Report of Short Term Scientific Mission of COST CA15127-RECODIS

STSM Topic: **Network Resilience for Communication Networks that support Cyber-Physical Systems**

STSM Applicant:	Dr Paul Smith (MC Member), AIT Austrian Institute of Technology, Austria
Host:	Prof David Hutchison (Action Vice Chair), Lancaster University, UK
Period:	6th – 10th February, 2017
Working Group:	WG5

Purpose of the STSM

The aim of this STSM was to investigate potential avenues of new research enquiry for communication network resilience that support cyber-physical systems. This activity aims to contribute to the existing work in the RECODIS WGs, which is oriented toward network and information resilience. During the STSM, the applicant conducted a number of discussions with researchers at Lancaster University on topics that are related to communication network resilience. Based on the experience of the applicant, the resilience of communication networks that underpin the smart grid – a cyber-physical system – was considered.

Smart Grids and Network Resilience

Smart grids are future energy systems that include a much larger Information and Communications Technology (ICT) and Supervisory Control and Data Acquisition (SCADA) component than is currently used in power systems [1]. These new ICT and SCADA systems enable new energy services and support the integration of Distributed Energy Resources (DERs), such as photovoltaics and wind turbines. Example energy services include smart metering, demand-response schemes, and remote voltage control. The resilience requirements on the communication infrastructure are varied. However, in general, for control systems, availability and integrity objectives tend to take precedence over confidentiality requirements. This is reflected in academic literature that focuses on timing [2] and data integrity [3] attacks to power systems. (The obvious exception is services that require data to be collected from consumers, such a load profiles, wherein confidentiality (privacy) is a primary concern.) In addition, the performance (Quality of Service) of communication networks can be critical, e.g., for networks that implement safety functions in substations [4].

Cyber-physical Systems Design for Resilience

A major concern is that cyber-attacks to these future energy systems could result in operational consequences, e.g., power losses, voltage violations, equipment damage, and safety-related incidents. A major blackout occurred in the Ukraine in December 2015, caused by a cyber-attack, brought this issue into sharp relief [5]. In the future, such attacks could be more prevalent, as energy systems become more open (in order to integrate new services and actors) and interconnect potentially insecure devices. Therefore, a challenge for operators, network planners, and solutions providers (the designers of future energy systems) is to plan for their systems to be secure and resilient to these new forms of attack. This is a non-trivial task, given the increasing complexity of the systems and the sophisticated and persistent nature of the threat.

In this context, resilience – the ability of a system to provide an acceptable level of service in light of challenges, such as cyber-attacks, and faults – is a key system property. In others words, future energy systems, and associated communication networks, need to absorb the effects of an attack (degrade gracefully); recover rapidly; and be survivable (collapse in a well-defined manner). This is both from a cyber (ICT and SCADA system) and physical (power) systems perspective.

Arguably, there are three main technical, i.e., not, for example, organisational or regulatory, approaches to ensuring the security and resilience of energy systems:

1. To design the physical power system to be robust to the effects of cyber-attacks, e.g., from a topological or structural perspective (considering line lengths, number of renewables that feed in, etc.);

2. Employ control strategies that aim to improve the robustness and resilience of energy systems in the presence of attacks, e.g., by adopting more conservative (less efficient), but safe, control behaviour; and
3. Make use of cybersecurity solutions, such as encryption, firewalls, intrusion detections systems, etc., and secure ICT architectures, whose purpose is to prevent attacks being successful (defensive security) and to remediate their effects (reactive security).

Of course, these three approaches will be used in combination. For example, microgrids are commonly cited as an approach to improve the availability of energy systems to faults or perturbations in medium voltage networks – a topological (or structural) and control arrangement. Recent research in the EU-funded SPARKS project[1] has begun to examine the interplay between cybersecurity intrusion detection systems and resilient control strategies [6].

