Institution: De Montfort University		
Unit of Assessment: 11		
Title of case study: Cyber Incident Response and Risk in Industrial Control Systems		
Period when the underpinning research was undertaken: 2015–present		
Details of staff conducting the underpinning research from the submitting unit:		
Name(s):	**Role(s) (e.g. job title):**	**Period(s) employed by submitting HEI:**
Dr Richard Smith	Associate Professor in Cyber Security	2005–present
Prof. Helge Janicke	Head of School of CSI	2004–October 2019
Dr Leandros Maglaras	Associate Professor in Cyber Security	2015–2016; 2018–present (PT)
Period when the claimed impact occurred: 2016–present		
Is this case study continued from a case study submitted in 2014? N		

1. Summary of the impact

Cyber attacks against Industrial Control Systems (ICS) are increasing in frequency and severity. New Incident Response (IR) techniques developed by DMU have trained hundreds of participants from the UK military, Airbus, Deloitte, Nettitude and more. The new working practices have improved response performance in over 350 incidents, through increased technical confidence and situational awareness in staff. This work contributed to DMU being one of only 19 universities to be recognised as an Academic Centre of Excellence in Cyber Security Research by the National Cyber Security Centre (NCSC) and Engineering and Physical Sciences Research Council (EPSRC).

2. Underpinning research

DMU's Cyber Technology Institute (CTI) provides world-leading research by delivering practical solutions for industrial issues to develop a smart, safe and secure cyberspace.

A common factor across our Cyber Security research is the strong industrial linkage and focus on organisational relevance, which is supported through the centre's exceptionally strong Industrial Advisory Group (IAG), consisting of Airbus, BT, Deloitte UK and Rolls-Royce. The membership is formalised through a Memorandum of Understanding, and exercised through regular meetings to advise on research, joint research projects and the taught provision undertaken in the centre.

This work has been the primary focus of Prof. Helge Janicke, Dr Richard Smith and Dr Leandros Maglaras. Fundamental research has been performed through a number of research projects (e.g. AIR4ICS) underpinned by practical industrial/governmental collaborations (e.g. Cyber Training exercises for UK military). In recognition of our work within the ICS domain DMU was admitted as one of only 13 universities to the Research Institute for Trustworthy Inter-Connected Cyber Physical Systems (RITICS) funded by EPSRC/NCSC in 2018.

This body of work has seen a paradigm shift in the operational procedures used by IR teams. Traditional IT cyber security solutions are often not viable within an industrial operational technology landscape, due to both the technology and the personnel involved. Through creative approaches to working, DMU has developed techniques to improve the security posture of these complex systems while successfully integrating existing personnel and processes. Protection of Critical National Infrastructure has been at the heart of our research, ranging in scope from local-level single organisations up to global recommendations.

One of the major difficulties in the protection of ICS equipment is the difficulty quantifying the risk to such systems. Attacks against ICS are low-frequency, high-impact events and therefore there exist insufficient datasets to produce robust risk estimates. DMU's work helps bridge the gap to

produce more informed risk estimation through the development of synthetic environments used in Cyber Warfare and IR training exercises to act as proxy indicators of real attacks [R1]. Key to a successful cyber IR plan is management buy-in; however, industrial cyber security risk is often difficult to quantify to business leaders. The Simulated Critical Infrastructure Protection Scenarios (SCIPS) serious game has been developed, incorporating real-world learning objectives into an interactive game environment, to increase cyber situational awareness of senior managers within Critical Infrastructure organisations [R2]. Placing participants into unfamiliar roles and requiring them to make decisions to balance financial, production, time and reputational risk factors of an ongoing cyber attack provides a greater understanding of the cyber threat risks faced by organisations.

To improve the operational readiness of IR teams it is vital to ensure that the developed exercise scenarios provide a realistic experience. Assessments of how traditional IT security mechanisms perform in an operational technology environment have been undertaken, and where gaps exist potential solutions have been identified [R3]. IR teams often have limited experience within an industrial control environment, due in part to the dearth of training opportunities in an operational environment. These exercises enable participants to address this skill shortage. By fusing virtualised elements with real-world components, participants are able to gain hands-on understanding of these environments [R4]. The work has allowed the creation of new methodologies fusing IR techniques with industrial network topography to produce a new triage process. This new approach allows IR responders to optimise effort allocation and reduce time to containment [R5]. The work has grown to encompass new technologies, such as the Internet of Things [R6], that pose unique challenges to defenders.

A new forensic acquisition tool, created with Airbus, has been developed to improve the ability of investigators to accurately identify and analyse attacks against programmable logic controllers by allowing the forensic acquisition of live data from these industrial devices for the first time.

