2017

The convergence of IT and OT in critical infrastructure

Glenn Murray
Edith Cowan University

Michael N. Johnstone
Edith Cowan University

Craig Valli
Edith Cowan University

DOI: 10.4225/75/5a84f7b595b4e
Originally published as: Murray, G., Johnstone, M.N., & Valli, C. (2017). The convergence of IT and OT in critical infrastructure. In Valli, C. (Ed.). (2017). The Proceedings of 15th Australian Information Security Management Conference, 5-6 December, 2017, Edith Cowan University, Perth, Western Australia. (pp.149-155).

THE CONVERGENCE OF IT AND OT IN CRITICAL INFRASTRUCTURE

Glenn Murray, Michael N. Johnstone and Craig Valli
Security Research Institute, School of Science, Edith Cowan University, Perth, Western Australia
{g.murray, m.johnstone, c.valli}@ecu.edu.au

Abstract

Automation and control systems, such as SCADA (Supervisory Control and Data Acquisition), DCS (Distributed Control Systems) and are often referred to as Operational Technology (OT). These systems are used to monitor and control critical infrastructures such as power, pipelines, water distribution, sewage systems and production control,). Traditionally, these OT systems have had a degree of physical separation from Information Technology (IT) infrastructures. With changing technologies and a drive towards data-driven and remote operations the two technology environments are starting to converge. With this convergence, what was a relatively standalone secure and isolated environment is now connected and accessible via the Internet/cloud. With this interconnection comes the cyber security challenges that are typically associated with only with IT infrastructures. OT data that is then accessible from these environments could include critical information such as pressures, temperatures, proximity levels, control signals and other sensor signals. Due to the aforementioned convergence, OT data and associated control mechanisms are now significantly vulnerable to cyber-attacks. This paper provides an understanding of cyber security in an operational technology context (rather than traditional IT environments) and discusses the underlying causes, vulnerabilities, and the risks that are created by convergence and interconnection. We report on evidence of convergence between IT and OT, and use Hofstede's model of organisational culture to explain the different attitudes and value drivers in IT and OT.

Keywords: Operational Technology, Critical Infrastructure, Cyber-physical systems, Internet of Things, Network Security

INTRODUCTION

Operation Technology (OT) refers to the hardware and software used with the automation controls systems within infrastructure. OT networks and systems including, Industrial Control Systems (ICS) or Supervisory Control and Data Acquisition (SCADA) are used in multiple industries such as power, oil & gas, water treatment, transportation, defence, traffic control and even within private facilities to monitor and control functions such as heating and cooling (Shahzad et al., 2015). These industries form part of our national critical infrastructures without which society and economy would fail. OT systems were designed to integrate data acquisition systems, data collection/transmission systems and Human Machine Interface (HMI) systems to create a centralised control and monitoring solution. Thus, allowing an operator to visually interpret the state of the plant for control and monitoring purposes (Shahzad et al., 2015).

The majority of the OT systems in use are decades old. These were the forerunners of today's 'smart' solutions. These systems are often highly engineered and use proprietary protocols that are specific to project requirements. There are a limited number of people capable of supporting these systems therefore such targets are relatively easy to exploit.

Threats to OT systems are evolving daily with cyber-attacks increasing in both frequency, sophistication and impact. As recently as July 2017, cyber-attackers gained access to a Kansas nuclear power network and other energy companies. The consequences of a cyber-attack on critical infrastructure OT systems goes further than a financial loss to include prolonged outages of critical services (e.g., electricity), possible environmental impacts, and even loss of life.

This research seeks to examine if the differences between IT and OT management structures, cultures and values explain the different attitudes to cyber security. The remainder of the paper describes the security landscape for Industrial IoT (IIoT) systems, describes the key differences between IT and OT systems and discusses the findings of the research.

SECURITY ISSUES IN IIOT (INDUSTRIAL IOT) SYSTEMS

The lack of security in IIoT systems has been a cause for concern recently, as noted by Harp & Gregory-Brown (2016). Many control systems run on standards, protocols and software designed and implemented at a time when the attack surface was small, due to limited interconnection between devices and networks. However, given the (reasonable from a facility manager's point of view) drive for interconnected systems, IIoT systems are gaining attention from cyber adversaries.

Lee, Assante & Conway (2016) point out that in 2015, Ukraine's power grid was attacked and availability severely compromised after attackers gained access to OT systems and shut down parts of the grid. This cyber-attack on power infrastructure, allegedly by a nation-state, indicates the level of sophistication of attacks against critical infrastructure. The attack did not only directly target OT systems controlling the electrical grid but also systems that owners would rely on to respond to the attack e.g., disabling the telephony systems. This outcome is, perhaps, unsurprising as other protocols have also been found to be vulnerable, e.g., BACnet, used in building management systems (Peacock & Johnstone, 2014). Table 1 describes a range of attacks on critical infrastructure that have occurred over the last 35 years.