In this context, future energy systems designers must determine a security and resilience configuration, given a set of constraints and potentially contradictory requirements. Some considerations (design constraints) that are necessary to consider include the configuration of an existing infrastructure – this is not a greenfield; financial cost; regulatory requirements; operational (organisational) processes; renewable energy (carbon reduction) targets; and market demand. These factors must be reconciled with the need to ensure the security and resilience of future energy systems to cyber-attacks. An understanding of the risks associated with such attacks plays an important role. More specifically, an understanding of the likelihood of a threat (a function of the system's vulnerability and the threat characteristics) and impact is needed. This understanding is necessary to prioritise (and justify) design decisions.

Arguably, we lack suitable approaches to measuring the security and resilience of cyber-physical systems, such as future energy systems. Metrics are essential in the design process. What is required is a metrics framework that acknowledges the interplay between the measurable properties of different sub-systems. Also, it is necessary to acknowledge the multi-dimensionality of measures – there are many ways that the security, resilience and operational behaviour of a system can be measured, e.g., depending on stakeholder interests. A well-designed approach to measuring these aspects can inform the overall planning process, for example, to identify which solutions provide the most benefit, in terms of security and resilience. Existing research tends to focus on communication network resilience, e.g., from Sterbenz et al. [7], or on physical (control) systems aspects [8] – little consideration has been given to measuring the interplay between the resilience of communication networks and the cyber-physical (control) systems they support. In recent work, we have begun to explore this issue [9].

Given a suitable framework for measuring the resilience of cyber-physical systems, which can identify the design decisions for resilience that provide the most benefit, it is necessary to rationalise those decisions with respect to the risk (how likely is the challenge and its impact) and their cost of implementation. To this end, a future avenue of research could investigate the relationship between a resilience metrics framework and decision theory – specifically, game theory [10]. The high-level idea is to model the defender behaviour in a game using the design decisions that have been evaluated for their efficacy in the metrics framework, including their payoff (as an improvement in resilience), and their cost of

[1] The EU-funded SPARKS Project: https://project-sparks.eu

implementation. Meanwhile, attacker behaviour could be modelled in the game – the attacker payoff being modelled as the impact to the cyber-physical system – with different challenge types and strengths being considered. The application of game theory to support risk assessment is being considered in the EU-funded HyRiM project[2], in which AIT and Lancaster University are both partners. It is our intention to follow-up on this line of enquiry.

Cyber-Physical Systems Resilience Management

The research community is investigating the potential benefits of novel network paradigms, such as Software-Defined Networking (SDN) and Network Function Virtualization (NFV). The primary motivations for these paradigms include cost-savings, the rapid introduction of novel network services, and more straightforward network management. Of course, these paradigms can be used to support network resilience to large-scale disasters. Cloud computing technologies (i.e., virtualized datacentres) are the primary means the research community has considered the deployment of network functions. However, Fog computing is emerging as another means of deploying network functions. Fog computing (or the Fog) aims to take advantage of computational and network resources that are located close to the network edge, e.g., wireless access points, set-top boxes, etc., in order to improve the performance of network services. For example, content distribution is a service that could be improved using this technology. At Lancaster University, there is ongoing research on the challenge of resource identification and allocation for the Fog – in other words, identifying, from a set of available resources, those that could be used to deploy a service. In this context, network functions are executed in containerized environments, such as Docker[3].

There are similar initiatives in the smart grid context: for example, in the EU-funded Nobel Grid project[4], a novel device called the Smart Meter eXtension (SMX) is being developed. An SMX resides alongside (and is connected to) the traditional metrology meter and can be used to support novel energy services, such as demand-response schemes. In addition to being connected to a smart meter, an SMX can connect to the Internet and with devices in the home. The SMX acts as an interface between electricity service providers (Distribution System Operators (DSOs), aggregators, etc.) and controllable devices (loads) within the home or facility. Energy services execute in a containerized environment, in a similar manner to communication network services in the Fog context.

