WHITE PAPER:

Open Testbeds for CNI

Open Testbeds for CNI

Authors

Chris Hankin (editor), Imperial College London

Deeph Chana, Imperial College London
Ben Green, Lancaster University
Rafiullah Khan, Queen's University Belfast
Peter M3, National Cyber Security Centre
Peter Popov, City University of London
Awais Rashid, Lancaster University and University of Bristol
Sakir Sezer, Queen's University Belfast

1 Introduction: Rationale/Justification

Industrial Control Systems (ICS), composed of combinations of hardware, software and ICT networks, orchestrate the myriad of functions needed to execute complex tasks such as the delivery of utility services and the operation of intricate and disparate manufacturing processes. ICS are examples of cyber-physical systems – digital systems that affect and are affected by, physical processes – whose use is growing through developments in smart-city technologies and the rapid emergence of the Internet of Things. Such systems are increasing in importance as techno-social components of the Critical National Infrastructure (CNI) of the future and as they extend their scope, becoming ubiquitous, accessible and transformative to wider society and the economy, the need to understand their security characteristics also increases.

To date the Research Institute in Trustworthy Industrial Control Systems (RITICS) activity has focussed on identifying existing technical and practical problems that surround the development of secure and trustworthy ICS. In order to develop realisable solutions to these problems RITICS has conducted a research programme that includes work in:

- Theory and analysis
- Simulation and experimentation
- Testing and implementation

To effectively execute this mission, the need for a simulation/lab space where components and instances of investigated digital systems may be physically configured for 'close to real-world' fidelity is vital. RITICS partners have developed small-scale testbed facilities. This white paper surveys the current range of facilities, summarises the lessons learnt, presents the issues with linking these facilities and concludes with a forward look.

Our ambition is to interconnect the existing systems together in order to achieve the scale of real-world systems and to use the capabilities to accelerate and increase efficiency/effectiveness of the UK investment. This will enable us to

- better understand the interdependencies between different sectors
- better understand the similarities and differences between Information Technology (IT) and Operational Technology (OT)
- test and prepare for targeted and untargeted attacks
- provide training to close the skills gap
- validate various theories about how to deal with new and unknown threats

- extend understanding of system-user relationships across an array of sectors

There will also be the need to develop a business model for how the Open Testbeds might operate.

2. The UK Landscape

The Lancaster ICS Testbed

The most extensive testbed facilities developed within RITICS have been developed by the MUMBA project at the University of Lancaster. In addition to their lab-based testbed which can be configured in a number of ways, they have also developed a table-top water treatment demonstrator.

A high-level view of Lancaster's ICS testbed is shown in Fig. 1 [1]. The architecture is based on the Purdue Reference Architecture. Currently split across six Manufacturing Zones, an ICS Demilitarised Zone, and an Enterprise Zone (with its own separate Demilitarised Zone), all equipment in the testbed is physical (unless otherwise noted as *Virtualisation Platform* in Fig. 1). It is important to note that Lancaster's testbed has focused on the development of systems and devices across Levels 0, 1, 2, 3, DMZ and 4 of the Purdue model.

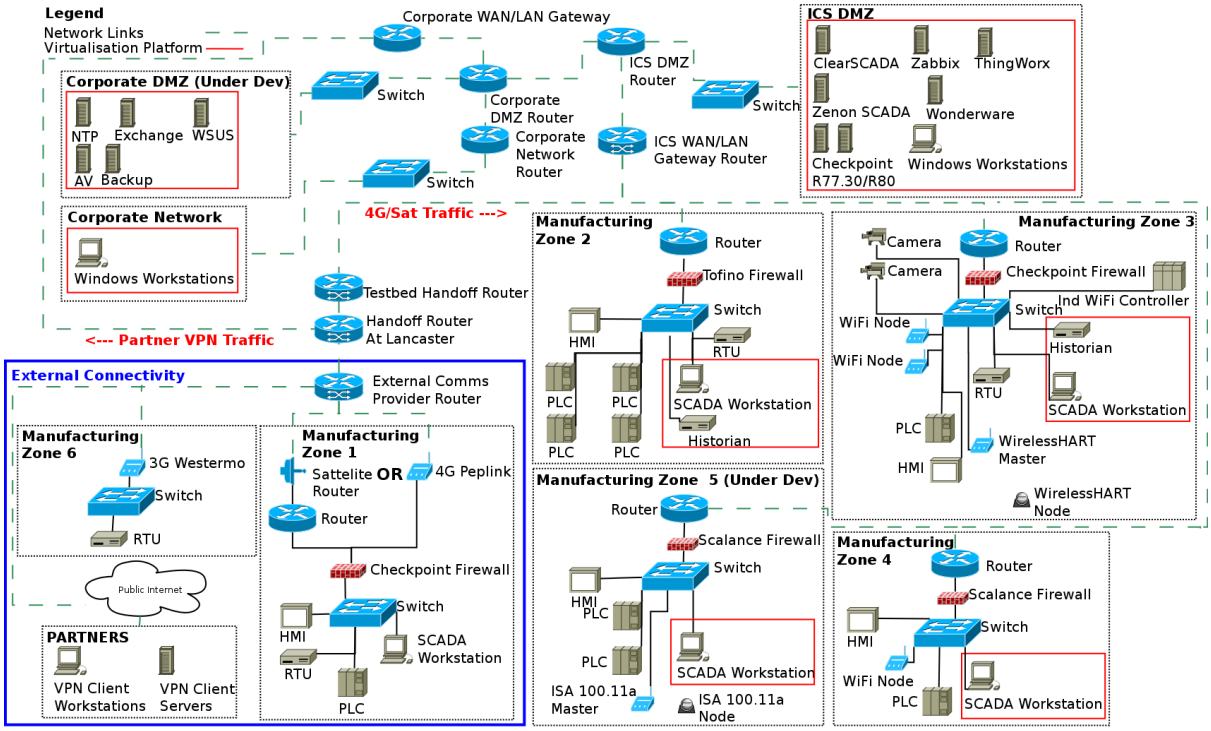

Figure 1: Network Diagram of Security Lancaster's ICS Testbed

ITRC's DAFNI project

The Infrastructure Transitions Research Consortium (ITRC) is a consortium of 7 universities (Cambridge, Cardiff, Leeds, Newcastle, Oxford, Southampton and Sussex), investigating ways to improve the performance of infrastructure systems in the UK and around the world. Their research is helping businesses and policymakers to explore the risk of infrastructure failure and the long-term benefits of investments and policies to improve infrastructure systems.

