SAND2020-6994R

Sandia National Laboratories

The Rise in the Utilization of IoT Devices in Nuclear Facilities

C. Alan Runyan-Beebe

July 2020

Sandia National Laboratories is a multimission laboratory managed and operated by National Technology and Engineering Solutions of Sandia, LLC, a wholly owned subsidiary of Honeywell International Inc., for the U.S. Department of Energy's National Nuclear Security Administration under contract DE-NA0003525.

Issued by Sandia National Laboratories, operated for the United States Department of Energy by National Technology & Engineering Solutions of Sandia, LLC.

NOTICE: This report was prepared as an account of work sponsored by an agency of the United States Government. Neither the United States Government, nor any agency thereof, nor any of their employees, nor any of their contractors, subcontractors, or their employees, make any warranty, express or implied, or assume any legal liability or responsibility for the accuracy, completeness, or usefulness of any information, apparatus, product, or process disclosed, or represent that its use would not infringe privately owned rights. Reference herein to any specific commercial product, process, or service by trade name, trademark, manufacturer, or otherwise, does not necessarily constitute or imply its endorsement, recommendation, or favoring by the United States Government, any agency thereof, or any of their contractors or subcontractors. The views and opinions expressed herein do not necessarily state or reflect those of the United States Government, any agency thereof, or any of their contractors.

Printed in the United States of America. This report has been reproduced directly from the best available copy.

1. Overview

The term Internet of Things (IoT) encompasses everything connected to the internet, but it is increasingly being used to define objects that "talk" to each other. A broader term is that IoT are the devices that connect to each other and to the internet. It has been mentioned that IoT offers the potential for a "Forth industrial revolution" (1). This is primally because of the ease of use and quick link-up of devices within an area. This poses options for great interactivity but also create security concerns as many of these devices may not have been vetted for industrial use.

By allowing for the intercommunication of these devices and combining with automated systems, we can now gather information, provide analysis and create automotive actions. This allows for faster response times as well as lowering the overall cost for operations in nuclear power facilities. (2)

2. Advantages

Advantages of the combination of Artificial Intelligence (AI) blockchain registries with combined IoT are changing the way that industry and business sectors think of normal operations. According to the World Economic Forum (WEF), the Industrial IoT is forecast to add $14 trillion to the global economy by 2030 (2) (3).

For options of improvement in Plant operations, the innovation in IoT can enable for improvements in the fuel designs and technology integrations, plant operations, decommissioning processes, transport and storage (5).   IoT capable devices can provide data which can be collected and interpreted to lead to ad hoc analysis. These devices can also identify when there are potential issues with operations and provide notifications to operators on areas of improvement and even possibly have automated interventions without human interactions.

An interesting aspect that can assist is having the ability and flexibility of having analysis and monitoring of plant operations and its emissions remotely as these devices can now send information to cloud services and store data remotely.

3. Technologies being deployed in the nuclear industry

As the capabilities for networking industrial machines is growing, there have been great improvements in utilizing IoT to reduce cost and improve safety. Many commercial companies have produced surveillance tools to watch and catch possible issue much faster than traditional tools used in nuclear facilities. They have also built IoT devices that enable those traditional tools to become IoT devices. These advancements have made it possible for the interconnection, surveillance and cross-check across multiple devices. It has been stated that the deployment of IoT has become the new revolution to improve nuclear facility operations (6).

Demands for power plant automation is not going away and correctly harnessing the IoT into operations will be increasing. It is estimated that more than half of major new business will operate through IoT (7).

4. Security Evaluation before IoT deployment

Optimizing the use of existing technologies and identifying the technical readiness levels (TRLs) of IoT before deployment in the nuclear industry is paramount. With the quick rush to interconnective capabilities, not all devices will meet the security concerns that need to be put in place before implementation of IoT systems. Each innovation and devices need to be assessed in terms of safety, security and reliability, ensuring that efficiency of processes is improved while the same levels of safety and security are assured (6).

The development of IoT was originally focused on the consumer sector but has grown to benefit other business industries. A basic security concern is that because these were made more for the commercial retail market, the security of the information and connections to the network was not vetted to ensure that the data was safe. Many devices came out with little to no protections and information was completely open. In some popular IoT devices that allowed for audio communications, the devices would not turn off and there was no protection from external devices to access the audio settings on these devices. This laxed security standard in these devices allowed for illicit actors to gain personal information and exploit these features. As many people do not think of the security aspects of these devices, many of these open IoT devices allowed for open gates into networks and the ability to jump from these devices into more sensitive areas on the networks.

5. Case Study – Cyberattack on the Kudankulam Nuclear Power Plant

The plant was a stand-alone site and was not connected to outside cyber network or the Internet. Believing that cyberattacks could not be accomplished electronically from the outside, humans error and complacency created a crack in the local network at the plant. With this laxed process, one of the IT personnel brought in a flash-drive to assist in the updates with some of the computers. The flash-drive had malware that was introduced when this person downloaded the updates from the internet on their personnel computer. As mentioned by DHS, this is one of the methods that illicit cyber actors will enter into a system as they will utilize vendor-related software updates that have compromised (9).   Complacency is one of the biggest threats and the utilization of flash-drives is considered an air gap and creates this sense of complacency that will allow for virus to enter a system.

