselbildet i en urovekkende utvikling, der vi har sett i andre land at trussel-aktører utfører vellykkede cyberangrep mot de kritiske kontrollsystemene. Sabotasje mot slike kontrollsystemer vil kunne gi fysiske konsekvenser med dårligere forsyningssikkerhet. Dessverre er tverrfaglig kompetanse innenfor elkraft, digitalisering, kontrollsystemer og sikkerhet en mangelvare.

NVE har derfor tatt initiativ til å utvikle tverrfaglig kompetanse i grensesnittet mellom elkraftteknologi, kontrollsystemer og cybersikkerhet. Avhengighetene og kompleksiteten mellom ulike systemer og komponenter som benyttes i kraftbransjen gjør at ulike fagdisipliner som i dag arbeider i bransjen trenger økt forståelse av hvilke sårbarheter og trusler som finnes, og hvilke konsekvenser utnyttelse av disse sårbarhetene vil kunne ha for forsyningssikkerheten. En slik forståelse er en premiss for å utvikle et velfungerende risikostyringsregime og en fungerende beredskap for alvorlige digitale hendelser.

For å sikre etterlevelse av kraftberedskapsforskriftens krav, har NVE tatt initiativ til og økonomisk støttet prosjekter som har hatt som mål å utvikle opplæringsprogram for bransjen, forskningsprosjekter og laboratoriekapasitet. I prosjektet som denne rapporten omhandler, har NVE satt søkelyset på laboratoriekapasitet. En tverrfaglig cyberfysisk lab vil berike eksisterende utdanningsmiljø og også kunne benyttes i forbindelse med etterutdanningskurs for dem som allerede er ansatt i sektoren. Fordelen med en lab er at denne vil kunne gi en helt annen praktisk forståelse enn hva ren teoretisk opplæring kan gi. NVE har derfor støttet NTNU over en periode på to år med å bygge opp en lab. Denne rapporten dokumenterer resultatet av arbeidet så langt og skisserer også en videreføring av arbeidet.

NVE har forventninger til at dette arbeidet vil bli videreført som en del av og i samspill med andre pågående prosjekter som setter søkelyset på cybersikkerhet og sikkerhet i kontrollsystemer i kraftbransjen.

Ingunn Åsgard Bendiksen

Ingunn Åsgard Bendiksen
Direktør

Eldri N. Holo

Eldri Naadland Holo
Seksjonsleder

Progress Report

NVE SCADA SECURITY LABORATORY

NTNU

Faculty of Information Technology and Electrical Engineering

Department of Information Security and Communication Technology

V. Gkioulos, S. Wolthusen (Ed.)

Report on NVE project on Laboratory for Power Systems Information Security

Revision 0 (08/12/2020 1345Z)

Revision 1 (15/12/2020 2350Z)

1. Introduction

Control systems are ubiquitous, yet there are surprisingly few educational and research facilities available that would allow substantially faithful configuration of cyber-physical systems in a simulated environment; instead this is largely restricted to fragmented components and tools.

At the same time there is an appetite on the part of candidates in cyber and information security in particular to engage with more hands-on activities such as lab-based education and training. The ability to offer insights into how control and cyber-physical systems operate and how these can be programmed and ultimately attacked or defended in a laboratory environment is a step change beyond what is possible to offer in a lecture format or with more crude simulation environments that capture only part of the system.

Power systems represent a crucial part of the national critical infrastructure in their own right as they have long been recognised together with telecommunications as the two infrastructures whose failure would result in the most rapid and wide-reaching cascading effects in addition to immediate consequences of failure. It is therefore natural to concentrate on this as a key cyber-physical system, but in addition the requirements such as timing and quality of service characteristics are more stringent in power systems than in others, making it a natural specimen to also study vulnerabilities and attacks.

Whilst there are logical and architectural security concerns which can be captured adequately otherwise, for attacks and vulnerabilities depending on sequencing and timing, the fidelity of models, particularly where these need to be joined on an ad-hoc basis raise questions as to the fidelity achievable.

In addition, there are implementation-related issues which are difficult to capture in simulation environments; whilst e.g. there are protocol simulators, these typically only implement subsets of control systems protocols rather than the full scope, and are also not adequately coupled semantically, therefore not capturing essential parts of the relevant standards.

The above clearly points to the need for laboratory-based security education for control and cyber-physical systems security, which thus far had been quite limited at NTNU and in Norwegian higher education. Clearly, however, there is a critical need for individuals with knowledge and skills in this area both in application domains and also in the wider research community.

Internationally, there exists a growing research community studying control systems security in academic environments alongside efforts by commercial entities and particularly government. Supporting the growth of an organic research capability in Norway and at NTNU enables academic staff to work in this area, resulting in both new knowledge and insight to be generated from the research, and also ensuring that sufficiently-qualified academics are able and motivated to pursue research and teaching in this critical field.

NTNU places great stock in research-led teaching, and the enhanced inclusion of students in research is an important objective as student surveys have demonstrated clearly that this greatly motivates learning as well as generates interesting and relevant outcomes alongside preparing candidates for employment e.g. in industry.

NVE conducted a survey in 2017 on the energy sector's security posture, which gave an insight into the gaps found in the sector. One finding emerging from this survey was the need to join the disciplines found in the sector (power systems, control, communications, cyber security, and security management) to enhance security and reliability.

NTNU is well-placed as a location for bringing together the required disciplines, and in the case of the Department of Information Security and Communication Technology (IIK), there already existed a location where some of this activity was being undertaken. The CCIS Centre for Cyber and Information Security had established a model for the university to be working closely with government and the critical infrastructure sector and energy in particular, with the recently-awarded Norwegian Centre for Cyber Security in Critical Sectors (NORCICS) Centre for Research-Based Innovation (SFI) awarded by the Research Council of Norway, there already exists a critical mass to coalesce other disciplines. Researchers at IIK are collaborating with the Department of Electric Power Engineering as well as the Department of Engineering Cybernetics in both research and education, and beyond this also with SINTEF Energi and SINTEF Digital, creating an unique environment capable of addressing the needs for cyber security research and education in the sector, and laboratory facilities provided by NVE are enhancing this offering

Structure of the Report

This report briefly summarises laboratories, albeit primarily targeted at research in other higher education settings in chapter 2 before describing the laboratory setup in chapter 3. We then report on initial results in education achieved over the course of 2020 in chapter 4 before an outlook over ongoing and planned work and conclusions in chapter 5.