In the smart grid, demand-response schemes aim to utilize flexibility in generation (battery storage) and load (air conditioning systems), in order to mitigate the reduced availability of supply (in the presence of inflexible generation, such as solar) or to maximize the utilization of low-carbon energy when it is available. A major task is to identify flexibility that can be used for demand-response schemes using load profiling and state estimation techniques, for example. As the interface to this flexibility, the SMX is a key device for supporting demand-response schemes. In many ways, this task of identifying flexibility is similar in nature to the identification of available resources in Fog computing.

During the STSM, the potential benefits of bringing these two domains closer together for resilience purposes was discussed – the cyber (network resources in the Fog) and the physical (energy flexibility in the smart grid). For example, one could envisage a scenario in

[2] The EU-funded HyRiM Project: https://hyrim.net/
[3] Docker: https://www.docker.com/
[4] The EU-funded Nobel Grid Project: http://nobelgrid.eu/

which a certain amount of flexibility is required for the stability (resilience) of the electricity network – perhaps loads need to be shed, in order to mitigate an under frequency situation. A load profiling scheme, using historical data that has been collected via a set of SMX devices, has identified locations (e.g., households or large buildings) where this flexibility exists. However, a number of these locations are not reachable because of communication network problems, e.g., caused by one of the forms of disaster considered in RECODIS, resulting in demand-response messages (requests to shed load) not being communicated. The physical locality of this flexibility is important: i.e., it is not possible to utilize flexibility in a geographically distinct region to mitigate a localized problem (e.g., on an electricity distribution line).

What is required in this setting is an approach to resilience management that considers requirements from (or the properties of) the communication network and the physical system under control, in order to mitigate the communication network challenge. In the aforementioned example, the resilience management scheme would seek to identify SMX devices (in a similar manner to that proposed for the Fog) that have the necessary power systems properties to effectively support a demand-response request, e.g., to shed load, and that fulfil a set of requirements for connectivity. Such a management approach might take advantage of the flexibility introduced by NFV in the Fog to improve communication network resilience, e.g., by instantiating new functionality to mitigate a challenge.

In general, what this discussion points to is a need for approaches to communication network resilience to be sensitive to (or aware of) requirements from the application (or service) level – in this case, communication network resilience should take into account the power systems requirements from the demand-response scheme application. Of course, this is not a new idea – perhaps the distinct challenge for cyber-physical systems, as opposed to purely cyber systems, is the need to take into account physical properties of the service being provided. Amongst other things, this indicates the need for new approaches to monitoring and detection, which account for both the physical and cyber behaviour of the system.

Large-scale Disasters and Cascading Effects

In December 2015, Storm Desmond caused flooding of the main electricity substation that feeds Lancaster. This resulted in the loss of electricity, over several days, to more than 100,000 people. This event demonstrated the extent to which society is dependent on electricity: with a lack of electric power, the communications networks failed, which in turn affected almost all other major essential services and functions, including education, work, transportation, sanitation, food and healthcare. In other words, the initial challenge – a flood – resulted in a loss of power and the failure of communication networks – an example of a cascading effect. (Closer inspection of this incident highlights more detailed cascading effects, which could be of interest to study.)

In the RECODIS COST Action, there has been recent activity that seeks to identify and reconcile resilience solutions that address the challenges from the different, specific challenge-oriented, working groups. This is rational, as the same (or similar) resilience solutions can be applied to different challenges: for example, NFV can be used to support the mitigation of cyber-attacks and earthquakes, alike. The aforementioned incident in the Lancaster region highlights the need to continue this line of enquiry and consider a more integrated approach to resilience that can address multiple (cascading) classes of challenge, which are part of the same overall incident.

The Role of the Human Factor for Resilience

In the HyRiM project, Lancaster University (along with others in the project) is investigating the resilience of utility systems, such as water and electricity distribution systems. Their research has a strong focus on the technical aspects, including the resilience of communication networks to new forms of advanced persistent threat. In addition to this technical focus, their activities extend into considering important human factors, and have resulted in the development of three interdependent views of resilience: Organisational, Technical, and Individual (OTI) [11]. Organisational resilience relates to organizational policies, including access control policies [12], and governance frameworks, for example, that aim to support resilience. The Individual viewpoint considers the role of employees, for example operators, in introducing vulnerabilities but also in facilitating resilience, in the context of both organisational and technical aspects.

