ARC INSIGHTS

APRIL 24, 2014

Securing the Internet of Things

By Sid Snitkin

Keywords

Internet of Things, IoT, Cyber Security, Industrial Cyber Security

Overview

The Internet of Things (IoT) was a key topic at the ARC Advisory Group 2014 World Industry Forum in Orlando. Throughout the conference, speakers and attendees discussed the explosion in the number of connected devices (industrial and otherwise) and the burgeoning amount of data being generated. Security was a common concern and standing-room-only attendance at the "Securing the Internet of Things" session helped underscore the importance this issue has on IoT adoption.

This report summarizes the presentation and panel discussions in the "Securing the Internet of Things" session at the recent ARC Advisory Group 2014 World Industry Forum in Orlando. It provides useful insight into end user concerns about the use of IoT devices within industrial plants and the strategies automation vendors are using to alleviate them.

While IoT spans many devices and applications, the "Securing the Internet of Things" session focused on the use of IoT in industrial plants. This included an excellent presentation by Mark Conde of Universal Parks and Resorts and a lively panel discussion of automation vendor IoT strategies and end user concerns.

Security Is Essential and Challenging at Universal Parks and Resorts

Safety is fundamental to the success of any theme park. Guests want thrilling experiences but even minor accidents can quickly undermine a park's reputation. Availability and reliability are also critical, particularly in popular park attractions. With over 30,000 guests a day, the immediate, financial impact of out-of-service venues can be enormous for Universal Parks and Resorts. Impact on customer satisfaction is equally important as it drives future revenues.

Universal Parks and Resorts understands that security is fundamental to ensuring safety, availability, and reliability. The organization also appreciates the complexity of its industrial cyber security challenge. They have a multitude of independent control systems that utilize a wide range of equipment from a variety of automation vendors. The themes and appearance of rides and attractions change periodically, but underlying control systems generally remain the same. This requires cyber security strategies that support a blend of legacy and new automation devices, controllers, and networks.

A particularly challenging, security aspect of theme parks is that guests are free to roam throughout the park and connect personal devices to public Wi-Fi networks. Not surprisingly, some guests also try to penetrate control system networks. This parallels many of the concerns that users have with industrial IoT.

A particularly challenging, security aspect of theme parks is that guests are free to roam throughout the park and connect personal devices to public Wi-Fi networks. Not surprisingly, some guests also try to penetrate control system networks. This parallels many of the concerns that users have with industrial IoT and made Mark's presentation an excellent kickoff point for the discussions in this Forum session.

Useful Lessons Learned at Universal Parks and Resorts

Universal Parks and Resorts' cyber security strategy focuses on addressing three key issues:

- **What is our exposure?**
  - What types of threats exist?
  - Which threats are we susceptible to and what is the potential impact?
  - How can these threats get into the environment? (e.g., what are the points of access?, etc.)
- **How do we address these threats?**
  - What changes can/should be adopted and where? How to address these threats in legacy and new systems? (audits, scans, etc.)
  - Who should lead this effort? (internal or external resources)
- **What needs to be done to maintain our security?**
  - Any new approaches needed for system implementation and management?

- How can this effort be sustained? (committed resources)
- What is an appropriate budget for defense?

Key lessons learned from Universal Parks and Resorts application of this strategy include:

- Safety networks should be isolated and secured. Periodic audits are also required.
- Adopt proven technologies wherever practical and don't reinvent the wheel.
- Maintain constant surveillance of all systems to ensure that threats are quickly detected and addressed. Analytics can be extremely valuable in detecting, troubleshooting, and managing intrusions.
- It is better to keep cyber security management in-house as opposed to relying upon external resources. This approach also requires executive sponsorship.
- Good security management requires collaboration among IT, automation, and operations groups. The best group to lead this effort depends on the organization and the knowledge of the people.

Automation Vendors Embrace IoT Concepts

Representatives from three leading automation companies joined Mark for a panel discussion on IoT and control systems. Each provided a brief overview of their company's IoT strategy and the growing need for process information sharing across the internet.

Peter Zornio described Emerson's "Pervasive Wireless" strategy, which enables broader use of sensors in industrial facilities for monitoring process and equipment condition. Much of this additional information is non-mission critical and separated from control systems, which makes security less of an issue and enables safe sharing with external systems and personnel.

Ashok Acharya of GE Intelligent Platforms focused his comments on the "Industrial Internet." While process monitoring is a key benefit of this IoT strategy, the potential performance benefits are the fundamental driver for exposing more process information. To that end, GE's strategy includes higher level optimization solutions that leverage information collected from multiple machines and sites.