The vast majority of OT systems are operated in relative isolation from IT systems and infrastructure, which is commonly referred to as 'air gapped', and are simply not designed with a cyber-attack in mind, neither from a detection or defence perspective. OT operating companies use the air gap theory as a barrier, believing that their respective sites are not vulnerable to cyber-attacks. This complacent mindset represents a significant vulnerability as during maintenance periods, where contractors use multimedia devices such as laptops, portable hard drives and USB flash drive as maintenance aids within the industrial infrastructure. The Stuxnet attack was an example of malware was transmitted through an infected USB flash drive allowing the virus to spread resulting in the centrifuges speeding up to the point they self-destructed (Falliere, Murchu, & Chien, 2011).

Contractors may also have set up full-time Internet access, through a cloud infrastructure, to workstations and equipment to enable remote management, including monitoring, technical support and software updates. On December 2014, ICS CERT identified that malware campaign ongoing from 2011, a variant of BlackEnergy malware known as BlackEnergy3, was delivered through Internet connected devices, which compromised industrial Human Machine Interfaces (HMIs). The alert "Ongoing Sophisticated Malware Campaign Compromising ICS" was issued in 2014 and later updated in 2016. The Ukraine power grid outage in 2015, initiated through a spear-phishing campaign targeting IT staff, was attributed to the BlackEnergy malware (Ongoing Sophisticated Malware Campaign Compromising ICS (Update E) | ICS-CERT, 2016).

Both the Stuxnet and Ukraine power grid attacks are examples where human intervention, either deliberate malicious intent or inadvertent, provided the opportunity for cyber-criminals to exploit OT environments. Hence, organisations must consider deploying multi-layer cyber-security defence measures, including implementing cyber technology, educating OT personnel in cyber risk reducing behaviours, introducing cyber resilient policies and physical security.

As OT systems evolve so does the need to apply updates, i.e., software updates and software patches. As explained, within OT systems production is the highest priority or in the CIA structure availability is pivotal. This juxtaposition on prioritisation comparative to traditional IT security has led to some OT systems operating for years without a patch being applied, leaving them highly vulnerable. Furthermore what exacerbates the issues around updates is that many OT equipment suppliers "freeze" the operating systems and subsequent application for elements in an OT system. This practice demands use of arcane and outdated systems.

Finally, when the opportunity does present itself to apply the update/patch, the air gap still exists and requires direct connection to these systems via vendor computers or USB drives, both of which are potential entry points for motivated, capable cyber criminals. The concept, or approach, of using the air gap as a means to avoid/stop a cyber-attack is now flawed and must be addressed in a meaningful way. This *modus operandi* is exactly how the zero day Stuxnet malware was introduced to spread through OT systems.

Date	Cyber-Attack Name	Industry	Location	Description	Effect
Oct 1982	Siberian Pipeline Explosion	Natural Gas	Siberia	Pipeline software programmed to reset pump speed and valve settings above the specifications of the pipeline joints and welds. Allegedly conducted by the CIA.	Explosion visible from space. Vapourised part of the Soviet Union's Trans-Siberian pipeline.
1992	Chevron Emergency System	Oil & Gas	USA	Chevron employee disabled the emergency alert system for 22 states in the USA.	Emergency occurred and no alert was issued.
2000	Maroochy Shire Sewage Spill	Sewage	Australia	Disgruntled employee spoofed controllers opening valves of the sewage system	264,000 raw sewage flooded into hotel and the surrounding parks and river.
2002	Venezuela Pipeline control system	Oil	Venezuela	Allegedly cyber criminals penetrated the SCADA system responsible for tanker loading at a marine terminal.	PLCs operating systems erased. Tankers couldn't be loaded for 8 hours.
2003	Israel Electric Corporation DoS	Electric	Israel	DoS attacks originating from Iran penetrate the Israel Electric Corporation	DoS attacks penetrated however failed to shut down the power grid
Nov 2007	Stuxnet Worm	Nuclear	Iran	Supposedly created by American/Israeli Governments to attack Iran' Nuclear Facilities.	Centrifuges and valves were sabotaged/destroyed
Nov 2011	Pump SCADA	Water	USA	Destroyed a pump remotely from gaining access through a SCADA network. Allegedly the access from gaining user names and passwords from manufacturer's customers.	Chemicals in treatment plant were changed. 2.5 million customers had data exposed to the internet.
Jan 2015	German Steel Mill	Steel Mill	Germany	Cyber criminals used Phishing emails to gain access and prevented the blast-furnace from shutting down.	Catastrophic damage to the steel mill.
Mar 2016	Ukraine Power Grid	Power	Ukraine	Cyber criminals gained access remotely and cut power to 30 substations through the installation of customer firmware.	225,000 customers without power. Deleted files from the master boot records and also shutdown telecommunications.