The Data and Analytics for National Infrastructure (DAFNI) project will create a national infrastructure database for visualisation and analysis. It will be a shared, secure system for academic research and a resource for businesses, innovators and policy-makers.

DAFNI welcomes ideas about how it will work with different partners, and on issues such as: security, access, suitable business models; and next steps.

A key feature will be DAFNI's simulation and visualisation facilities to allow use of models in a more flexible way, enabling the systems of systems analysis and incorporating observed and simulated datasets. DAFNI will benefit from the experience of the ITRC) which has been developing a one-stop database for UK infrastructure (National Infrastructure Systems MODel – NISMOD). It's much more than a curation of data, and allows representation of interdependencies to inform planning decisions, including via a visualisation dashboard. Although NISMOD contains over 400 data layers (representing multiple sectors, demographics, economics), the infrastructure sector needs greater detail, to represent individual buildings and to develop plausible connectivity networks, which DAFNI can deliver. ITRC-Mistral is developing a meta-database to give users the experience of a single interface, although it brings together many databases, and this is the model that will be applied to DAFNI.

One challenge will be how to make DAFNI successful operationally. DAFNI's vision is to build an environment where people can try different solutions, which means being responsive to all users. Existing models might include JASMIN that uses the desktop as a service tool using a standard toolkit, with no restrictions on users.

5G Testbeds

The Department of Digital, Culture, Media and Sport (DCMS) are investing in a 5G technology test network aiming to put Britain at the forefront of the next wave of mobile technology.

5G research institutions at King's College London and the Universities of Surrey and Bristol, have been awarded £16m to develop the cutting-edge 5G test network which will bring academia and commercial companies together to trial the technology and make sure people and businesses can realise the benefits sooner.

This test network will trial and demonstrate the next generation of mobile technology and is the first part of a four-year programme of investment and collaboration in the Government's new 5G Testbeds and Trials programme.

The universities will work together to create three small-scale mobile networks which together will form the test network. Each network will have a number of the elements expected in a commercial 5G network - including mobile signal receivers and transmitters and the technology to handle 5G signals - to support trials of its many potential uses.

Other academic institutions, industry and local authorities will also be able to bid for further funding to be part of this programme from 2018/19 onwards. Further details on opportunities and the funding available are published in the prospectus.

UKCRIC

The UK Collaboratorium for Research in Infrastructure & Cities (UKCRIC) will provide leadership and support for the development and growth of a coordinated and coherent, world class, UK-based national infrastructure research community, spanning at least 14 universities. It will engage government, city and commercial policy makers, investors, citizens and academia in a joint venture that drives innovation and value creation in the exploitation of services provided by national infrastructure. Through central coordination, providing a focal point for knowledge transfer, UKCRIC will support a step-change in the nation's approach to infrastructure investment. It will also develop a commercial resource that has considerable export potential for an international market that is valued at $57 trillion in the period up to 2030.

UKCRIC will understand how to make the system of systems that constitutes the nation's infrastructure more resilient to extreme events and more adaptable to changing circumstances and contexts, and how it can provide services that are more affordable, accessible and usable to the whole population.

PETRAS

The PETRAS Hub has funding for the creation of a number of demonstrators. The project is still debating what form these should take.

University of Bristol

With the Mumba project team's move to the University of Bristol, a new ICS testbed is being set up that will include multiple field sites and industrial processes to support research on security of industrial control systems, including both legacy and non-legacy devices and Industrial Internet of Things (IIoT).

3. International Facilities

Holm et al [3] present an overview of international facilities as at the end of 2015. They identify 30 testbeds that were either planned or in operation, almost half of which were in the US. They cite Siaterlis et al [4] who present the following criteria that cyber security testbeds should fulfil:

- **Fidelity:** to be as accurate a representation of the real system as possible
- **Repeatability:** repeated runs should give consistent results
- **Measurement accuracy:** observing runs should not perturb the outcome
- **Safe execution of tests:** the effect of a test should be contained within the testbed

These are reasonable requirements to expect of any testbed facility.

The iTrust Water testbeds (Singapore) are small-scale networks within a controlled laboratory environment, composed of a small-scale water distribution network (WADI) and a treatment plant (SWaT). The testbeds are used for security analysis for water distribution networks, to assess detection mechanisms for cyber and physical attacks, as well as to understand cascading effects to other connected systems. The [iTrust] Internet of Things Automatic Security Testbed (Singapore) is a small-scale laboratory composed of GPS simulator, Wi-Fi localization simulator, time simulator, movement sensor, to simulate the different environmental conditions in which IoT devices operate. The testbed supports standard and context-based security testing and analysis for IoT devices under real conditions against a set of security requirements.

Power-Cyber (USA) is a smart grid testbed with the purpose to perform vulnerability assessment (i.e inspect weaknesses within the infrastructure), design mitigation methods, and develop cyber-physical metrics (i.e metrics combining cyber-physical properties), cyber forensics tools (explore ways to detect cyber-attacks specific to industry protocols and field devices), and secure models (exploration of innovative security approaches).

The University of Illinois at Urbana Champaign has developed the Cyber-Physical Experimentation Environment for Remote Access Distributed ICS (CEER). A summary of this effort (included verbatim here) has been extracted from: https://iti.illinois.edu/research/energy-systems/cyber-physical-experimentation-environment-radics-ceer

"*The goal of this project is to provide a testbed on which prospective techniques and tools can be developed, refined, and validated in a context with unprecedented system fidelity. We are closing the gap between needs and state of the art through a testbed, CEER, that is innovative in several ways.*

CEER brings to the ICS domain for the first time production quality software to flexibly (and remotely) define experiments, configure testbed resources, and run experiments. It brings the fruits of state-of-the-art modeling of grid systems to provide synthetic but realistic dynamic grid state. It brings cutting-edge applied research in temporal coordination of real devices, device emulation, and simulators of diverse kinds to enable creation of experimental topologies that are much larger than the ensemble of physical ICS devices in the testbed. CEER brings best-of-breed ICS system instrumentation and monitoring technology to enable users to closely track the results of testing. It will be able to accurately represent the smart grid interactions from generation, transmission, and distribution. It will also support high-fidelity exploration of assets in each of these domains, including, but not limited to, generation assets, grid components in transmission and distribution substations, control center operation, and advanced metering infrastructure."