2. Related Efforts

A number of US universities have labs and programmes with at least some facilities related to cyber-physical and not in all cases power systems. These may operate as part of regular educational offerings at undergraduate, graduate, and postgraduate levels, or can also form part of larger initiatives typically at the postgraduate level. The latter includes e.g. secondments by U.S. Department of Defence staff, or initiatives such as the Scholarship for Service administered by the National Science Foundation supporting tuition and stipends for degree programmes provided that candidates can secure a clearance and commit to work in a shortage area either within government or an approved entity for a duration equivalent to the stipend period.

Florida International University (Miami, FL, USA) hosts the Cyber-Physical Systems Security Lab (CSL) headed by Prof. Selcuk Uluagac with research projects such as energy management systems for domestic environments; teaching in the space is limited to a module on Security of Internet of Things.

Similarly, Duke University (Durham, NC, USA) hosts a Cyber-Physical Systems Security Lab (CPSL) headed by Prof. Miroslav Pajic; whilst research is more focused on manufacturing systems and IoT, teaching is focused on bridging Electrical and Computer Engineering and Computer Science with modules on topics including Cyber-Physical System Deisgn and Formal Methods for Cyber-Physical Systems.

Prof. F. Hu from the University of Alabama (Tuscaloosa, AL, USA) and T. Morris (at the time Mississippi State University, now University of Alabama at Huntsville) developed virtualised classrooms for CPS security in the 2013-2016 time-frame with teaching materials alongside pre-packaged simulated labs suitable for undergraduates and some lab configurations for pre-configured research questions

A number of researchers at Virginia Tech College of Engineering work on cyber-physical systems security but with an emphasis on aerospace applications.

University of Tulsa has some laboratory facilities also for the use in CPS security with research and education on CPS topics related to oil & gas, nuclear, and power systems.

The Embedded and Cyber-Physical Systems Lab led by Al Faruque at the University of California, Irvine studies security aspects of CPS systems including smart grid and EV systems with an emphasis on cross-domain topics and teaching including cyber-physical systems design at the graduate level.

The University of Texas Dallas (Dallas, TX, USA) Software & Systems Security Lab (S3 Lab) led by C Kim offers small-scale student laboratories in cyber-physical systems security with an emphasis on IoT.

In addition groups at the University of Michigan Ann Arbor and the University of Illinois at Urbana-Champaign are developing facilities for testing and evaluation of IoT and control systems which can also be used in educational lab settings, a similar effort has also been undertaken by researchers at Arizona State University.

A number of further higher education institutions in the US offer CPS security courses, laboratories, and classes as part of their regular degree programmes; hence this list is necessarily only a very partial view and focuses on institutions where there is also an organisational entity in the form of a laboratory rather than in embedded form. One group undertaking relevant work since 2007 and sharing resources as well as best practices worth noting in this context is the I3P consortium of 18 academic research centres including Binghamton University, Carnegie Mellon University, Dartmouth College, George Mason

University, George Washington University, Georgia Institute of Technology, Idaho National Laboratory, Indiana University, Johns Hopkins University, Lawrence Berkeley National Laboratory, MITRE Corporation, New York University, Oak Ridge National Laboratory, Pacific Northwest National Laboratory, Purdue University, RAND Corporation, Sandia National Laboratories, SRI International, University of California Berkeley and Davis, University of Idaho, University of Illinois, University of Massachusetts Amherst, University of Virgina and recently the University of Tulsa already mentioned explicitly above.

In Germany the DFKI associated with the University of Saarbrücken as the Max Planck Institute for Security and Privacy undertake research and to a limited extent education in cyber physical systems security with an emphasis on embedded systems rather than cyber-physical systems in particular. Other cyber-physical systems research activity such as the Cyber-Physical Systems Laboratory at the University of Potsdam Hasso Plattner Institute concentrate more on autonomous systems and robotics or industrial systems in the scope of their laboratory facilities.

In the United Kingdom several universities also hold smaller scale relevant facilities; these include the University of Oxford and Imperial College Systems and Algorithms Laboratory.

Activities in Singapore centre on Nanyang Technical University with work mostly concentrating on water management and automation systems and at SUTD which hosts several test beds, including one on electrical power systems intelligent control which are also utilised for training and education purposes.

In the Norwegian context, the University of Oslo maintains a CPS Lab at IFI with some activities mostly related to networking and IoT, most other aspects are handled by way of modelling and simulation; at NTNU the Norwegian Cyber Range is part of the infrastructure established by NTNU IIK and augmented by the laboratory described in this report in more detail later on.

Test Beds

Chen et al.[1] proposed a real time cyber physical testbed; their architecture contains a physical system modeller, a cyber system modeller, and a data exchange mechanism where the physical system modeller consists of a Real Time Digital Simulator (RTDS) and physical IEDs. The cyber system modeller consists of a simulated control centre, simulation of other substations, and networking; this test bed, however was not intended for cyber security exercises.

Genge and Siaterlis[2] proposed a framework for security studies of future smart-grids is presented. The physical environment (generation, transmission, substation distribution and customer end) is represented by a simulated model using Matlab/Simulink. Prototypes of the cyber elements SC, R-PLC and Master Units were developed in C for emulation on Unix-based systems. Emulated components can be replaced with real components in their architecture.

