Cyber-Physical-Security Model for Safety-Critical IoT Infrastructures

Xavier Bellekens, Amar Seeam, Kamila Nieradzinska, Christos Tachtatzis,
Alison Cleary, Robert Atkinson, Ivan Andonovic
Department of Electronic and Electrical Engineering
University of Strathclyde, Glasgow, G1 1XW, UK
{xavier.bellekens@strath.ac.uk}

***Abstract*—The Internet of Things (IoT) and the number of sensors integrated within safety critical environments is increasing exponentially. System designers employ off-the-shelf hardware to reduce development time and cost, however, the early adoption of consumer hardware and software raises numerous security questions. Several successful attacks and threats to critical infrastructures have been reported. This paper reviews safety-critical applications in aviation, connected cars and power plants. An engineering development roadmap is proposed with cyber-security in mind from "cradle-to-grave" rather than an afterthought. The development roadmap introduces a cyber-security review at each design step to strengthen the robustness of IoT hardware and software. However, considering these systems have an extremely long lifetime (>20 years), secure maintenance and integrity of ageing infrastructure is usually a secondary consideration. The paper proposes the use of a cyclic cyber-physical security model after system commissioning that allows knowledge transfer between regulatory bodies through sharing of best practices. The sharing will enable system operators to identify exploits encountered from other industries and maintain high security levels and improve the IoT architectures.**

I. Introduction

With the growth of the IoT and 5G coupled with the increased reliance of industry on commercial off-the-shelf (COTS) hardware and software, safety critical system can be exposed to devastating cyber-attacks. Users often fail to understand the security challenges, the potential vulnerabilities, and persistent threats such systems may face [1].

Computing and wireless communications are now embedded in every control systems ranging from medical applications to nuclear power plants. These applications often have a high economic and societal impact and require high-fidelity networks in order to operate successfully. Such systems often communicate with the control system using the standard TCP/IP stack, common GNU/Linux, Windows servers, VoIP (Voice over IP) and network sensors; This creates a number of problems and issues for regulators and users.

Firstly, these systems have been designed using commercial equipment that have not been audited prior to their use in a safety-critical environment. Secondly these systems require extensive monitoring due to an increasing amount of vulnerabilities being uncovered on a daily basis. Finally, users and regulators need to understand these system at the same level as full-stack engineers to mitigate cyber attacks, and learn lessons from previous incidents in the world of safety-critical applications.

Increasing the number of COTS equipment in safety-critical infrastructures often reduces the costs bringing significant savings to manufacturers, developers and operators, however this tendency allows hackers to take advantage of these infrastructures with the same simplicity as when targeting lambda users with mass-market malwares.

The introduction of wireless communications and sensors in nuclear power plants, aviation and other safety-critical sector often unravels security flaws (i.e. described in section II) that operators are not usually confronted with, and demonstrates the requirements for and IoT cyber-security model based on the lessons learned in other safety-critical systems.

II. Assessment of Wireless Security in Safety Critical Environments

IoT is focused on introducing Internet connectivity to mass consumer devices, allowing continuous monitoring and control of everyday objects and users. IoT examples include devices to monitor personal and animal health, automobile and consumer electronics, home appliances and other machinery. These digital representations of physical objects often communicate using wireless technologies and 5G networks to communicate, transfer data and create alerts.

This paper focuses on the use of IoT sensors and wireless communications for safety-critical environments and the risks associated with them. Wireless communications and sensors play a major role in tomorrow's environment through monitoring, reducing cabling, enabling data accessibility, data transfer without human-to-human interactions, and advancing machine-to-machine (M2M) communications.

These communications will often generate a large cohort of data that can be used later by operators to predict system failures and avoid them in the future, or to receive and detect anomalies in real time. In a safety-critical environment these data require high security and privacy requirements, as the operator, manufacturer, and engineer actions will depend on the data transmitted wirelessly by the sensors.

Data misinterpreted or corrupted could lead to accidents, and death [2], it is therefore important to establish a strong cyber-security model enabling users to assess the system, and establish failure points.