An approach taken by the colleagues behind this testbed is to use high-fidelity simulators of the "physical world", which allows for close-to-true impact of cyber- attacks to be accounted for.

The US National Institute of Standards and Technology (NIST) is developing a cybersecurity testbed (see Fig. 2 [2]).

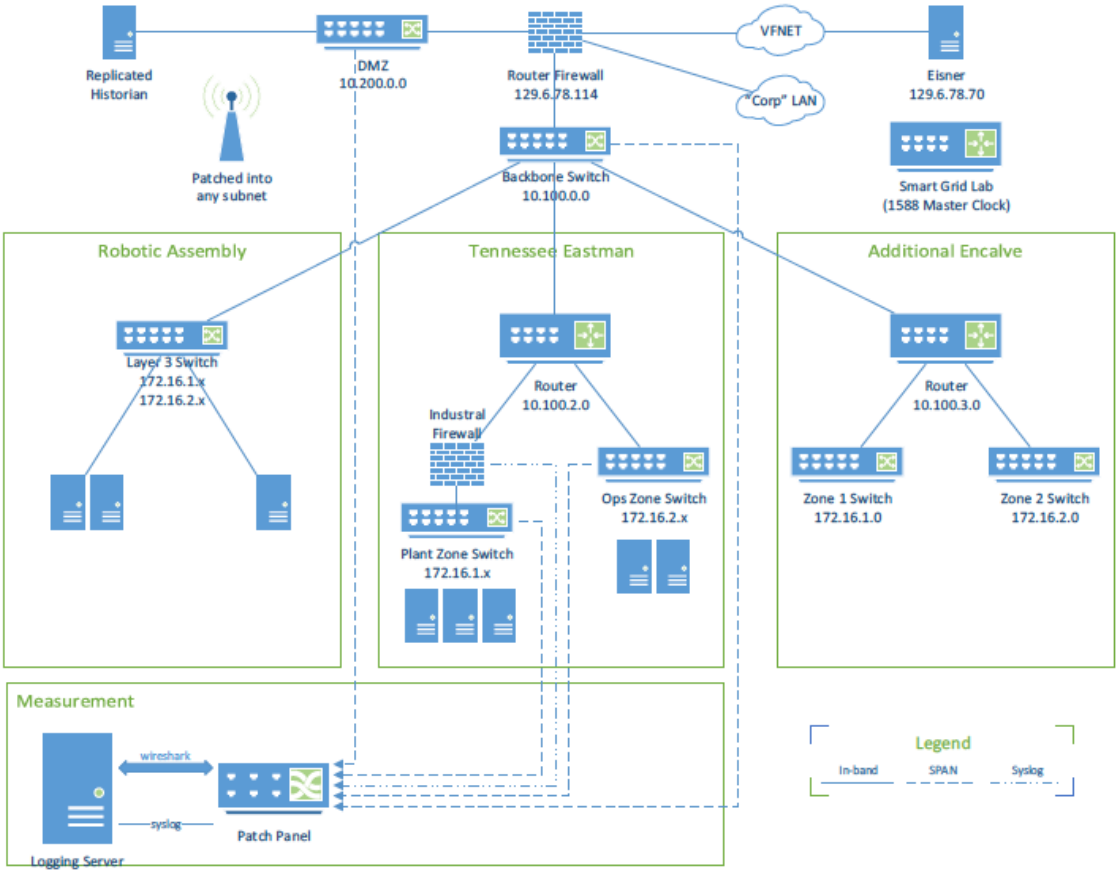

Figure 2: The NIST Testbed

The aim is to measure the effect of prevailing standards and guidance on the performance of control systems. The testbed is designed as a series of enclaves that address different industrial sectors. The testbed uses simulation where appropriate with Hardware-in-the-Loop (HIL) components simulating the interfaces between sensors/actuators and the controller. The different enclaves allow study of continuous processes (such as chemical manufacture), discrete processes (such as automotive assembly) and hybrid processes (such as pharmaceutical manufacture). Performance is measured using appropriate technical performance indicators for the processes.

The Department for Business, Energy and Industrial Strategy Civil Nuclear Team is in the planning phase regarding an upcoming joint exercise with Estonian MOD officials. The Estonian offer is a network defence exercise scenario making use of a fully-equipped cyber test range in Tallinn, and will involve participants from across the civil nuclear sector. The National Cyber Security Centre will also have involvement in the exercise using the Estonian Defence Forces Cyber Range, consisting of a simulated office network consisting of typical servers and workstations as well as facilities support systems will be implemented.

Hitachi are developing a Security Training Arena (SeTA) at their Omika Works in Japan. The emphasis of this centre is to train operators how to deal with cyber incidents in a nuclear power plant. They plan to run joint exercises with the UK (and possibly US) in 2018. They have had preliminary discussions with Imperial College London and Royal Holloway University of London as potential academic partners in this programme.

The largest security cluster in Europe is situated in The Hague Security Delta. In 2015, they published a proposal for a national, multi-sector testbed [5]. At the time of writing, they are still recruiting partners to assist in the construction of the facility; the initiative is supported by TNO, KPN NV and the Municipality of The Hague. The minimum requirements for the Dutch national testbed are as follows:

- The platform should host test labs for multiple, different critical infrastructure sectors
- The platform should generate knowledge that can be used to create solutions for critical infrastructure equipment
- It should be available for training of information security staff on threats and exploits
- The testbed should facilitate the creation of a network of highly qualified information security staff
- The testbed facility should periodically produce confidential reports about newly discovered threats and vulnerabilities
- The testbed facility should provide open and freely available security reports with the security solution
- The testbed facility should turn security requirements into new industry standards
- The testbed facility should educate critical infrastructure companies in best practices and lessons learned from across all sectors
- The testbed facility should establish cooperation and information sharing among participating partners

These requirements overlap significantly with the ambition that we outlined in Section 1 above.