3. References to the research

The ICS-CSR conference proceedings papers have all been be peer reviewed by at least two members of the Programme Committee. Papers are selected based on their originality, timeliness, significance, relevance, and clarity of presentation. Distinguished papers, after further revisions, are published in the BCS special issue. The conference and proceedings have an international audience drawn from across Europe and the US.

[R1] Cook, A., Smith, R., Maglaras, L. and Janicke, H. (2016a) 'Measuring the risk of cyber attack in industrial control systems', *4th International Symposium for ICS & SCADA Cyber Security Research 2016* (ICS-CSR), 23–25 August 2016; http://dx.doi.org/10.14236/ewic/ics2016.12

[R2] Cook, A., Smith, R., Maglaras, L. and Janicke, H. (2016b) 'Using gamification to raise awareness of cyber threats to critical national infrastructure', *4th International Symposium for ICS & SCADA Cyber Security Research 2016* (ICS-CSR), 23–25 August 2016; http://dx.doi.org/10.14236/ewic/ics2016.10

[R3] Cook, A., Janicke, H., Maglaras, L. and Smith, R. (2017) 'An assessment of the application of IT security mechanisms to industrial control systems', *International Journal of Internet Technology and Secured Transactions*, 7(2): 144–174; https://doi.org/10.1504/IJITST.2017.087163

[R4] Hallaq, B. Nicholson, A., Smith, R.G. and Maglaras, L. (2018) 'CYRAN: A hybrid cyber range for testing security on ICS/SCADA systems', in M.A. Ferrag and A. Ahmim (eds) *Security Solutions and Applied Cryptography in Smart Grid Communications*, Hershey, PA: IGI Global, pp 226–241; ISBN 9781522518297; https://www.igi-global.com/gateway/chapter/172681

[R5] Cook, A., Janicke, H., Smith, R. and Maglaras, L. (2017) 'The industrial control system cyber defence triage process', *Computers & Security*, 70: 467–481; https://doi.org/10.1016/j.cose.2017.07.009

[R6] Cook, A., Smith, R., Maglaras, L. and Janicke, H. (2018) 'Managing incident response in the industrial Internet of Things', *International Journal of Internet Technology and Secured Transactions*, 8(2): 251–276; https://doi.org/10.1504/IJITST.2018.093336

4. Details of the impact

(1) INDUSTRIAL IMPACT

The ICS work performed by the CTI has led to the recognition of DMU as an Academic Centre of Excellence in Cyber Security Research (ACE) by the NCSC and EPSRC, which includes a grant of GBP60,000 [C1]. DMU is one of only 19 ACEs in the country, the first ACE in the East Midlands and the joint-first post-92 university to gain this recognition.

Dr Richard Smith is also a full member NCSC's Industrial Control System's community of interest – open only to those with a demonstrable expertise within the field with a track record of impactful work for industry – and is currently leading a workstream on how organisational readiness of a critical infrastructure provider can be tested and exercised. Membership of the community of interest has also provided Dr Smith the opportunity to contribute to the NCSC cyber research problem book, used to inform research direction for cyber security projects nationwide. He has been invited to give keynote presentations at industrial events in the UK, Romania, Australia, Austria, the USA, Germany and France.

DMU has also been recognised as one of only two Airbus Academic Centres of Excellence in ICS cyber security in Europe [C2]. This has been realised in the form of an enhanced Knowledge Transfer Partnership, supported by Innovate UK, in Tools and Techniques for ICS/SCADA Digital Forensics, with Airbus Group supported by GBP225,000 funding. The work has generated a forensic memory acquisition tool used by Airbus workers on their factory floors to allow direct memory acquisition from industrial devices for the first time, increasing the chance of identification and mitigation of attacks against the company. Previously, suspect devices would simply be thrown away, losing valuable forensic information. Now, the evidence is extracted and stored for the investigative team [C3].

Cyber Warfare and incident response exercises have been used to enhance participants' skillsets and change the way IR teams operate. The DMU Agile Incident Response for ICS (AIR4ICS) project, worth GBP250,000 with additional contributions in kind of GBP160,000 from Airbus, Rolls-Royce, BT and Limes Security, has produced new Agile methodologies and tools providing benefits for IR teams who have adapted their business practices [C4]. This modular framework was funded by the NCSC and allows organisations to choose which elements they feel can be best incorporated into their working practices. Organisations such as Nettitude have chosen to adopt practices and tools from AIR4ICS, such as the Sprint cycle, Incident backlog and Incident board which focus on communication and information sharing between team members and have seen a number of benefits. 'The first is an increase in technical confidence of the participants, which has manifested itself in more confident decision making' and 'The improved situational awareness has assisted the management team and the SOC analysts to be more efficient' [C5], and the UK military 'On the exercise itself, there was a clear uplift in capability and performance … demonstrated in the feedback from the exercise assessors in both qualitative and quantitative terms' [C6].