[1] *B. Chen, K. L. Butler-Purry, A. Goulart, and D. Kundur, "Implementing a real-time cyber-physical system test bed in RTDS and OpNet," in* North American Power Symposium (NAPS), 2014*, IEEE, 2014, pp. 1–6. DOI:* 10.1109/NAPS.2014.6965381

[2] *B. Genge and C. Siaterlis, "Developing cyber-physical experimental capabilitiesfor the security analysis of the future smart grid," in* 2011 2nd IEEE PES International Conference and Exhibition on Innovative Smart Grid Technologies*, Dec. 2011, pp. 1–7. DOI:* 10.1109/ISGTEurope.2011.6162766

Tebekaemi and Wijsekera[3] describe the design of an IEC 61850 based testbed for distribution substation simulation/emulation. The testbed is described to enable security research such as IED vulnerability analysis, test and analysis on security protocols, the implementation of cyber security functions & controls, physical attack simulation and analysis. Key benefits of the model is described as modular design, scalability, low cost, ease of setup and the use of interoperability. The physical part of this testbed is a substation simulated in MatLab; IEDs are implemented as Virtual Machine (VM)s and the network is emulated with the GNS3 network emulator.
Poudel et al. [4] describe a cyber-physical system testbed applications as vulnerability analysis, stability and control, disturbance scenarios, training and education, cyber-physical assessment metrics, impact analysis and mitigation module. A CPS testbed for a power systems is proposed, but the implementation status is not entirely clear. The physical environment proposed as a simulateion environment based on Matlab/Simulink with OPAL-RT used to provide an interface between Matlab/Simulink and the IEDs. We note that in this testbed real production IEDs are used as protective relays while Distributed Network Protocol 3 (DNP3) protocol is used for control and measurements between control centre and substation.
Finally, the SoftGrid testbed is described by Gunathilaka et al. [5]. This is a software based smart-gridtestbed for evaluating substation cyber security solutions. The system simulates a SCADA Control Centre and IEDs. The physical element is simulated with the PowerWorld simulator, and SoftGrid interfaces PowerWorld with the PowerWorld COM API; here, the OpenMUC library is used to implement the protocols IEC 60870-5-104 and IEC 61850. Security solutions like Intrusion Detection System (IDS), firewalls and security enhanced gateways can be plugged into the SoftGrid testbed for evaluation.

[3] *E. Tebekaemi and D.Wijesekera, "Designing an iec 61850 based power distribution substation simulation/emulation testbed for cyber-physical security studies," in* Proceedings of the First International Conference on Cyber-Technologies and Cyber-Systems*, 2016, pp. 41–49*

[4] *S. Poudel, Z. Ni, and N. Malla, "Real-time cyber physical system testbed for power system security and control,"* International Journal of Electrical Power & Energy Systems*, vol. 90, pp. 124–133, 2017*

[5] *P. Gunathilaka, D. Mashima, and B. Chen, "Softgrid: A software-based smart grid testbed for evaluating substation cybersecurity solutions," in* Proceedings of the 2nd ACM Workshop on Cyber-Physical Systems Security and Privacy*, ACM, 2016, pp. 113–124.*

3. Laboratory Design

Whilst the remit for the laboratory was to create an exemplar for a laboratory to be used primarily in an educational setting, the design has been performed with the intention to also maximise the ability to utilise and integrate with further facilities hosted by NTNU and also SINTEF Energi to maximise value and flexibility.

As the bulk of the laboratory was to be located in Gjøvik, the use of actual power systems equipment was considered but postponed since the price points for suitable systems would have been well outside the available budget.
Instead, the focus for the design of the laboratory has been on the control and communication systems. This is driven in part by the requirements for the laboratory itself and also by the availability of power systems for validation both at the Department of Electric Power Engineering and at the Norwegian Smart Grid Laboratory (NSGL).

To facilitate educational use, moreover, a single system would impose a substantial bottleneck for access in scheduling session time; hence as far as practical the laboratory was designed to allow many educational activities to be taken with several seats. For simple UI/HMI tasks, moreover, there exist simulators for the S7-1500 described below as well as the user interface, allowing e.g. students to prepare code before testing in a lab environment.

Figure 1: Siemens Simatic S7-1500

Moreover, given the distributed nature between Gjøvik and Trondheim of both department and lab facilities, care was taken that where possible the components were configured in a way which is transportable (although dimensions and weight imply that public transportation is not ideal in this case).

Workstations

Three individual workstations are equipped with the widely used Siemens Step 7 software. To allow flexible use in a portable environment, the lab consists currently of four workstations based around a Siemens S7-1500 controller; these are supported by the Siemens Simatic Step 7 Pro TIA Portal V16 widely used in the power industry.

The S7-1500 allows both the direct connection of analog I/O as well as connection via the Ethernet interface (primarily Profinet in the lab configuration). Whilst this system is restricted in its computational capabilities, it is adequate for many control tasks and compatible with widely used software systems, allowing users, trainees, and students to become acquainted with engineering and operator views.

Unlike the S7-1200 equipment originally anticipated for purchase at the time of submitting the bid to NVE, the price point for the S7-1500 has been reduced to where it became viable to purchase these instead; the principal advantage of this newer unit is that it is better able to not only support standard IEC 60870 but also IEC 61850 protocols for power systems.

Figure 2: Siemens Simatic TP1500 HMI

The S7-1500 units are mounted in 19" racks (12U) equipped with a generous 24V power supply to allow the integration of both further I/O modules on the DIN rail as well as of IEDs to be able to have self-contained configurations at least for emulated IEDs and physical systems.

No separate computing equipment is part of the workstations, it is assumed that users will rely on separate machines to operate and access these. We note that this is a constraint owing to the somewhat baroque and rather expensive software licensing mechanism used by Siemens for the TIA Portal software requiring explicit licence migration between users, and may consider the purchase of a 1U rack-mount PC to address this issue, then giving remote access to this machine instead.

To be able to provide also a realistic operator perspective as well as to study the communication and control flow to HMI, each of the workstations was equipped with a Siemens Comfort Panel TP1500 and the Siemens Simatic WinCC Comfort V16 software; this is directly supported by the interface of the S7-1500.