Table 1: Selected Disclosed OT Cyber Attacks

Possible results that could occur from an OT cyber-attack include:

- A delay in the information that is being communicated to an ICS/DCS/SCADA Master from a Remote Terminal Unit (RTU). These could ultimately lead to a catastrophic event as the information could be turbine speed, level sensor, alarm sensor or actuators.
- Interrupting a connection between an ICS/DCS/SCADA Master to engage an event through a safety system.
- Changing the values received from an ICS/DCS/SCADA Master. This could either have an automatic response, e.g., shutdown a section of a plant or it could lead to a human response which could lead to an inappropriate action.
- Set point values of the RTUs. An example would be changing the HH set point for an alarm for a level sensor for a vessel. Hence causing the vessel to overflow.
- Change/modify the operation of equipment protection systems e.g., speeding up a turbine in a plant causing the blades to be destroyed.

Considering the wide range of vulnerable protocols used in the IIoT, and the high cost of data breaches (e.g., plant re-start costs, declining stock price), further research is necessary to reduce the risk to critical infrastructure. The following section describes the convergence between the IT and OT worlds and highlights the discontinuity caused by widely differing priorities. We do not assert that OT priorities are correct and that IT priorities are faulty in some way, just that they are different and that this is the root cause of a security issue.

THE CONVERGENCE OF IT AND OT

Figure 1 highlights the trend in industry to converge the IT and OT systems in order to access real time data and to interconnect facilities. The convergence is being driven by the need for quantitative management reporting, assisted by 'big data' and sensor technology, artificial intelligence, physical automation, remote operations, cloud computing, analytics. All of which have the potential to enhance productivity/production. To facilitate all of this requires operators to increase network connectivity and access to both IT and OT systems using Ethernet, WI-FI and TCP/IP standards (Shahzad et al., 2016).

By converging IT and OT, systems that were previously closed in many respects are now linked and exposed to all of the risks that have existed in the IT space for years. With this exposure, and not unexpectedly, individuals or groups looking to exploit these new-found vulnerabilities have emerged.

Convergence of itself is not the problem, although figure 1 highlights some obvious differences between the IT and OT worlds. What is a significant problem is the profoundly different priorities between IT and OT that cause a discontinuity in the security space.

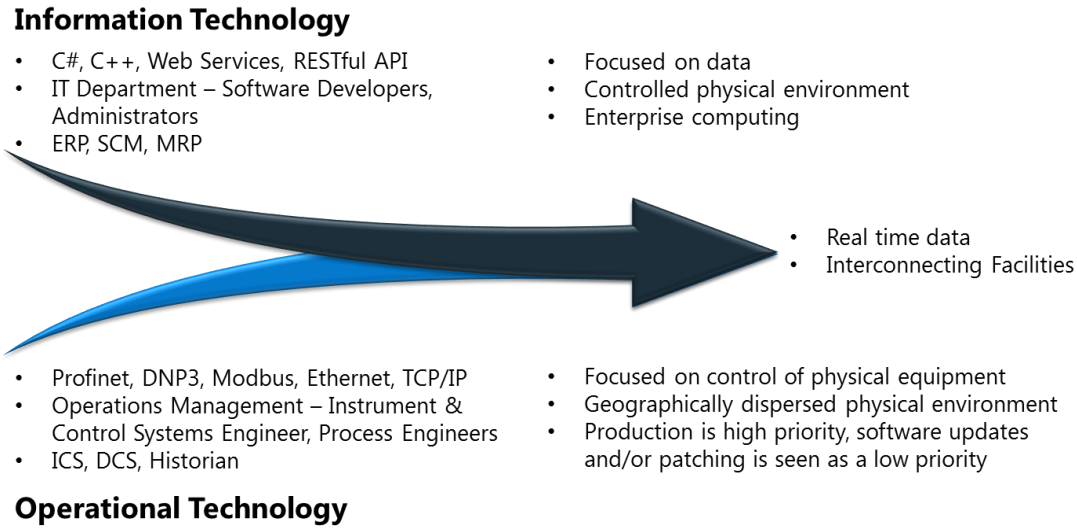

Figure 1: Convergence of IT and OT

As shown in table 2, IT security focuses where the concerns are most often associated with financial integrity, denial of service or loss of information, properties can be grouped and prioritised into confidentiality, integrity and availability, as is common in information security.