A. Aviation

Wiring in aircraft consumes weight, and man-hours to install and maintain at significant cost. For example the Airbus

A380 has 500 km of cabling, and a complex wiring infrastructure that led to delays and cost overruns totalling nearly $2 billion [3]. Wireless technology has now sufficiently matured, that it is now being seriously considered by the Aviation industry for intra-aircraft communications in forthcoming generations of aircraft, as evident by the recent formation of working groups such as Aerospace Vehicle Systems Institute Wireless Avionics Intra-Communication (WAIC) project [4], which has been set up by the major aerospace companies to address common issues associated with wireless avionics. It is important to note that WAIC is specifically being proposed for safety related avionics but the existing availability of wireless technologies in the provision of Internet connectivity in the cabin using standard 802.11 WiFi also poses interesting challenges in terms of security and availability, such that other frequency band are being considered including Ultra Wide Band (UWB) and most recently the ITU and ICAO are working towards establishing 4.2 GHz-4.4 GHz for future WAIC systems. These frequencies are focused on the provision of radio-communication between safety-related avionics components integrated or installed onboard the same aircraft, rather than wireless in cabin entertainment, and passenger communications which will continue to be serviced by conventional WiFi. Previous frequencies that have considered include 2700-2900 MHz, 5350-5470 MHz, and portions of 15.4-15.7 GHz.

There are several potential benefits in replacing some of wired avionics network infrastructure with wireless alternatives, such as, the weight reduction through removal of cabling and connectors (contributing to more efficient aircraft, the reduction of effort and cost in wiring design and installation. The improvements also leads to a greater system design flexibility and scalability, and create infrastructure for introduction of mobile devices into avionics networks.

However, wireless technology cannot be adopted if it compromises safety of flight. Users of commercial wireless technology are familiar with temporary loss of network connectivity (availability) or, worse still, intrusion from unauthorised users (security). These remain the challenges that require to be addressed, particularly with respect to long term deployments and trust of wireless hardware for the communications of safety-related avionics. These challenges include physical security of installation, maintenance and robustness of wireless nodes, as well the management of longer term upgrade paths, which will require further consideration of standards that can accommodate changes in wireless specifications spanning several decades at the minimum.

B. Nuclear Power Plants

Nuclear Power Plants are considering wireless sensors technologies in safety-critical environments to replace ageing cabling, and decrease the maintaining costs, hence avoiding human interaction with potentially dangerous areas of the nuclear power plant and health and safety related issues [5].

Major players in the nuclear industry have been advocating for wireless sensor networks (WSN) and have started trials by introducing VoIP devices, monitoring communication failures and electromagnetic problems, often setting aside cyber-security concerns, and physical-security concerns.

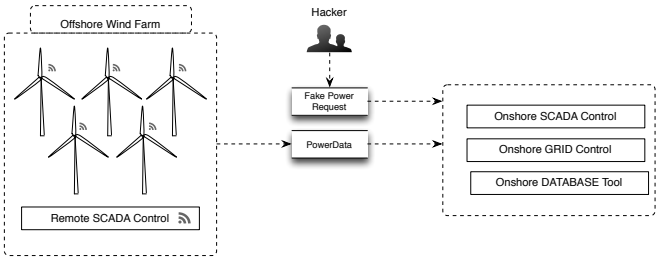

Fig. 1. Malicious Data Acquisition Scenario

Multinational nuclear power plant companies have also been considering mass consumer hardware such as the Peach bottom nuclear power plant which uses VoIP spectralink 6000 systems, and uses wireless radiation hardened cameras to monitor the fuel replacements in the reactor [6] [7]. The River Bend nuclear power plant has deployed wireless access points linked to the auxiliary control room for sensor data acquisitions in SCADA systems [5]. Other nuclear power plants such as Comanche Peak, monitor over 50 critical devices and stations using wireless sensors [8]

These IoT architectures however require intensive maintenance, security and privacy, as the network growth and the number of sensors increases different technologies will have to be maintained and communicate within the same "language" increasing the security risk factor. Sensors will also require physical security as some might have to undergo replacement, repairs, or targeted checking.