SCADA Configuration

The components above represent minimal functional units for work requiring the development, deployment, and testing of code running on the PLC, and allows interfacing with IEDs, but this would be somewhat restrictive in terms of the attacks one may be able to simulate for control systems. More realistic control systems such as used in substation automation would normally require a SCADA architecture relying on a combination of multiple PLC and RTU as well as a combination of network protocols. The Siemens ET200SP supports Modbus TCP, Profinet, and Ethernet/IP, and can hence be used to simulate a SCADA environment. These units are further configured with a number of I/O modules, specifically an Energy Meter (for up to 400VAC), 4-wire input ports, 4 2-wire outputs and an 8-port digital interface. For future expansion, the ET200SP can also be equipped with I/O ports suitable for e.g. direct motor starters, giving the option of integrating physical components into the lab environment by simply adding relatively inexpensive interface modules.

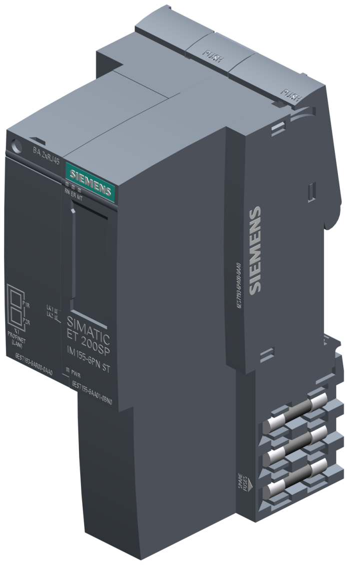

Figure 3: SIemens ET200SP Multi-Fieldbus Interface

The S7-1500, ET200SP including I/O modules, TP1500 HMI and power supply are each mounted in mobile 19” racks and leave sufficient room for connections as well as the placement of (emulated) IEDs, allowing the equipment of three lab workstations with a deskside rack and a table used to set up ancillary equipment such as cyber-physical components, networking equipment and user workstations.

Moreover, where more complex configurations are required, these can be joined together via Ethernet and one of the supported layered protocols.

Intelligent Electronic Devices

At present the laboratory has no dedicated actual power systems equipment (loads or generators), although we are considering to add such facilities, particularly loads and inverter-connected battery systems allowing to simulate generator behaviour as well as control over the injection of active and reactive power.

Instead, work in 2020 has concentrated on the development of IED emulators which fit into a co-emulation environment.

For this, two different types of single board units were considered. A low-cost, but lower powered Arduino board based on a 16MHz ATMega 328P was used, which has the advantage of both low cost and being able to operate rapidly after reboots and power cycles; these devices also have the advantages of being sufficiently simple that deterministic behaviour can be achieved easily as there is no operating system worth mentioning that can interfere with their operation. However, these boards are not realistically capable of implementing more than a rudimentary IEC 61850 protocol variant, and hence our work has concentrated on offering an IEC 60870-5-104 server and client.