1. The confidentiality of data is of paramount importance,
2. The integrity of the data, and;
3. The availability of the data (Zhu, Joseph & Sastry, 2011).

In an OT control system environment, safety and operational risk are critical, which changes the order of security properties to:

1. The availability of the data is paramount to safely maintain production,
2. The integrity of the data, and
3. The confidentiality of the data (Zhu, Joseph & Sastry, 2011).

Table 2: Differences in IT and OT priorities

	Protecting	Priority	Update Frequency	Operating System	Protocols	Cyber Criminal Motivation	Cyber Attack Mission
IT	Data	Confidentiality Integrity Availability	High	Standardised	Standardised	Monetisation	IT Stack Specific
OT	Asset	Availability Integrity Confidentiality	Low	Proprietary	Proprietary	Disruption	Industry Specific

As explained, the priority of IT is to protect data, therefore the IT evolution has seen tools, practices and procedures put in place to protect IT systems from cyber threats.

In the OT space the main priority is to protect the asset base and its associated production. This has translated to minimal effort or changes being undertaken in the OT cyber security space, as production almost certainly would have to be taken offline to accomplish this goal. This production loss, and the associated loss of revenue combined with the cost of designing and implementing the necessary solutions has resulted in OT systems significantly lagging behind IT systems in addressing cyber security threats.

ANALYSIS AND DISCUSSION

In this initial work, based on our combined experience in the IT/OT spheres of at least (conservatively) 60 years, we posited that there is a convergence occurring between IT and OT. There is evidence of that convergence in the IoT area identified by Baig et al. (2017) in terms of the range of disparate IoT networks and systems that are being connected in smart cities-of course critical infrastructure, as managed by OT systems, is one aspect of a smart city. Further, we suggested that security problems might arise from the different priorities encountered in the IT and OT spheres. We assert that these differences are due to elements of organisational culture that have not yet been examined and compared across these two intersecting spheres.

In this section, we use Hofstede's theory of organisational culture as a lens through which to view and explain the differences between IT and OT. Hofstede (1998) perceives culture as 'programming of the mind' where members of one culture can be distinguished from members of another culture. Pertinent to our discussion, Ahmed, et al., (2012) note that when teams from different cultures interact, the complexity of the work relationship can be challenging.

Hofstede's work has been widely cited by many subsequent researchers, but acceptance of his theory and constructs is by no means universal. Probably the most often-cited criticism is that Hofstede studied a single firm, as pointed out by Soares et al. (2007). Nonetheless, a single multi-national firm can exhibit a myriad of cultures. As noted by Jones (2007), Hofstede's survey covered 60,000 employees of a multi-national firm over 50 countries and "the research framework used by Hofstede was based on rigorous design with systematic data collection and coherent theory".

Hofstede's model comprises five dimensions or variables, viz.: Power Distance Index, Individualism/Collectivism, Masculinity/Femininity, Uncertainty Avoidance Index and Long Term Orientation. Of the five, Masculinity/Femininity deals with social gender roles and is therefore not relevant to this analysis. The remaining dimensions are discussed briefly below.

A high power distance index culture accepts the decisions of superiors in a hierarchy without question. Such a culture accepts inequality in the power relationship. Conversely, a low power index culture may operate by consensus and discussion of the decisions of superiors is the acceptable norm. Interestingly, with respect to the deployment of system development methodologies, Iivari and Huisman (2007) found in their study of organisation culture, that IS managers promoted a hierarchical culture that was oriented toward security, order, and routinsation- a stark contrast to managers' take-up and acceptance of agile methodologies.

An individual culture values individual authority and achievement, the right to make self-decision, to hold self-opinion and to exercise some degree of autonomy. In contrast, a collectivist culture values a group's well-being over any individual's desires.

Uncertainty avoidance index is a measure of the extent to which members of a culture feel vulnerable or endangered by uncertainty. In uncertainty avoiding cultures, members are seen to be expressive, and in uncertainty tolerating cultures the expression of thought is repressed. Thus, in the former there is a necessity for consensus.

Long-term orientation is perhaps self-explanatory and refers to a cultural orientation that is not focussed on short-term goals.

Table 3: Core cultural dimensions related to IT vs. OT teams.