Key Panel Discussion Takeaways:

1. Industrial IoT is a clear trend
2. Industrial IoT can be secure
3. Each organization needs its own strategy
4. Security must be managed internally
5. Security is a shared responsibility between vendors and operators

Rockwell Automation's Mike Hannah focused his remarks on the company's "Connected Enterprise" IoT strategy. This recognizes the burgeoning use of embedded intelligence in control system components and the significant performance benefits that can be achieved when connected devices, people, and processes can share information.

Secure Industrial IoT Is the Future for Control Systems

Following these introductions, the panel commented on Mark's presentation and responded to a variety of questions from attendees and the ARC moderator. Some of the key takeaways from these discussions include:

- The trend towards more sharing of control system information is clear and strong.
- Information can be shared securely if the organization develops an appropriate cyber security strategy and diligently follows it.
- While information sharing will become pervasive, strategies will vary across industries and organizations. They will reflect differences in the opportunities for performance improvement, regulatory restrictions, and the need to protect intellectual property.
- Given the need for information sharing, people will eventually embrace good security practices. This will parallel the shift that occurred in safety management as people understood that security is everyone's responsibility and demands continuous attention.
- Given the importance of security, management of industrial IoT programs will generally remain within the organization ("You can't outsource safety and you can't outsource security.").
- While vendors should be held accountable for providing secure systems, owner-operators have the ultimate responsibility for ensuring that these capabilities are used. For example, vendors need to enable robust access protection, but owner operators need to ensure that passwords are protected and changed on a regular basis.

Openness Reduces Cyber Security Risk

"Open systems are more secure than closed systems," was a theme that reverberated throughout the "Securing the Internet of Things" session. Not

While counterintuitive and conflicting with commonly held views, panelists made a strong case for the inherent security benefits of industrial IoT strategies.
They were unanimous in their belief that organizations that enable accessibility are more secure than those that follow protection through isolation.

surprisingly, this position was met with some skepticism, since it conflicts with commonly held views that security is one of the biggest hurdles that IoT must overcome for widespread adoption. ARC's analysis of this situation suggests that the two positions can be reconciled by considering the differences between general-purpose IoT and industrial IoT.

For many people, IoT means billions of independent, smart devices connected directly to the Internet. Such devices clearly have to be protected against malware infiltration and information exfiltration. The diversity of devices and general lack of overall standards creates an enormous security challenge for device designers and owners alike. Direct, unmanaged connection to an internet polluted with hackers further heightens the likelihood of security breaches and raises the risk profile for general-purpose IoT.

Industrial IoT represents a different, more controlled, application of this technology that can be secured. Smart devices are applied, but only within the confines of a managed environment. While the associated information is communicated to external systems via the Internet, these connections are still managed to ensure end-to-end security. Many industrial IoT use cases are also unidirectional, providing non-critical information to external sites for troubleshooting and performance improvement. When bi-directional exchanges are used to optimize performance, the integrity of control commands is always guaranteed through security techniques like VPN and encryption.

Considering this industrial view of IoT, it is understandable that automation vendors and knowledgeable end users like Mark Conde are confident about the ability to manage security. Successful intrusions like Stuxnet show that isolation does not guarantee security. Organizations with industrial IoT strategies have the opportunity to leverage system accessibility for real-time monitoring that enables faster detection, identification, and resolution of problems. This reduces the impact of any security breech and thus cyber security risk, which is the combination of intrusion likelihood and impact. Based on this, it's clear that organizations with industrial IoT strategies can ultimately be more secure than those that continue to use closed systems.

Recommendations

The lively and informative ARC Forum session on IoT security addressed a variety of issues of importance to end users. It reinforced ARC's view that future control systems will support broad information sharing with external systems. This shift to industrial IoT will not undermine system security. On the contrary, industrial IoT will reduce the risk of damaging cyber attacks by enabling cyber events to be detected, analyzed, and resolved faster and more effectively. Considering this, ARC recommends that clients consider how they can leverage openness to improve the cyber security of existing systems. Similar consideration should be given to the design of new systems.

While adoption of industrial IoT will be universal, deployment strategies will vary among organizations. Potential benefits are different and each organization will need to decide what information to share and how those channels will be protected. ARC encourages clients to prepare themselves for these developments by reading the various industrial IoT reports ARC will be publishing and attending future ARC forums. Building on the work of others can save you time and money.

For further information or to provide feedback on this Insight, please contact your account manager or the author at srsnitkin@arcweb.com.