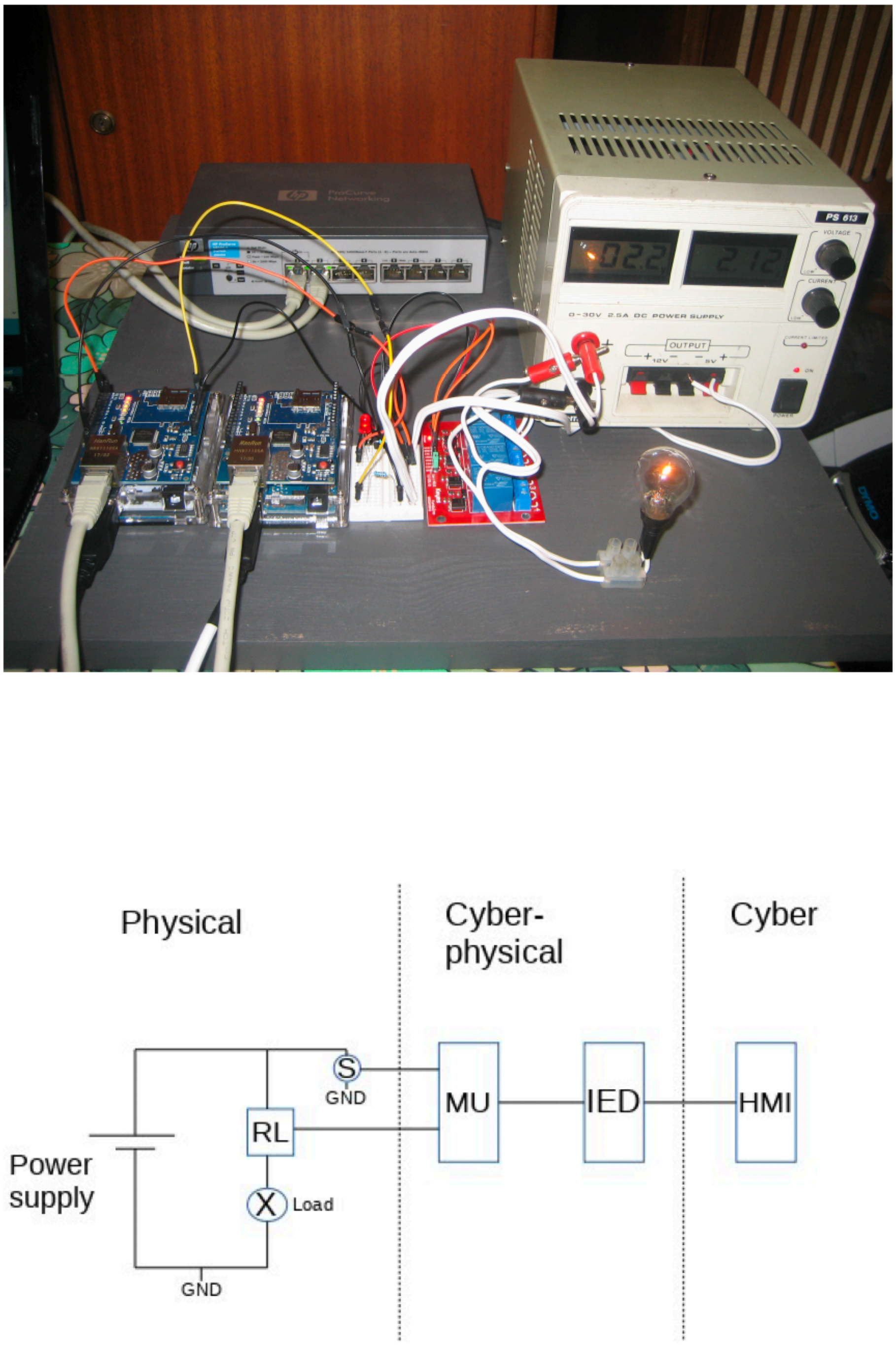

Figure 4: Arduino-Based IED and MU Emulators with Test Environment

In this context we implemented an emulated measurement unit (MU) on the basis of one Arduino board (server), while the IED is emulated by another Arduino board, allowing observation of real network and measurement traffic, particularly as the analog and digital I/O capabilities of the Arduino board are sufficient to perform simple direct measurements and actuations on low-voltage circuits. For more advanced operation, these must then be coupled with I/O modules such as those of the ET200SP described above.

Whilst limited, IEC 60870 is still in widespread use in power system automation, and the Arduino boards are both cheap and robust so that they can be deployed in experiments and educational settings with ease.

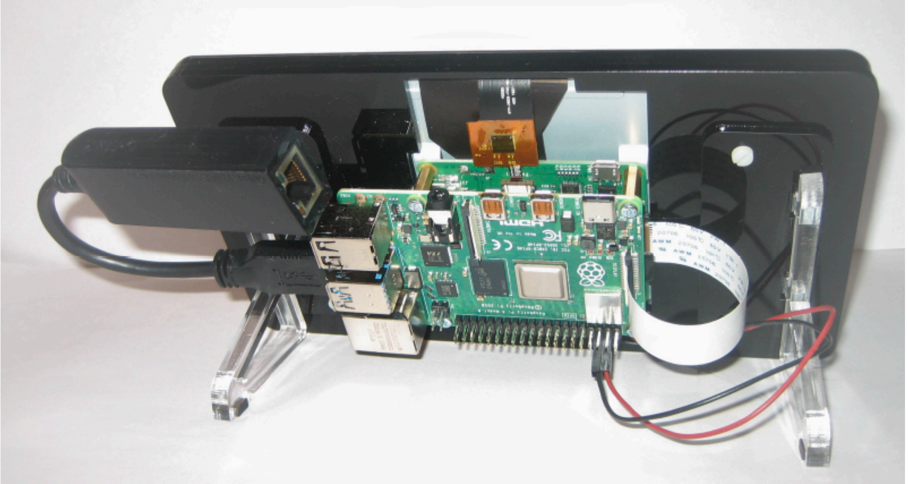

Figure 5: Raspberry Pi IED with Touch HMI and Gbit Ethernet Interface

For more complex IED requirements, particularly to support IEC 61850 protocol runs required for the simulation of substation automation, a more potent platform in the form of a Raspberry Pi (Model 4B, 4GB) was chosen. The Raspberry Pi provides several interfaces that are relevant for the development of emulated IED, but has only one integrated Ethernet interface. In order to provide an extra Ethernet interface, a USB-3 to Ethernet adapter was used.
This is slightly problematic in that timing variance of both USB-3 and Ethernet will compound, but are a design restriction that would have otherwise required the use of substantially more expensive boards.

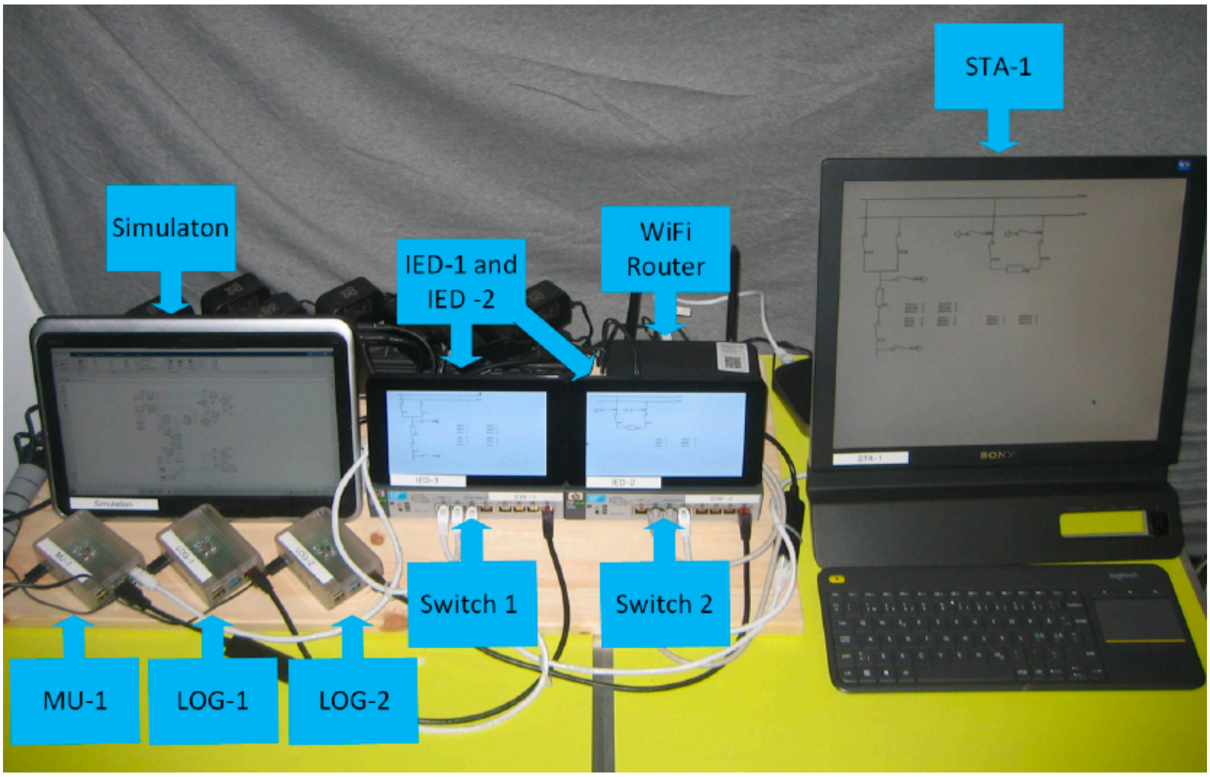

Figure 6: Test setup with multiple IED and MU emulators based on Raspberry Pi modules