C. Off-shore and On-shore Wind Turbines

Off-shore and on-shore wind turbines faces similar problems to those of the nuclear power plants. Each of the wind turbines can be considered as a sensor and be represented as a mesh network communicating via wireless communication with an on-shore base station [9].

These communication systems allow better monitoring of wind turbines and help operators to send individual commands to each turbines. Such systems reduces the costs induced by submarine redundant communication cables however introduces cyber-security concerns [10] [11].

Figure 1 depicts a scenario where a malicious user spoofs the wireless communication between an off-shore wind farm and creates fake power requests to the base stations, increasing the power network load, leading to failure.

Such malicious actions requires the operator to learn about existing and future threats during their training in order to monitor efficiently these power stations on a long term basis. With the quick evolution of hardware and software, these networks will require extended monitoring.

With the increasing number of off-the-shelf equipment security operators will be required to monitor the network usage of each of the critical hardware and software levels, ranging from personal communication devices between operators to wind turbines communicating with the base station.

D. Connected Cars

Vehicles to everything (V2X) communications is one major part of the Internet of Things and can be categorised as a safety critical environment when moving at high speed. With over 25,700 fatalities in the EU in 2014 inter-connected cars require extensive cyber-security scrutiny.

Recently (August 2015) Tesla inc. released a patch against a security flaw allowing malicious users to turn off the engine of the car while driving. This problem is not an isolated incident as in June 2015 two hacker have been able to remote control a car of the Fiat Chrysler group leading to recall over 1.4 million vehicles [12].

V2X communications require cyber-physical analysis, and behavioural system monitoring in order to spot flaws being exploited by malicious users. These problems require extensive policies as often, mass-user will not be able to spot any malicious activities of their car such as inappropriate location broadcasts via compromised Here-I-Am (HIA) units, requiring the car API to implement some levels of trustworthiness. Other informations could maliciously be gathered on the users in order to perform more targeted attacks [13].

The consequences of a Vehicle to Vehicle (V2V) communication could lead to attacks, advertising a clear road instead of a traffic jam and increase the risk of accidents. These problems can be introduced by packet replays, or packet jamming leading to critical consequences for drivers and passengers [14].

These attacks demonstrates the flaws of IoT hardware and software in safety critical environments and the requirements for a roadmap highlighting the key findings and best practices for future hardware and software that are required to last long. Furthermore research as demonstrated the barriers of current security tools in safety-critical environments, decreasing the overall resilience of these systems [15]

III. Roadmap for IoT Wireless Sensors in Safety-Critical Environments

Wireless Sensors Networks and connected mass-consumers hardware for safety-critical environments have been demonstrated to be unreliable and require extensive support, despite decreasing the initial costs. These key findings and general trend shows that extensive scrutiny and extended support will be required in order to keep the security of these infrastructures up to date and avoid compromising these devices.

Figure 2 shows the roadmap proposed for IoT cyber-security in safety-critical environments. The roadmap demonstrates the basic principles of product development but integrates at the end of each stages meetings with a consortium of regulatory bodies in different fields such as the FAA, IAEA, and leading companies in order to improve upon the design of hardware and software. This will allow regulatory bodies to learn from each other and learn from their individual mistakes, thus making the focus of the roadmap on competency training, as proposed in different areas such as incident reporting [16], and situation awareness [17].

This roadmap focuses on competencies during the development of the product, hence enabling fast incident response, as well as improving the overall development and upgrade cycle.