6. IoT Risk and Risk Mitigation

Regardless of the needs for IoT, there is a risks to utilizing and implementing IoT technology in nuclear facility that needs to be addressed in the sites communication security plan. Before the deployment of these devices, the cybersecurity teams need to identify the risk in the utilization of IoT and provide a mitigation plan to prevent and deter illicit activity that may take advantage of these deployed devices. As these devices have increase capabilities of providing more data and analysis, plans should also address the protection of data processing and information transmission to data centers that may no longer need to be at the facility. As stated in a recent report “There is a very clear danger that technology is running ahead of the game (1)."

Understand that there is increased risk in the utilization of IoT devices at nuclear facility and that there needs to be an evaluation whether the benefits outweigh the danger that these devices can create. With the right mitigation plans that are reviewed and updated on a regular basis, this will assist in preventing new cyber-attacks.

Another area of concern with the utilization of IoT is not just in the deployment at the industrial level but the accidental introduction of network virus onto the system through human error. In the short case study above, it was discussed that the nuclear power plant had processes in place that prevented the site from having access to external networks or the internet. Through human error, a person was allowed to introduce a virus into the system.

With the increase in technologies, cloud computing and the utilization ease of IoT connections, the introduction of illicit code and cyber-attacks is increasing. Personnel that work at the nuclear facilities may inadvertently introduce virus just through the utilization of the wearable IoT devices (5) (1). Most people have smartphones as a minimum for daily life. Many have watches that have IoT type communications. The availability of these wearable IoT devices is increasing as more companies develop commercial market goods. To prevent these devices from inadvertently trying to connect to a sites network, training and surveillance of these devices needs to be addressed in the risk mitigation plan. The Cybersecurity teams need to understand that these devices may be allowed at a site but there needs to be training of all the staff on the security risk that they may pose as well as provide how they might reduce that risk.

7. Summary

As mentioned at the beginning, the IoT industry is dramatically increasing and the capabilities to improve the nuclear industry is apparent. With the initial development of IoT to be focused on the retail market, the growth of security in the systems has been lagging. Now that these devices have shown great opportunities to increase revenue and lower overall cost, there needs to be discussions on the risk of the implementation of these devices. There also needs to be training with nuclear facility staff on the use of wearable IoTs that may compromise the sites network and computer systems by inadvertently providing gaps in the security infrastructure.

8. Works Cited

1. **Burgess, Christopher.** What Happens When The Internet of Things Crashes? *Clearance Jobs.* [Online] 10 24, 2016. https://news.clearancejobs.com/2016/10/24/ddos-attack-dyn-leveraged-iot/.

2. **KhaledSaab, Abraham Clements, and Saurabh Bagchi.** *Benchmark for Security Testing on Embedded Systems.* Albuquerque : Sandia National Laboratories, 2016. SAND2016-7135A.

3. **World Economic Forum.** Shaping the Future of Technology Governance: IoT, Robotics and Smart Cities. *World Economic Forum.* [Online] 2020. https://www.weforum.org/platforms/shaping-the-future-of-technology-governance-iot-robotics-and-smart-cities.

4. **Sandia National Laboraotries.** *Internet of THings will thrive by 2025-Pew Research Center.* Albuquerque : Sandia National Laboraotries, 2015. SAND2015-9765A.

5. **Conca, James.** How Well Is The Nuclear Industry Protected From Cyber Threats? *Forbes.* [Online] 11 08, 2019. https://www.forbes.com/sites/jamesconca/2019/11/08/how-well-is-the-nuclear-industry-protected-from-cyber-threats/#4edefb433497.

6. **IEEE Computer Society.** *Top 10 Technology Trends for 2018: IEEE Computer Society Predicts the Future of Tech.* Los Alamitos, California : IEEE Computer Society, 2017. SAND2017-13665M.

7. *IoT Security: The Internet of Other People's Things.* **Jack Wampler, Thanh Nguyen.** Albuquerque : Sandia National Laboratories, 2016. SAND2016-7015.

8. **Robbins, Melissa.** Cyberattack Hits Indian Nuclear Plant . *Arms Control Association .* [Online] 12 2019. https://www.armscontrol.org/act/2019-12/news/cyberattack-hits-indian-nuclear-plant.

9. **Security, Dept. of Homeland.** Cybersecurity & Infrastructure Security Agency. *CISA.* [Online] 2020. https://www.cisa.gov/.

10. **Todd, Felix.** What impact is the IoT having on the nuclear sector? *NS Energy.* [Online] 08 08, 2019. https://www.nsenergybusiness.com/news/iot-nuclear-sector/.