4. Design Issues and Lessons Learnt

The key design issues and lessons learnt from the construction of the Lancaster testbed [1], which also find echoes in the other cited papers are:

1. The need to include, either physically or virtually, a diverse range of different devices (vendors and versions)
2. The need for scale to provide faithful representations of real systems
3. Appropriate mechanisms to manage the complexity of the infrastructure

Diversity

An effective testbed should be able to mimic a variety of ICS setups. Key questions include:

1. Selection of devices and protocols for inclusion;
2. Providing different configurations of devices/manufacturers typical in ICS settings; and
3. Balancing device and protocol diversity against other requirements, such as the implementation of the physical process itself.

Experiences within the Lancaster testbed have highlighted that [1]:

- Device and technology selections should be market-driven;
- Field sites in a testbed should represent different real-world scenarios such as homogeneity and heterogeneity of vendors as well as combinations of legacy and non-legacy devices;
- Process diversity can help model stealth attacks that exploit physical aspects of the process but that such process diversity may be traded-off in favour of diversity of devices and field sites.

Scale

Software does not provide simulations of many essential types of devices, i.e. from different vendors or the same vendor but distinctive versions. The accuracy and reliability of such simulations in mimicking real-life operations also remain an issue. Therefore, while the cost of physical equipment can be a limiting factor, the benefits it can bring in relation to experimental rigour is an overriding constraint. On the other hand, virtualisation and VLANs can provide ease of integration and scaling of the testbed infrastructure [1].

Complexity

Although the underlying architecture may be complex and involve a number of network zones, this should be as transparent to the user as possible. Transparency can be achieved by providing a single point through which access to and extraction of data from the different zones can be managed. A second lesson learnt by the Lancaster team [1] is the necessity to create and maintain good documentation of the testbed as it evolves.

Further Lessons

The NSF report on Cybersecurity Experimentation of the Future [6] provides a detailed roadmap for the development of future experimentation infrastructure over the near-term (3 years), mid-term (5 years) and long-term (10 years). The report also reviews the experience of 46 US-based experimental facilities.

The top 5 recommendations from the report are as follows:

- Focussing on multidisciplinary experimentation drawing on both “hard” sciences and social science will have the greatest impact in accelerating cybersecurity experimentation in the near term.
- The ability to accurately represent fully reactionary complex human and group activity in experiments will be instrumental in environments that realistically represent real-world systems.
- Creating open standards and interfaces is a mid-term priority.
- Research and development using the latest advances in data science is needed to create reusable, extensible, validated experiment designs.
- Research infrastructure must be usable by a broad range of researchers and experts, not just restricted to computer science researchers.

5. Linking Testbeds

Most UK academic institutions and research centres are provided connectivity by Janet, a high-speed, secure and reliable world-class network. Janet provides at least a 10Gb/s physical link and a Class-B IP address pool, enabling all types of Internet services within UK academic campuses, including low-latency Voice over IP (VoIP). However, experimental lab facilities and research test networks are significantly constrained in taking advantage of the Janet infrastructure. In order to avoid security and Quality of Service (QoS) related threats to the Janet network, research lab facilities are, in most cases, disconnected and rely on external multi-megabit ADSL lines via local ISP providers. These limitations not only constrain research capabilities within these institutions, but also impair national and international collaborations that require high-speed connectivity amongst collaborating partners.

Another key factor that limits the research capabilities, quality and effectiveness is the limited availability of resources within academic institutions and research centres. Setting up an experimental lab facility or research test network is extremely expensive especially in the ICS and SCADA domain due to the need for expensive devices/equipment. The non-availability of state-of-the-art experimental resources significantly limits research potential of individual academic institutions.

The aim for linking testbeds is to enable all partner institutions with leading edge research capabilities, experimental lab facilities and test networks by sharing resources over secure and reliable high-speed Janet infrastructure. The team at QUB have recently proposed an approach which is unique of its kind by inter-linking lab facilities of all universities across the UK as shown in Figure 3. This proposal does not just focus on linking ICS and SCADA facilities but proposes a more general network of testbeds.

As highlighted on the right in Figure 3, the sharing nature will enable all participating institutions to benefit from the same search facilities and have access to test/experimental networks which they were lacking individually. The proposed research network will be built upon Janet’s network infrastructure using configurable multi-gigabit VPN tunnels, providing connectivity of up to 10Gb/s amongst the partners, while facilitating strict isolation from each node’s main campus network; a similar architecture is already under evaluation to allow external connectivity to the Lancaster testbed. Centralised network administration and management will provide project specific configuration of the network (topology, bandwidth) and external connectivity to national and international partners, and the Internet, via a secure gateway using Janet and third-party ISPs. The

baseline architecture will be laid out as such that the network can be scaled to expand beyond the current partners, capable of servicing the UK academic research community for many years ahead.