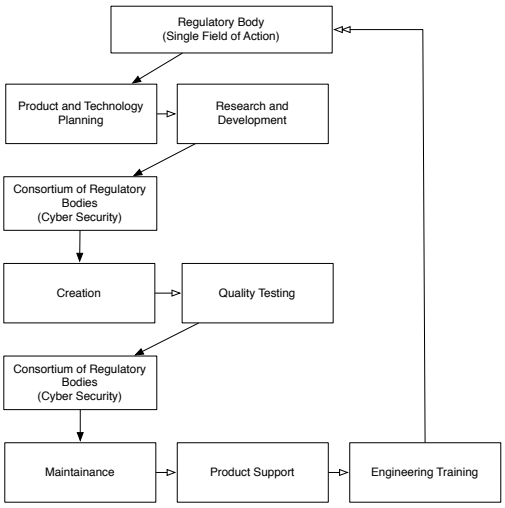

Fig. 2. Development Security Roadmap for IoT Devices

Our roadmap includes appropriate engineering training for all operators, in order to understand the flaws of the product and report them to the appropriate regulatory body for the second iteration of the product development or to integrate them for a future maintenance project. This technique also allows the appropriate regulatory body to report to the consortium and increase the resilience of safety critical environments against product flaws.

The roadmap is also extremely flexible as different steps can be added during the “Product Planning”, “Creation” and “Maintenance” and demonstrates adaptability allowing our roadmap to be used in different fields based on each requirements while increasing the cyber-security scrutiny and testing of each stages, improving upon each iteration.

IV. Cyclic Cyber-Physical Security model for Long Term IoT

The number of flaws will only increase with the amount of connected objects launched everyday and used in safety-critical environments. These findings are leading towards the need of a software and hardware security roadmap allowing companies to mitigate the risks and increase the resilience against cyber attacks [18].

In order to enable long term support and increase the longevity of the hardware and the software against cyber-attacks a cyclic cyber security model is proposed, building upon the IoT and WSN roadmap design.

The design of the cyclic cyber security model primarily improves upon the GateKeeper Reporting Architecture proposed by Johnson et al [19], which introduces regulatory bodies contact during or after an incident. The GateKeeper architecture also defines two types of incidents based on their severity. The improvement of the cyclic model over GateKeeper is the introduction of a consortium of regulatory bodies layer, and including an essential perspective on physical safety as well as a continuous feedback cycle. The regulatory body helps facilitates the communications between the different industries,

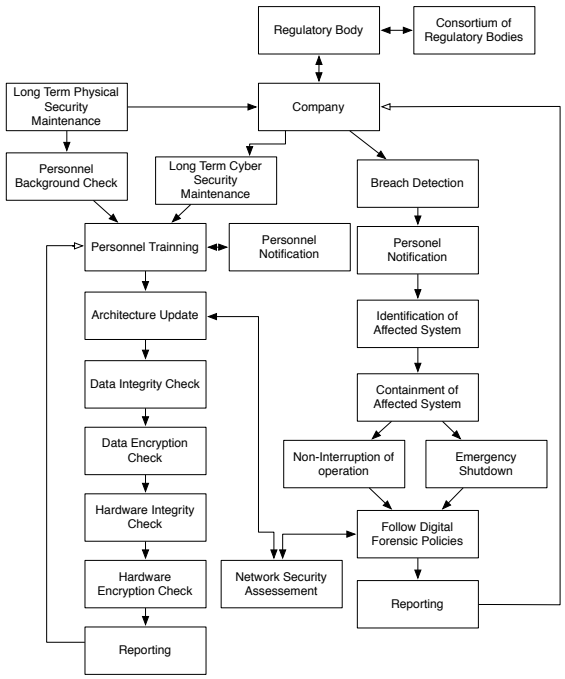

Fig. 3. Cyclic Security Model for Long Term IoT Support

hence increasing the resilience of industry towards cyber-threats, while the physical safety ensure proper training before and after maintenance of IoT devices.

The regulatory consortium also helps the redaction of agreements, clarifying the responsibilities of each of the actors, and establishing future cooperation between new comers and established public/private industry players [19].