Cultural dimensions	**IT**	**OT**
Individualism / Collectivism	Collectivist	Collectivist
Power Distance Index	Low	High
Uncertainty Avoidance Index	Low	High
Long-term Orientation	No	Yes

Our preliminary analysis, summarised in Table 3, shows that IT and OT exhibit widely-differing cultural values across several dimensions. Both IT and OT are classed as collectivist as they both value a team outcome (product, in the case of IT, and production in the case of OT). IT teams are also likely to be using agile development methods, which tend to promote values resulting in a low power differential within a team. Similarly, in IT, changes in technology are embraced swiftly, leading to a low uncertainty avoidance index. This same dimension is paired to a lack of long-term orientation in IT, which is a marked contrast to OT, where the operating technology has not changed for decades (because the focus is availability, as noted in the previous section). This contrast in values, coupled with the difference in priorities described in table 2 leads to the inevitable conclusion that, rather than a peaceful co-existence or a smooth transition to convergence, the clash of cultures will lead to less secure OT systems and the benefits accrued from experiences in the IT world will likely not be realised in the OT world without a substantial readjustment and realignment by both parties.

CONCLUSION

This research set out to examine the state of cyber security in operation technology (OT). As was outlined previously, there is evidence that OT systems have been attacked. We showed that the convergence of IT and OT, whilst inevitable due to other forces, is problematic in terms of cyber security. Additionally, we used Hofstede's organisational culture theory to show the contrast in values between the IT and OT worlds. This variance in cultural values explains the difference in importance placed by each group on information security properties, viz., that OT values availability and that IT values confidentiality.

In future work, we intend to explore both the technical and social dimensions of the problem that we have identified. In the former, we will examine unknown-unknown vulnerabilities of physical and virtual OT systems using a machine learning approach. To address the latter, we will embark on an action research programme to surface and examine the cultural differences in detail and provide a framework for successfully fusing the IT and OT worlds whilst maintaining both availability and confidentiality.

REFERENCES

Ahmed, F., Capretz, L., Bouktif, S., & Campbell, P. (2012). Soft Skills Requirements in Software Development Jobs: a Cross-cultural empirical Study. *Journal of Systems and Information Technology, 14*(1), 58 - 81.

Baig, Z., Szewczyk, P., Valli, C., Rabadia, P., Hannay, P., Chernyshev, M., Johnstone, M., Kerai, P., Ibrahim, A., Sansurooah, K., Syed, N., Peacock, M., (2017). Future Challenges for Smart Cities: Cyber-Security and Digital Forensics. *Digital Investigation*, 22(1), pp. 3-13.

Falliere, N., Murchu, L. O., & Chien, E. (2011). *W32.Stuxnet Dossier*, 1-68. Retrieved from http://www.symantec.com/content/en/us/enterprise/media/security_response/whitepapers/w32_stuxnet_dossier.pdf

Harp, D., & Gregory-Brown, B. (2016). SANS 2016 State of ICS Security Survey. SANS. Retrieved from https://www.sans.org/reading-room/whitepapers/analyst/2016-state-ics-security-survey-37067

Hofstede, G. (1998). Attitudes, Values and Organisational Culture: Disentangling the concepts. *Organisational studies, 19*(3), 477.

Iivari, J. and Huisman, M. (2007). The Relationship between Organizational Culture and the Deployment of Systems Development Methodologies. *MIS Quarterly*, 31(1), pp. 35-58.

Jones, M (2007). Hofstede – Culturally questionable?, Oxford Business & Economics Conference. Oxford, UK, 24-26 June, 2007.

Lee, R. M., Assante, M. J., & Conway, T. (2016). Analysis of the cyber attack on the Ukrainian power grid. SANS Industrial Control Systems.

Ongoing Sophisticated Malware Campaign Compromising ICS (Update E) | ICS-CERT. (2016). Retrieved from https://ics-cert.us-cert.gov/alerts/ICS-ALERT-14-281-01B

Peacock, M., & Johnstone, M. (2014). An analysis of security issues in building automation systems. Australian Information Security Management Conference. doi:10.4225/75/57b691dfd9386

Shahzad, A., Lee, M., Xiong, N., Jeong, G., Lee, Y., Choi, J., … Ahmad, I. (2016). A Secure, Intelligent, and Smart-Sensing Approach for Industrial System Automation and Transmission over Unsecured Wireless Networks. *Sensors*, *16*(3), 322. doi:10.3390/s16030322

Soares, A. M., Farhangmehr, M., & Shoham, A. (2007). Hofstede's dimensions of culture in international marketing studies. *Journal of Business Research, 60*(3), 277.

Zhu, B., Joseph, A., & Sastry, S. (2011). A Taxonomy of Cyber Attacks on SCADA Systems. *2011 International Conference on Internet of Things and 4th International Conference on Cyber, Physical and Social Computing*. doi:10.1109/ithings/cpscom.2011.34