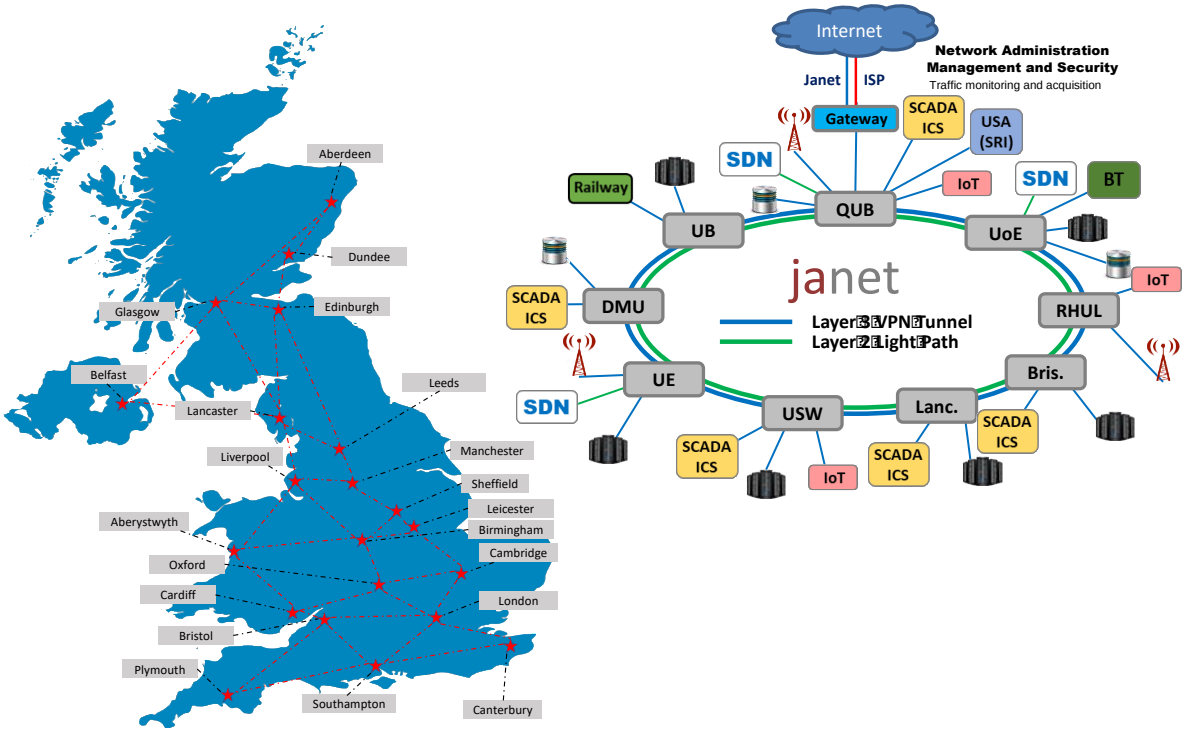

Figure 3: A Proposed UK Network

Direct Benefits to UK Universities and Research Centres

The academic and industrial partners will be able to take immediate and full advantage of the proposed connectivity by providing them: (i) an extended research network infrastructure for experimental studies, (b) access to the collective pool of state-of-the-art expensive technologies, tools, testbeds and datasets, which are currently only available to the owning institution, (c) provide the necessary infrastructure for generating research specific traffic samples, log files and other specialist datasets, and the facility to share a large repertoire of existing datasets amongst the partners, (d) limited access to specialist networking skills and domain knowledge by taking advantage of the network and its dedicated staff.

The scale and diversity of the proposed research network and test facilities provides unique research opportunities for end users, such as enterprises and corporations relying on large IT networks and IT security. The proposed research network will provide numerous benefits for partners by sharing or providing access to expensive and rare resources, access to more realistic experimental environment and improving research collaboration.

QUB has an extensive experimental network and test lab infrastructure closely coupled to a system penetration test and training lab. The inter-linked research network will extend that test capability and provide a more realistic and distributed ICS system to experiment with. In addition to the

benefits of scale that will accrue to existing RITICS testbeds, such as the one at Lancaster, the network will also benefit other new RITICS partners. For example, the planned testbed at Bristol will be linked into the network as well as those university facilities currently supported by Airbus. The collaborative project between the University of South Wales (USW) and Airbus Defence and Space called SCADA Cyber Security Lifecycle (SCADA-CLS), is targeting the development of a cyber forensic capability for SCADA process control systems. The inter-linked research network will provide an extended ICS network that USW can effectively utilise for forensic/incident management triage process modelling, and the development of SCADA forensic tools for data acquisition, incident management and situational awareness, using SCADA test facilities at QUB and its FP7/H2020 partners. De Montfort University's (DMU) CYRAN cyber range technology, which will be directly accessible by all partners, provides a platform for cyber-attack/defence scenarios for experimental research and for educational games that include physical artefacts such as PLC controlled production lines and filtration systems. DMU will be able to extend the CYRAN capability, accessing PLC controllers at QUB, USW and European partners. SCADA and other types of ICS related large datasets can now be generated, taking advantage of the additional physical resources from the partners' testbeds. This data is directly relevant to existing projects within DMU on SCADA Forensics, undertaken with Airbus Group Innovations as well as research on Privacy Metrics and Incident Response management.

By combining many test networks with unique properties, more general cyber security research projects will also benefit. Log files from next generation firewalls (ngFW) within the proposed research network will be used to analyse malicious traffic in LAN networks; working with multiple ngFW data will enable the analysis across a wide area network. A key benefit is the generation of large log files within the experimental network without being constrained by the privacy and ethical challenges of live campus networks. Dedicated monitoring and interception technology within the proposed research network will provide advanced traffic visibility and packet processing capability for many projects. The proposed research network will allow partners (a) to further analyse repetitive external attacks to their IT infrastructure by replaying attack patterns, (b) use cross-site test capabilities to undertake stress and penetration testing on new or experimental security and network appliances, and (c) assess new cyber security architectures and threat mitigation strategies on corporate networks and websites.

Dataset and test traffic generation and sharing is one of the most important and challenging topics in network and cyber security. Available datasets such as intercepted traffic are constrained and in most cases relevant to a specific type of threat. Privacy and ethical considerations prevent the use of any intercepted data, such as from a University campus network. Further constraints are that malware, APT and DDoS related projects requires fresh datasets and traffic containing targeted threats in order to understand traffic patterns related to threats, and for optimising detection algorithms such as machine learning classifiers. The proposed research network brings together highly diverse test networks at a scale and the traffic capacity of a large network, providing a unique opportunity for generating tailored datasets and sample traffic.

Transport experimental lab facilities are quite expensive to establish and only few universities have advanced testbeds. The interconnected research network will be of significance for improving collaboration amongst academic institutions and effectively sharing their transport lab facilities. Birmingham Centre for Railway Research and Education (BCRRE) of the University of Birmingham (UoB) has significant experimental lab facilities for research in addressing grand system-wide as well as component level challenges. UoB railway research covers various aspects including safety, operations and management, data integration and cyber security. Recently, the UK Rail Research

and Innovation Network (UKRRIN) research centre has been established for supporting new innovations in rail transport. UKRRIN aim is to bring together existing facilities at different academic institutions and accelerate innovation and new product development in the rail industry. As part of UKRRIN, UoB will carry out research in digital rail systems covering cyber security, traffic management and railway condition monitoring and sensing. University of Newcastle (UoN), Loughborough University (LU) and University of Huddersfield (UoH) within UKRRIN will collaborate on high value rolling stock systems, asset optimisation and through-life management and energy management. Whereas, University of Southampton (UoSA), University of Sheffield (UoS), University of Nottingham (UN) and Heriot-Watt University (HWU) are carrying out research on railway infrastructure within UKRRIN. The proposed interconnected research network will be the medium enabling all partners of UKRRIN to collaborate effectively and share experimental resources.