The cyclic cyber-physical security model is designed to help engineers, operators and major company player to maintain the security level of the hardware and software, by applying good practices during the design of a product, enabling a constant assessment of the sensors deployed. This model also enables data and experience sharing. Allowing not only to learn from lessons during the engineering process, but also to learn from the security breaches detected and reported to the regulatory bodies, allowing more reactivity between the hardware and software manufacturers.

Figure 3 shows the cyclic security model proposed. On the top of Figure 3 the company is in charge of every operational decision regarding the long term cyber-physical maintenance, while constantly reporting towards its own regulatory body, which reports to the consortium of regulatory bodies. This technique allow a seamless integration of the lessons learned into the development roadmap and improves the reaction time, as each flaw is directly reported and broadcasted within the different regulatory bodies.

The regulatory bodies can also enforce manufacturers and companies using off-the-shelf hardware to apply appropriate security practices during the development process and help improve business to develop secure products for major safety-critical environments increasing market opportunities, and their client base while keeping mass-consumers safe as the development and deployment process undergoes thorough review.

Figure 3 also demonstrate that long term physical maintenance can be integrated within the long term cyber-security maintenance, as devices undergoing replacement require appropriate testing and need to be replaced by appropriate personnel with relevant qualifications.

The model also supports breach detections and helps companies and regulatory bodies to work together when a breach is detected, allowing a fast incident response process leading towards an incident reporting step. Private companies, and industry often lack of in-house forensic and incident response team, this can increase the response time, which, in a safety-critical environment is of high importance [20]. However, by enabling, communication between the cyber physical world, the companies, the consortium of regulatory bodies, and regional organisations such as Computer emergency response teams (CERT) and Computer Security Incident Response Teams (CSIRT), it is possible to enable a fast response action, limiting possible intrusion and incidents.

As companies will report directly to regulatory bodies, and be provided with help during an incident, the regulatory body will be able to provide immediate support during similar incidents. This will also enable a wide range a companies to benefit from to cyber-physical work achieved in other fields, and improve their overall cyber-physical incident response time. Hence improving the life-cycle of the IoT devices.

V. Conclusion

Off-the-shelve hardware and software are continuously integrated in high-risk environments helping companies to reduce deployment costs. The use of COTS devices raise significant security issues. This paper presented a roadmap for mitigating security concerns and flaws during the development process of IoT devices applied to safety-critical environments. Furthermore the paper presented a cyclic cyber-physical security model allowing operators, companies and regulatory bodies to communicate efficiently during and after the creation process, while allowing an extensive security scrutiny over the IoT system and during its lifetime.

The proposed technique is allowing companies to extend the longevity of their IoT hardware and software while maintaining a safe environment. The cyclic security model highlights the necessity to train personnel on-site and off-site in order to be able to distinguish between normal and abnormal behaviours. The training includes demonstrations of full incident response processes in highly guarded areas and comply with digital forensic policies required when breaches are detected.

The cyclic security model and the roadmap assumed that regulatory bodies, CERTs, and public/private companies will work closely in the future, assisting in both the investigation of cyber-physical incidents and enabling the communication between industries. The proposed approach can only succeed with an additional legislative layer, introducing responsibilities, when poor development, programming or maintaining techniques have been used, rendering IoT devices vulnerable to different types of attacks, hence decreasing their longevity.

REFERENCES

[1] R. C. D. Jr., C. Carver, and A. J. Ferguson, "Phishing for user security awareness," *Computers & Security*, vol. 26, no. 1, pp. 73 – 80, 2007.

[2] J. Knight, "Safety critical systems: challenges and directions," in *Software Engineering, 2002. ICSE 2002. Proceedings of the 24rd International Conference on*, pp. 547–550, May 2002.

[3] D. Deckstein, "The a380 delayed again: Airbus in a nosedive." http://www.spiegel.de/international/spiegel/the-a380-delayed-again-airbus-in-a-nosedive-a-422254.html, 2006. [Online; accessed 07-August-2015].

[4] W. A. Intra-Communications, "Wireless communications for safety-related avionics." http://waic.avsi.aero/, 2012. [Online; accessed 07-April-2015].