Cyber Warfare and Incident Response exercises designed, developed and delivered by DMU, for the UK Army, Navy and Air Force response teams in January 2016 and February, April, June, August, November and December 2017 have been used to improve the skills of 124 participants. These skills were then demonstrated and described during cyber exercises of up to 1,000 international participants from NATO countries [C6, C7]. Events during DMU CyberWeek in 2018 and 2019 and AIR4ICS which have trained 123 participants from 22 organisations including SMEs, NHS, local government, industry such as Emerson and Rolls-Royce. These events have utilised DMU's state-of-the-art hybrid cyber range CYRAN [R4] to create realistic sandboxed cyber environments along with the new IR approaches to introduce new working practices for industry, such as at Nettitude where 11 staff were trained on the AIR4ICS techniques, who have since introduced them to their colleagues and adopted them within the organisation. The main benefits of adopting these techniques has been seen in task management and tracking, 'the 15 Security Operations Centre staff have implemented a number

of measures to improve the efficiency of the Nettitude SOC. These include SCRUM meetings and kanban boards. We have also introduced sprints into aspects of the platform, monitoring and IR operations' [C5].

Valuable hands-on practical experience of the ICS equipment used in DMU's CYRAN cyber range has had the added benefit of providing device penetration tests, identifying vulnerabilities for manufacturers to be used to inform their patch cycle. The work has also allowed the Red team participants, from Austria, Germany and Denmark, who were responsible for attacking the network, to use AIR4ICS techniques to increase the efficiency of their penetration testing service and therefore provide better security recommendations:

> Our staff doing blue team benchmarking projects became certainly more efficient through the AIR4ICS contributions. Also, in cases where we support customers with incident response, the agile approach gives guidance yet does not bloat the activities like a formal process, so we certainly consider it useful for real-world projects. The value provided even for senior OT security staff as in our case, where realistic attacks lead to realistic responses is substantial, we are glad to have joined the consortium as our invested resources have had a good knowledge-return already. [C8]

To raise awareness of the risk posed to ICS by cyber threats and to increase the understanding of the unique environment in which they exist, SCIPS exercises have been performed at both private events, such as for UK Cyber Defence Academy, and at public events like DMU CyberWeek 2018 and 2019. Some 104 participants have successfully taken part in these SCIPS exercises, including people from organisations including Thales, Rolls-Royce and Emerson. Successful identification of industrial cyber risk increased by 75% and 90% of respondents registering an increased cyber awareness of the threats to ICS [C9].

DMU's expertise in the area of IR and security operations has been recognised by Deloitte with GBP20,000 funding provided to create a new research Security Operations Centre that will be used to define more effective defensive offerings in the future for Deloitte: 'It is essential that when providing advice to our clients we are informed by research that is subjected to rigor and scrutiny. Shaping research with DMU in the SOC allows us to develop solutions that address organisations' most complex cyber security challenges' [C10].

(2) SOCIETAL IMPACT

DMU has changed the perception of industrial risk within the cyber security and engineering community. Cyber Security attack demonstration devices developed by in conjunction with Airbus and Claroty have successfully been included at major international events where previously there was no ICS representation. These include the first ever ICS 'capture the flag' event at RSA 2018, an event attended by over 25,000 people. Some 250 participants were trained and reported an increased understanding of issues within ICS security at the RSA 2018 international conference [C3]. Additional demonstrator devices developed by DMU have also been presented at international events including DEFCON25 ICS Village, the Hong Kong GREAT festival of Innovation, BruCon (Belgium's largest hacking conference), the IET/BCS Turing EngTalk and DMU have hosted events at their Leicester campus for participants from organisations such as British Gypsum and Siemens Rail.

5. Sources to corroborate the impact

[C1] https://www.ncsc.gov.uk/information/academic-centres-excellence-cyber-security-research

[C2] https://www.airbus.com/innovation/open-innovation/airbus-cyber-innovation.html

[C3] Testimonial from Head of Cyber Innovation and Scouting, Airbus.

[C4] AIR4ICS Framework document.

[C5] Testimonial from Technical & Security Operations Manager, Nettitude.

[C6] Testimonial from UK Army Major, UK StratCom Joint User, Cyber Operations.

[C7] Cyber Exercise Report, forming part of PhD thesis for Allan Cook.

[C8]	Testimonial from Managing Director, Limes Security.
[C9]	PDF of Internal CyberWeek18 Report.
[C10]	https://www.dmu.ac.uk/about-dmu/news/2020/september/dmu-offers-state-of-the-art-cyber-security-training-for-businesses.aspx