Proposed System Architecture

The proposed inter-linked research network would be developed in multiple phases, taking advantage of the available Janet connectivity and spare bandwidth capacity of the academic institutes.

Figure 4 outlines the overall network and testbed architecture amongst the partners. An initial phase would target the development of the basic overlay architecture on top of the existing layer3 Janet connection via multi-gigabit VPN tunnels and the establishment of the network with the necessary network administration and management tools and support resources. A control centre with network administration and management tools would be established, responsible for the administration and management of the links amongst the partners, Janet and the external connectivity to the Internet. Phase-2 development would provide additional physical link capacities and external connectivity to international and industrial partners.

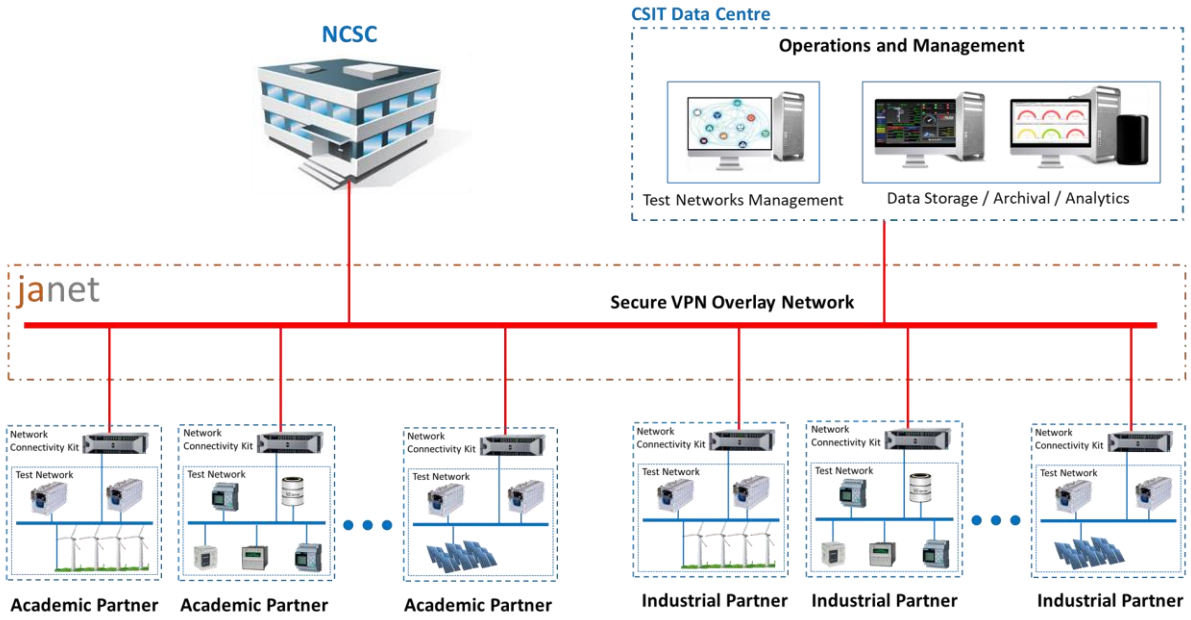

Figure 4: The Proposed Architecture

Janet layer2 Light Path provides the lowest cost and highest-bandwidth connectivity, for the proposed network it also introduces significant challenges providing the necessary layer3 network infrastructure and supporting cybersecurity (malware, DDoS, cloud), IoT, and Industrial control

related test labs. Numerous SDN and cloud network testbeds can take full advantage of the layer2 bandwidth such as streaming terabytes of data between big-data labs.

Requirements for Secure Inter-linking of Diverse Testbeds

The objective is to develop a platform, based on a secure overlay network architecture, for interconnecting various academic and industrial testbeds into a larger UK wide research network. As depicted in Figure 4, such a private overlay network approach has three basic requirements: (i) network connectivity kit, (ii) centralized operations and management and (iii) high speed Janet network.

Network Connectivity Kit

The network connectivity kit enables remote testbed sites from partners to be connected to the private overlay network as shown in Figure 4. The solution is scalable and new testbeds can be easily integrated within the network without major technical support. To become part of the interconnected physical testbed infrastructure, each academic or industrial partner should be provided with a network connectivity kit or rack-mounted kit. The basic architecture of the rack-mounted kit is shown in Figure 5 and consists of:

- A Firewall/Router/VPN which will be managed from the CSIT Test Network Management centre.
- A distribution switch that has port mirroring capabilities to permit traffic capture.
- Traffic data storage capability. Terabytes of network traffic data may need to be captured and stored for later analytics.