While not strictly necessary for an IED, for experimental purposes it was considered to be helpful to have a direct HMI for the Raspberry Pi IEDs; this is readily available and integrated with the basic board (see figure 5), for providing a simple HMI a Cairo and GTK+-based interface was implemented. Not all Raspberry Pi were equipped with a HMI, where this was not the case (primarily for MU deployment) these were controlled by a remote access mechanism (which is not part of the emulation environment).

The actual protocol support is based on the LibIEC library, which offers open source support for IEC 60870-5-101 and -104 as well as selected elements of IEC 61850.

As the IED emulator may need to emulate measurements when used in MU mode, a simple Postgres database was implemented.

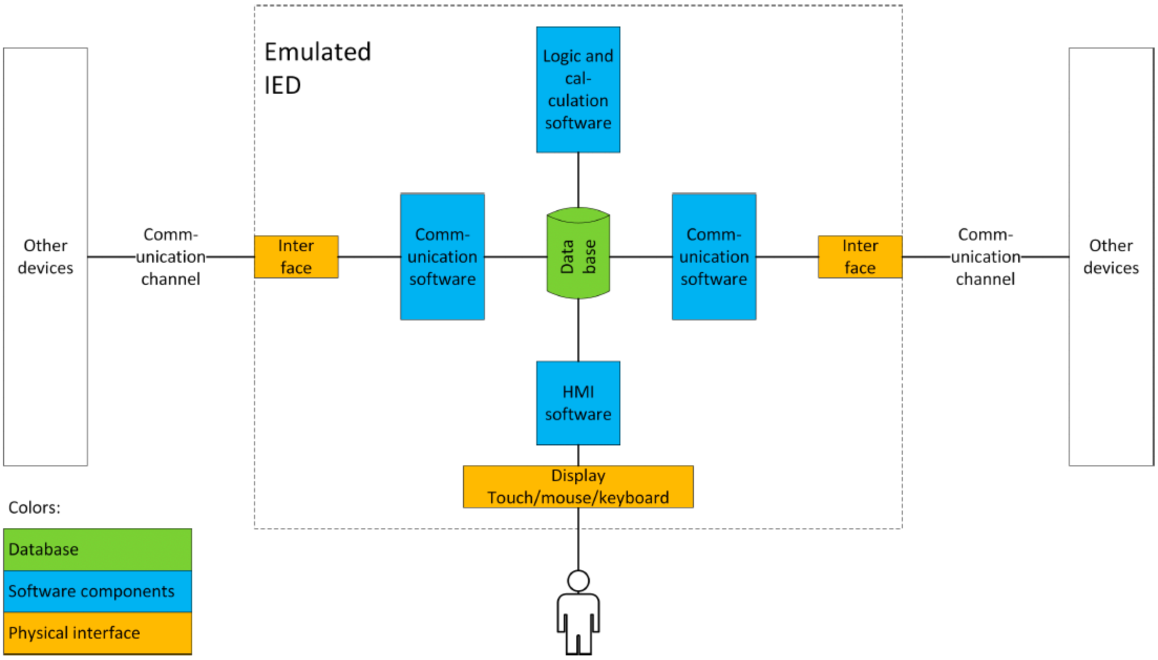

Figure 8: Emulated IED Architectural Model

Figure 8 shows the overall software architecture of the higher-end emulated IED, which allows the flexible deployment of a combination of simulated components and hardware-in-the-loop.

This system offers greater flexibility than the Arduino model but at the price of losing some fidelity for timing, particularly as the different components were developed not as monolithic code but rather as interfacing individual processes embedded in the operating system context. This, however, gives the option of changing e.g. new or different components without affecting the architecture or other components.

Care has also been taken to enable more detailed logging of events and debugging facilities as these are critical to the understanding of attacks and defence mechanisms; the open source architecture here gives greater freedom for instrumentation compared to closed source implementations at the cost of lower fidelity in terms of timing behaviour and relying on the open source library (up to this point) for implementing the IEC 60870 and 61850 protocols; so far no IEC 62351 implementation has been attempted for either base protocols.

Figure 7: Experimental setup with multiple IED and MU Raspberry Pi modules

Co-Emulation Environment

The Merging Units (MU) developed on the same software basis are able to operate both interfacing to hardware in the loop (not currently implemented; this requires interfacing with physical equipment not currently in place in the lab in Gjøvik) as well as with a simulated environment.

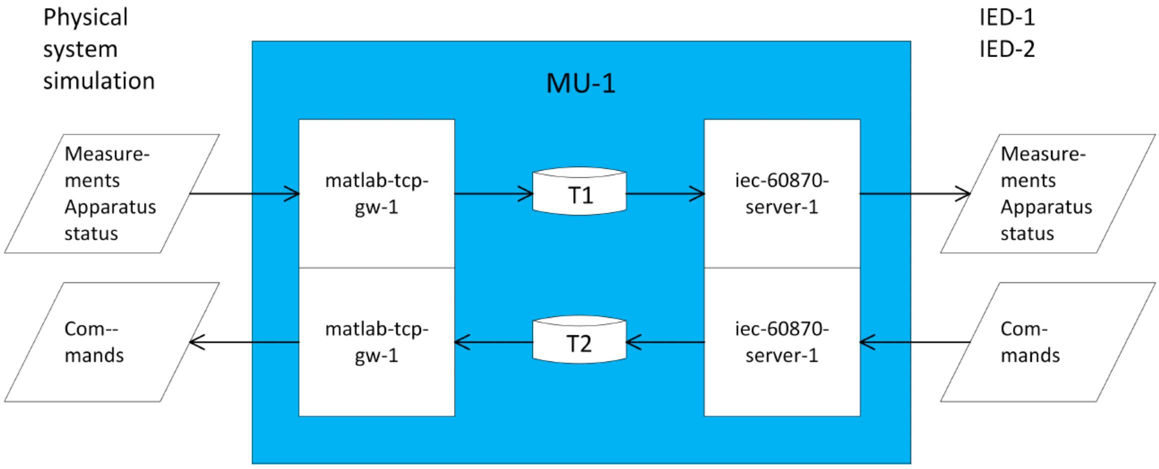

Figure 9: Emulated Merging Unit Architecture

For simulation the RTDS and MatPower are used; in principle these models should be interchangeable with other simulation environments such as Opal-RT used in the NSGL as well as hardware-in-the-loop environments.