For the most part, in the RECODIS COST Action the human is largely considered the origin of a challenge: misconfigurations and cyber-attacks are created by humans. However, considering the solutions and interplay between the OTI viewpoints as a resilience enabler could have significant benefits. We propose that considering the OTI viewpoints to support communication resilience should be taken forward in WG5 of RECODIS.

Acknowledgements

The applicant is grateful to the researchers from Lancaster University that contributed to the findings that are reported here: Matthew Broadbent, Linden Fawcett, Antonios Gouglidis, Benjamin Green, David Hutchison, Angelos Marnerides, Andreas Mauthe, Daniel Prince, Nicholas Race, Noor Shirazi, and Steven Simpson.

References

[1] P. McDaniel and S. McLaughlin, "Security and Privacy Challenges in the Smart Grid," in *IEEE Security & Privacy*, vol. 7, no. 3, pp. 75-77, May-June 2009.

[2] S. Barreto Andrade; M. Pignati; G. Dan; M. Paolone; J. Y. Le Boudec, "Undetectable PMU Timing-Attack on Linear State-Estimation by Using Rank-1 Approximation," in *IEEE Transactions on Smart Grid*, vol.PP, no.99, pp.1-1.

[3] Y. Liu, P. Ning, and M. K. Reiter, “False data injection attacks against state estimation in electric power grids,” in *ACM Transactions on Information and System Security (TISSEC),* vol. 14, no. 1, June 2011.

[4] V. C. Gungor *et al.*, "A Survey on Smart Grid Potential Applications and Communication Requirements," in *IEEE Transactions on Industrial Informatics*, vol. 9, no. 1, pp. 28-42, Feb. 2013.

[5] SANS ICS and E-ISAC, “Analysis of the Cyber Attack on the Ukrainian Power Grid,” March 2016. URL https://ics.sans.org/media/E-ISAC_SANS_Ukraine_DUC_5.pdf

[6] Parida K., Sandberg H., O’Mahony N., Kupzog F., El-Din Mady A., McLaughlin K., Kang B.: “High-level Design Documentation (for Grid Control System) and a Deployment Architecture for the Monitoring Solution” https://project-sparks.eu/publications/deliverables/

[7] J. P. G. Sterbenz, D. Hutchison, E.K. Çetinkaya, A. Jabbar, J.P. Rohrer, M. Schöller, P. Smith, “Redundancy, diversity, and connectivity to achieve multilevel network resilience, survivability, and disruption tolerance invited paper,” Telecommunication Systems, 2014, vol. 56, no. 1, pp. 17-31

[8] C. G. Rieger, D. I. Gertman, M. A. McQueen, “Resilient control systems: Next generation design research,” 2009 2nd Conference on Human System Interactions, Catania, 2009, pp. 632-636.

[9] I. Friedberg, K. McLaughlin, P. Smith, M. Wurzenberger, “Towards a Resilience Metric Framework for Cyber-Physical Systems,” 4th International Symposium for ICS & SCADA Cyber Security Research 2016, Belfast, UK, August, 2016, pp. 19-22.

[10] Rass S., König S., Schauer S. (2015) Uncertainty in Games: Using Probability-Distributions as Payoffs. In: Khouzani M., Panaousis E., Theodorakopoulos G. (eds) Decision and Game Theory for Security. Lecture Notes in Computer Science, vol 9406. Springer, Cham

[11] Gouglidis, A, Shirazi, SNUH, Simpson, S, Smith, P., Hutchison, D., “A Multi-Level Approach to Resilience of Critical Infrastructures and Services,” Paper presented at ICT 2016, Thessaloniki, Greece, 16/05/16 - 18/05/16.

[12] Gouglidis, A., Hu, V.C., Busby, J.S., Hutchison, D., “Verification of Resilience Policies that Assist Attribute Based Access Control,” in ABAC’17. ACM Workshop on Attribute Based Access Control, Arizona, United States, 24-24 March.