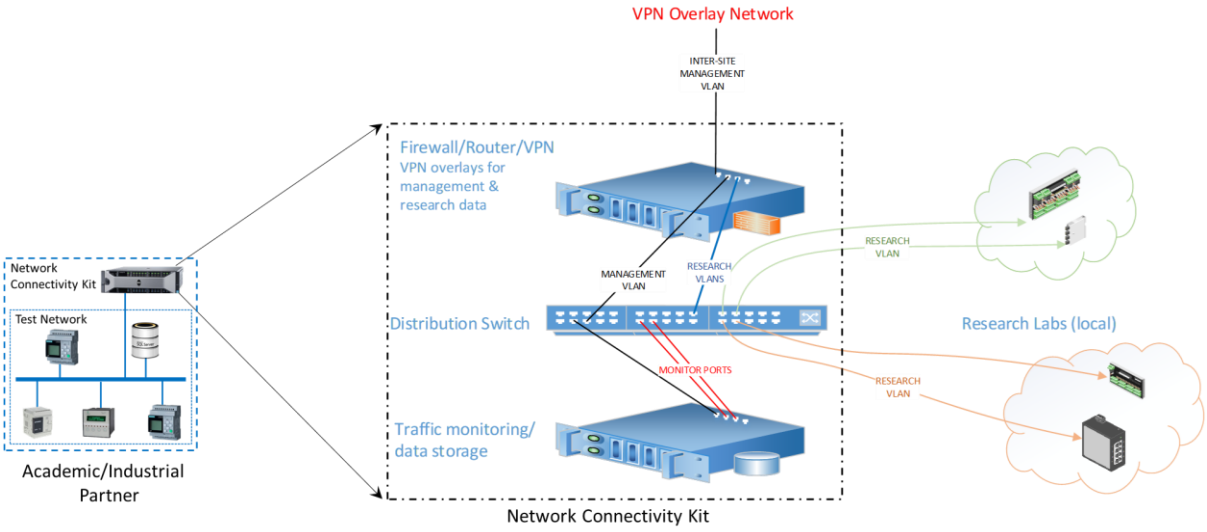

Figure 5: Architecture of the Network Connectivity Kit

The network connectivity kit has a VPN client and appropriately dimensioned communication and storage hardware. It is tailored for the proposed research network comprised of appliances for a traditional IP network and an SDN network, capable of supporting advanced firewall, and VPN tunnel with VLAN segregation capability.

Operations and Management

The proposed research network has centralized management for managing connectivity between distributed testbed sites, network access control and data acquisition. It also has a data-set (sampled data and traffic patterns) repository with post processing, indexing and access control. An effective

management and administration structure is essential to ensure the success of the proposed research network and its efficient utilisation by the partners and the wider research community.

The centralized operations and management system will be hosted at the Centre for Secure Information Technologies (CSIT) data centre. The proposed research network will be managed by Queen's University Belfast, as part of CSIT operation and management infrastructure, in collaboration with all partners.

High speed network

The high speed link capacities will be leased from Janet which will act as the backbone and fabric of the proposed research network. The majority of cost in the development of proposed research network is associated with the leasing of communication links from Janet and providing the network connectivity kit to each partner. Going beyond the current QUB proposal, it should also be considered how 4G technologies, as used at Lancaster, can be incorporated into the network in a secure, reliable, and managed format. There could be a further extension towards PSTN/GSM services, in which legacy dial-up technologies may also be applied.

Use Case Examples

Inter-linking experimental resources from academic and industrial partners makes the proposed research network quite heterogeneous consisting of diverse testbeds in all different research areas. Based on the research topic, a partner can request resources in a specific domain from control operations and management centre. The Control centre will create a secure segregated VLAN with dedicated experimental resources based on the request. The allocated resources can then be exploited by the partners to experiment and determine effectiveness of their developed technologies and research tools. To illustrate the utility of the network, this section presents two ICS use cases where the proposed research network can be utilized.

Distributed Intrusion Detection and Prevention

An Intrusion Detection System (IDS) monitors a network/system for malicious activities or violation of policies and raises alerts. Whereas, Intrusion Prevention System (IPS) complements IDS by also taking defensive actions when a malicious activity is detected. Several academic institutes and research centres are activity involved in IDS/IPS research to improve detection efficiency and effectively handle emerging threats. NIST published recommendations that IDS/IPS systems should be hybrid, distributed in nature, have decentralized decision making and centralized management and refinement of detected events. The hybrid IDS/IPS systems perform both host-based monitoring as well as network-based monitoring for malicious activities detection. The distributed nature suggests multiple sensors to be deployed in system instead of relying on a single sensor for redundancy and better malicious activities detection.

Several ICS systems are distributed in nature e.g., power systems. To investigate IDS/IPS technologies for a distributed ICS network, a partner can request resources from the control centre of proposed interconnected research network. The partner will benefit from not having its own but utilizing shared ICS testbeds from other partner institutes. This will enable the partner to continue research in this topic even if it is lacking equipment.