For substation automation a bay control infrastructure was developed for software emulation; this currently supports only IEC 60870 as the communication protocol mostly due to the effort required to synthesise and parse bay descriptions in IEC 61850 this was left for a later implementation stage.

Networking Infrastructure

The lab is supported at present by industrial Ethernet switches supporting IEEE 1588 (PTPv2) time synchronisation; these were purchased from funds related to another, European project but can be utilised as part of the laboratory setup.

Whilst not part of the original plan for the laboratory, a research project jointly undertaken with Rebecca Montanari (U. Bologna, Italy) funded by the Erasmus programme allowing the visit of a student (Beatrice Giannini) allowed the development of a SDN infrastructure which can emulate a number of different network topologies using the Mininet simulator which goes beyond what is available in terms of interconnection of different components. A number of such topologies are available as a library for configuring an OpenFlow emulation environment operating within the confines of a simulation; this is a largely seamless process whereby the controller running OpenFlow (based on the OpenDayLight controller

framework) can be provisioned on either a virtual machine or on a separate physical machine and will interface with either real forwarding engines (currently not implemented; in the context of a European Horizon 2020 project SDN-uSense the relevant equipment has been purchased and deployed within the setup of the NSGL, however).
This architecture allows the deployment of more complex network architectures as well as the injection of arbitrary modifications to network behaviour such as packet loss rate, delay, and jitter.

4. Education

A key educational element in 2020 was the aforementioned development of simulated IED platforms; this formed the basis of two M.Sc. projects (Thomas Johansen and Tore Wist) and was mostly concerned with developing the actual platforms as well as the emulation environment allowing the partial substitution of real physical components and within limits also of PLC equipment for bay control.

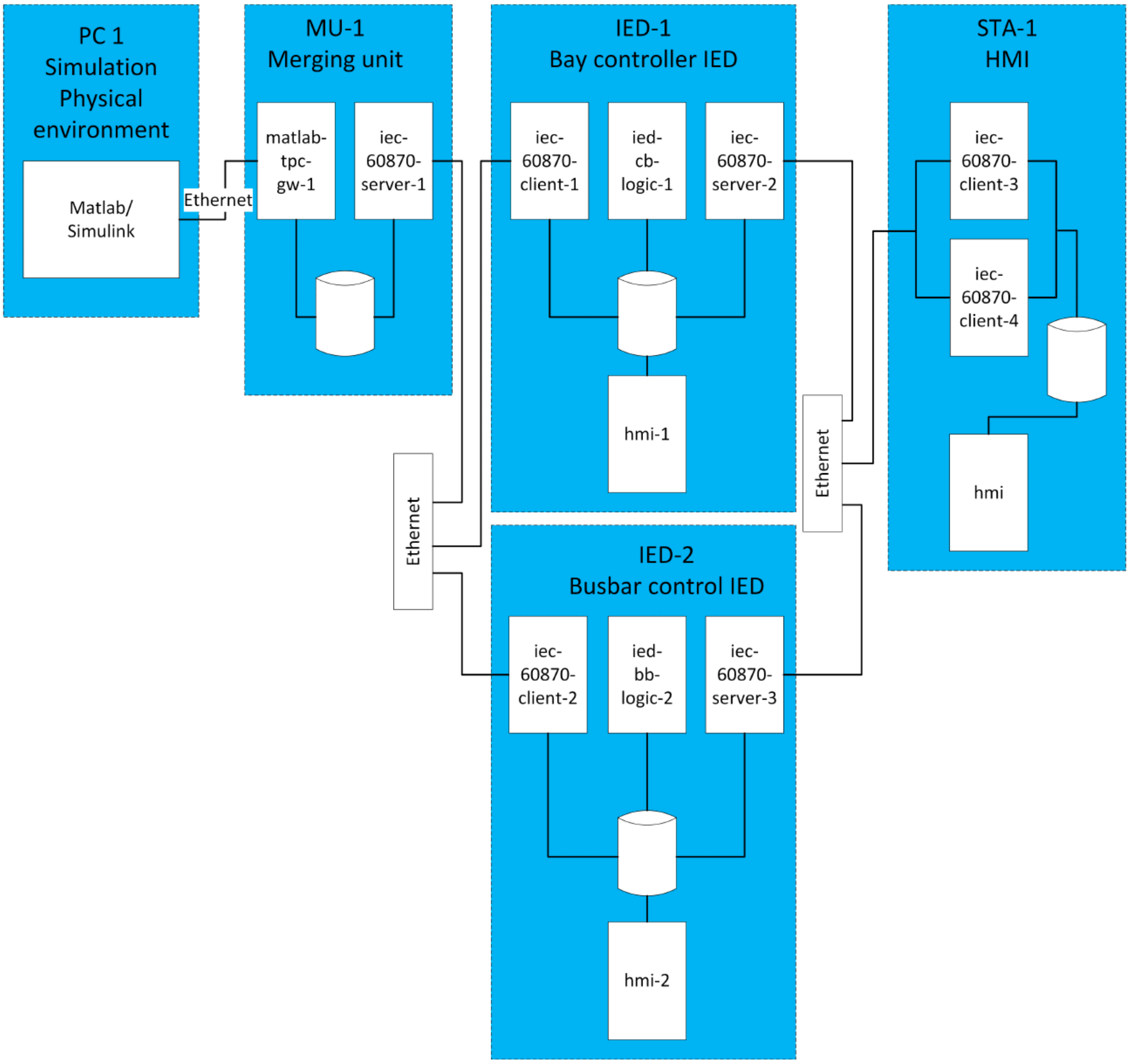

Figure 10: Reference Scenario for IED Emulation Validation

For validation a reference scenario was developed (see figure 10 above) which allows a simulated power system (left hand side in figure 10) to interact with the HMI, populating all pathways along the way and resulting in verifiable traffic on the network interconnection.