[5] N. Spring, "Opting for wireless technology." http://www.power-eng.com/articles/print/ volume-114/issue-2/features/opting-for-wireless.html, 2010. [Online; accessed 07-April-2015].

[6] C. F. G.-H. J. Garcia-Hernandez, J. C. Velazquez-Hernandez and M. A. Vallejo-Alarcon, "Design considerations for the implementation of a mobile ip telephony system in a nuclear power plant, nuclear power." http://www.intechopen.com/books/nuclear-power-control-reliability-and-human-factors/design-considerations-for-the-implementation-of-a-mobile-ip-telephony-system-in-a-nuclear-power-plan, 2011.

[7] P. W. HQ, "Exelons peach bottom power plant chooses polycom wireless communication." http://docs.polycom.com/global/documents/company/ customer_success_stories/enterprise /ex-elon_peach_bottom_power_plant.pdf, 2009. [Online; accessed 07-April-2015].

[8] PLatts, "Wireless monitoring making in-roads." https://online.platts.com/PPS/P=m &=1029337384756.1478827&e=1118939314184.-7636612064576698864/? artnum=20gB05Ma0LC608ty110641_1, 2005. [Online; accessed 07-April-2015].

[9] Y. K. Tan and S. K. Panda, "Optimized wind energy harvesting system using resistance emulator and active rectifier for wireless sensor nodes," *Power Electronics, IEEE Transactions on*, vol. 26, no. 1, pp. 38–50, 2011.

[10] C. M. Vigorito, D. Ganesan, and A. G. Barto, "Adaptive control of duty cycling in energy-harvesting wireless sensor networks," in *Sensor, Mesh and Ad Hoc Communications and Networks, 2007. SECON'07. 4th Annual IEEE Communications Society Conference on*, pp. 21–30, IEEE, 2007.

[11] M. Dalbro, E. Eikeland, A. in't Veld, S. Gjessing, T. Lande, H. Riis, and O. Sorasen, "Wireless sensor networks for off-shore oil and gas installations," in *Sensor Technologies and Applications, 2008. SENSORCOMM '08. Second International Conference on*, pp. 258–263, Aug 2008.

[12] R. Nasr, "Fiat chrysler recalling 1.4m vehicles amid hacking defense." http://www.cnbc.com/2015/07/24/fiat-chrysler-recalling-14m-vehicles-amid-hacking-defense.html, 2014. [Online; accessed 07-August-2015].

[13] A. Weimerskirch, "V2x security & privacy: the current state and its future,"

[14] E. Schoitsch, C. Schmittner, Z. Ma, and T. Gruber, "The need for safety and cyber-security co-engineering and standardization for highly automated automotive vehicles," in *Advanced Microsystems for Automotive Applications 2015* (T. Schulze, B. Mller, and G. Meyer, eds.), Lecture Notes in Mobility, pp. 251–261, Springer International Publishing, 2016.

[15] C. W. Johnson, "Barriers to the use of intrusion detection systems in safety-critical applications," 2015.

[16] C. Johnson and C. Holloway, "A roadmap for safer-systems engineering," in *System Safety, 2011 6th IET International Conference on*, pp. 1–6, Sept 2011.

[17] M. Evangelopoulou and C. Johnson, "Empirical framework for situation awareness measurement techniques in network defense," in *Cyber Situational Awareness, Data Analytics and Assessment (CyberSA), 2015 International Conference on*, pp. 1–4, June 2015.

[18] C. W. Johnson, "Contrasting approaches to incident reporting in the development of safety and security–critical software," 2015.

[19] C. W. Johnson, "Architectures for cyber-security incident reporting in safety-critical systems," in *Disaster Management: Enabling Resilience* (A. Masys, ed.), Lecture Notes in Social Networks, pp. 127–141, Springer International Publishing, 2015.

[20] D. Horn, "Taking the right approach to digital forensics," *Computer Fraud & Security*, vol. 2008, no. 12, pp. 16 – 17, 2008.