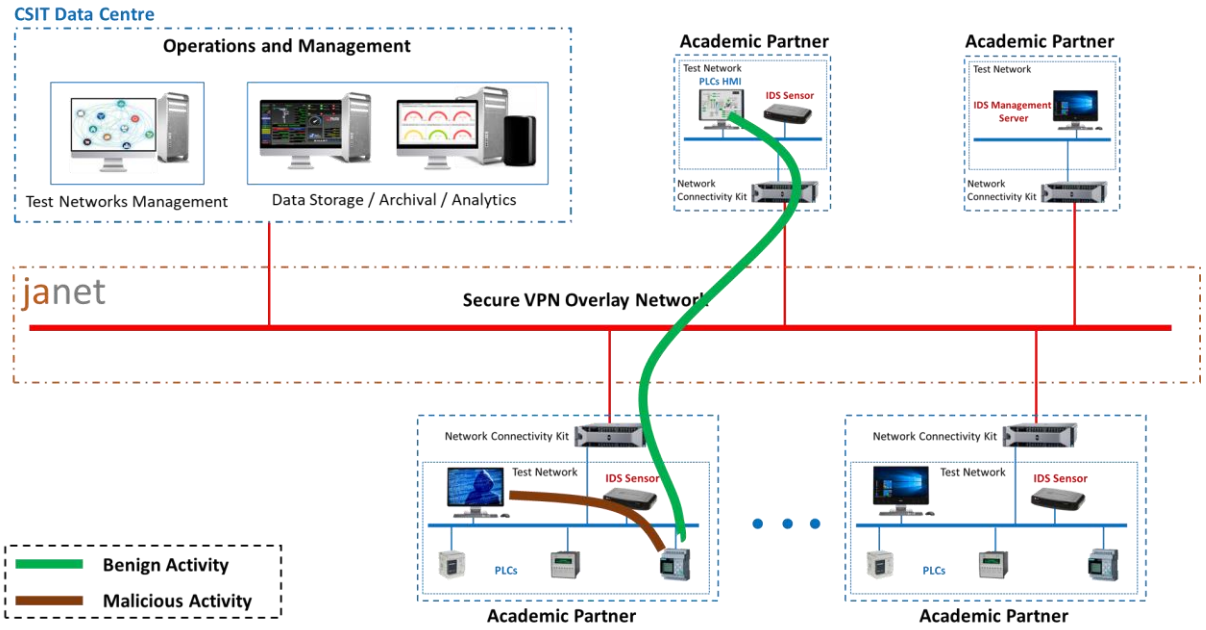

Figure 6: The Distributed IDS scenario

Realistic Experimental Power Systems Platform

The proposed research network can be used to conduct research in a more realistic distributed experimental platform. E.g., power systems are highly distributed nowadays due to development of renewable and green energy sources (e.g., wind farms, solar panels, etc). This trend is becoming more and more common and green electricity sources are predominantly located at geographically isolated areas. Several universities are conducting research on distributed generation and transmission, microgrids and substations including Queen's University Belfast, Manchester University and Strathclyde University. Distributed generation and integration into main grid takes benefit from synchrophasor technology. Synchrophasor technology includes a control centre that receives GPS timestamped electrical measurements from microgrids (or distributed generators) and main grid. Control centre performs processing to determine if a microgrid is synchronized with the main grid and can be safely connected to contribute electricity to the main grid. Normally, microgrids can dynamically connect and disconnect from the main grid which increases the risk for power systems (if connected in non-synchronized state). Queen's University Belfast has a local testbed on distributed generation and specifically researching solutions to ensure safety, resilience and cyber security. Since power systems are distributed in nature, such systems need to be studied in a more realistic and geographically distributed experimental platform. As shown in Figure 7, the proposed interconnected research network can provide such a distributed experimental platform by combining resources available at other partners as well. This will enable Queen's University Belfast to experiment with any newly developed safety and security technologies in a more realistic distributed power system. Further, partners interested to conduct research in this area but lacking resources can also benefit by accessing shared resources from other partners.

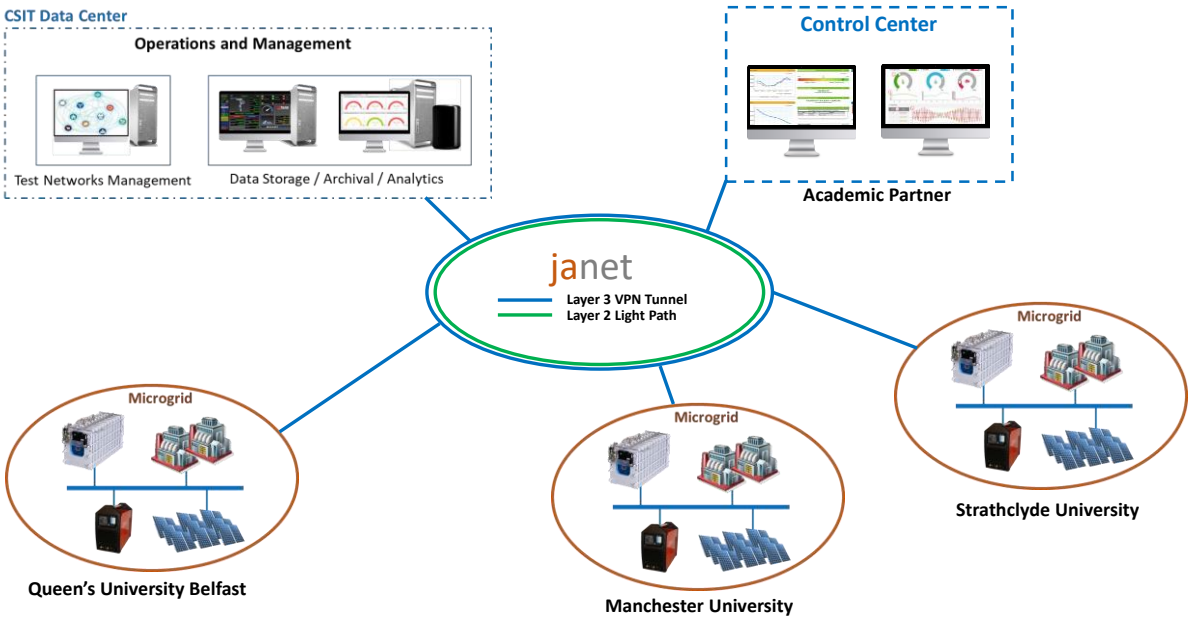

Figure 7: The Distributed Power scenario

6. Future Directions/Conclusions

This white paper envisages an inter-linked network of open testbed facilities that will support the growing RITICS community to:

- better understand the interdependencies between different sectors
- better understand the similarities and differences between Information Technology (IT) and Operational Technology (OT)
- test and prepare for targeted and untargeted attacks
- provide training to close the skills gap
- validate various theories about how to deal with new and unknown threats
- extend understanding of system-user relationships across an array of sectors

The proposal from RITICS is ambitious and requires considerable investment to realise but recently announced NCSC funding will allow the development of a prototype in Belfast. We feel that creating such a national facility will allow the UK research community to meet the criteria outlined above and repeated below:

- **Fidelity:** to be as accurate a representation of the real system as possible
- **Repeatability:** repeated runs should give consistent results
- **Measurement accuracy:** observing runs should not perturb the outcome
- **Safe execution of tests:** the effect of a test should be contained within the testbed

and place us in a leading international position for this work.

References

[1] B. Green, A. Le, R. Antrobus, U. Roedig, D. Hutchison and A. Rashid: **Pains, Gains and PLCs: Ten Lessons from Building an Industrial Control Systems Testbed for Security Research**. CSET @ USENIX Security Symposium 2017.

[2] R. Candell, D.M. Anand and K. Stouffer: **A Cybersecurity Testbed for Industrial Control Systems.** ISA Process Control and Safety Symposium, 2014.

[3] H. Holm, M. Karresand, A. Vidstrom and E. Westring: **A Survey of Industrial Control System Testbeds**. NordSec 2015, Lecture Notes in Computer Science, 9417, Springer Verlag, 2015.

[4] C. Siaterlis, A. Garcia and B. Genge: **On the use of emulab testbeds for scientifically rigorous experiments**. IEEE Communications Surveys & Tutorials 15(2), 2013.

[5] The Hague Security Delta: **Securing Critical Infrastructures in the Netherlands: Towards a National Testbed**. https://www.thehaguesecuritydelta.com/images/HSD_rapport_Testbed_EN.pdf

[6] D. Balenson, L. Tinnel and T. Benzel: **Cybersecurity Experimentation of the Future (CEF): Catalyzing a New Generation of Experimental Cybersecurity Research.** http://cyberexperimentation.org/files/2114/5027/2222/CEF_Final_Report_Bound_20150922.pdf