This setup was then used to develop a number of simple attack scenarios based on the ISA95 architecture targeting interactions between the different levels (ERP, Historian and EMS, HMI/SCADA, and ultimately PLC/RTU/Sensors).
As the bulk of the work in 2019-20 was given over to the development of tools and lab environments, the attacks developed so far are relatively simple, but are part of a larger library developed based on a more extensive taxonomy following the ISA95 architecture and linked to related work on risk and threat analyses in the power systems automation domain.

Targeted attacks thus far concentrated on network-based attacks where packet- and message flooding was undertaken at different interfaces, while other attacks sought to capitalise on the relatively unfettered access to buses and performed Man-in-the-Middle attacks. A more sophisticated attack scenario targeted the updating of IED firmware and demonstrated the feasibility of this approach. Naturally this is part of an ongoing development.

Courses

The course IMT4203 (Critical Infrastructure Security) was expanded to include a substantial elements on power systems as well as the security of power systems and protocols, students are further given the option to take up a term paper mini-project as part of this course offered in the autumn semester each year; it is also well-placed as a springboard to recruit M.Sc. and future integrated Ph.D. candidates interested in the field.
It had been planned to integrate lab activities into the course in the 2020 iteration of the course; however, the restrictions that had to be imposed for access to buildings and labs in particular have caused this to be postponed to 2021.

A professional development course was also offered (IIKG6502) at the same time based substantially on the format and contents described above. This has been taken up considerably with over 20 candidates enrolling in the initial 2020 iteration.

5. Conclusions

This report has briefly summarised the work undertaken as part of the NVE supported laboratory build-up.
Most effort has been devoted to creating a flexible setup which can support as many different network and control configurations as possible based on common components that may also be utilised individually for research and education purposes such as for individual lab workstations.

The installation of the Siemens Simatic workstations after the summer of 2020 now allows the flexible configuration of co-emulation of both network components and control system components, which provides with the ability to study attacks and vulnerabilities in greater scope than where one is restricted to a relatively small number of physical components.

One remaining limitation of the lab is the absence of dedicated power system equipment; it is anticipated that some of this may be added as part of the recently granted SFI NORCICS as well as currently pending proposals including the ElectriFAI initiative jointly run between SINTEF Energi and NTNU; whilst most of the equipment for the latter is earmarked for the Trondheim site, the integration with the lab and wider CP-NCR in Gjøvik is part of the proposed effort where the competence particularly for control systems and networks is to be based in the group in Gjøvik.

Outlook

As a further step to enable capabilities for more in-depth evaluation and attack modelling for IEC 61850 in particular and time-sensitive aspects of importance to power systems in the GOOSE/SV subprotocol regime, we aim to purchase a Siemens CP8000 system; this then also has the capacity to interact with PMUs at a frequency relevant for smart grid applications.
At present no power systems with PMUs are present in the Gjøvik lab environment, hence the CP8000 system will also need to be set up in a mobile environment similar to those already described in chapter 3.
Similarly, particularly for studying QoS aspects of network interconnections in power systems, we aim to build on the work reported above on instrumented SDN environments; for this we seek to acquire a dedicated server and network configuration for SDN environments with several packet forwarding engines and a server system capable of handling multiple controller instances, NFV components, simulated network topologies as well as instrumentation for attacks and monitoring; at present hardware limitations constrain what is possible to emulate.
We also seek to (presumably in both Trondheim and Gjøvik, as this requires the physical installation of GNSS antennae) the provisioning of grandmaster clock in anticipation of further studies of timing-based attacks.
Preliminary work has already been undertaken (by T. Jenkins at Royal Holloway under the supervision of S. Wolthusen) on constructing a spoofing mechanism based on SDR for GPS timebase spoofing using HackRF SDR in conjunction with a dedicated Raspberry Pi module

for both spoof transmission and monitoring/interception; this is a key element in attacks on PMUs as well as timebase attacks for SCADA systems previously studied by A. Baiocco and S. Wolthusen.

Theoretical work has also been undertaken on the security of protective relays and SIS components; the relevance of these was underlined in recent years by a number of attacks such as the Triton malware targeting Saudi Aramco and SABIC systems as well as attacks against the Ukrainian power grid. These can be integrated into the bay controller architecture described above.

As noted previously we will investigate the integration of physical power equipment including motors, batteries and inverters including local control modules, and PMU components. However, here, both space and health and safety constraints will need to be negotiated carefully. At the time of writing the report (December 2020), the lab rooms have not yet been provisioned with required safety equipment (emergency power switches for each workstation and the lab), hence only low-voltage experiments can currently be undertaken.

We also aim to develop an attack library based on work undertaken in 2020 by T. Wist, and which will allow the integration of multi-stage attacks.

This will also facilitate the development of lab exercises for students as the time typically allocated to lab exercises will not realistically allow for the complete development lifecycle for attacks and rather will need to build on existing components to enhance the understanding and enable the construction of reasonably complex and realistic scenarios.

Contributors

Beatrice Giannini

Vasileios Gkioulos

Thomas Johansen

Lars Erik Pedersen

Tore Wist

Stephen Wolthusen

NVE

Norges vassdrags- og energidirektorat

MIDDELTHUNS GATE 29
POSTBOKS 5091 MAJORSTUEN
0301 OSLO
TELEFON: (+47) 22 95 95 95

www.nve.no