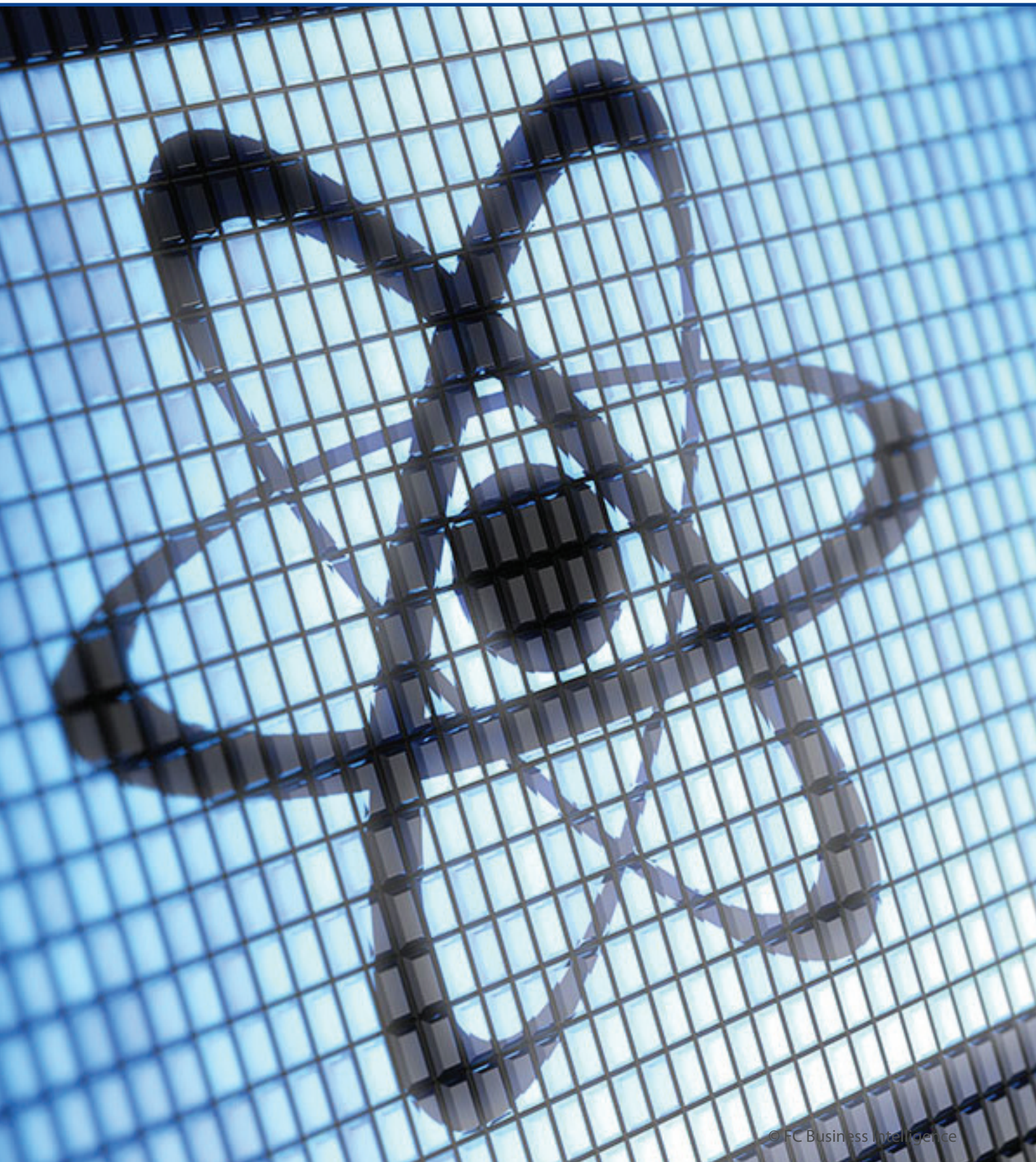
NUCLEARENERGY INSIDER

Cyber security and the Digitization of Nuclear Power Plants



NUCLEARENERGY INSIDER

Cyber security and the Digitization of Nuclear Power Plants

At the annual Nuclear Security Summit held in Washington D.C. in April last year, the U.S. and U.K. governments announced plans to hold a joint civil nuclear exercise in 2016 that will test government and industry response to cyber security threats.

In recognition that nuclear facilities now deploy a multitude of digital technology and assets to improve the efficiency and performance of industrial control systems (ICS), the U.S. and U.K. are urging the industry to ensure these critical systems can withstand malicious attacks or accidental damage from any origin.

Cyber security solutions that mitigate risk to vulnerabilities in information management systems have been spotlighted as needing to be extended to cover ICS. These solutions are increasingly pertinent to a rapidly developing digital arena, which now encompasses Internet of Things (IoT) and the cloud.

The latest digital innovations such as IoT are already being deployed at nuclear facilities, as operators move to optimize performance in an increasingly competitive energy market. However, in an industry that faces global scrutiny, a strict regulatory framework and high safety and security standards, the nuclear industry must tread carefully in its uptake of digitalization. Constant reminders of the cyber security challenges that arise with a move towards digital systems remain a contentious point amongst nuclear experts.

Nevertheless, the nuclear industry is beginning to wake up to the potential of digitalization. Many operators have initiated various programs that employ innovative strategies and cutting-edge data analytics to minimize downtimes and drive down maintenance costs.

Cyber security will need to be central to digital strategies if costly and potentially devastating effects of threats emerging alongside the innovative technology are to be avoided.

Cyber Security: Emerging Threats

Attacks common across power utilities target business networks and customer data, as well as critical control systems to disrupt electricity supply. The nuclear industry has the added risk of an attack that tampers with reactors and triggers catastrophic radiation dispersal.

Major known attacks on nuclear facilities include:

- 2010 Stuxnet worm breached air-gapping to attack uranium enriching centrifuges in facilities in Iran
- 2014 Malware hidden in phishing emails breached data files at Korea Hydro, South Korea
- 2016 Malware-infected portable USB drives found in RWE's Gundremmingen plant in Germany

Several reports into cyber security and its application to protect business networks and ICS have contributed to the knowledge of emerging threats and steps that can be taken to prevent and mitigate the risks.

NUCLEARENERGY INSIDER

Cyber security and the Digitization of Nuclear Power Plants

From this research, IoT and the operations technology (OT) interface with information technology (IT) are likely to come under more scrutiny by nuclear utilities as they progress towards greater integration of digital technology.

Internet of Things

IoT is the online connectivity between a system of physical digitized devices such as computers, smart phones and sensors that creates a network over which these devices collect and exchange data. Data collection and exchange can take place without human-to-human or human-to-device interaction.

In 2015, the International Data Corporation (IDC) forecast the global IoT market will grow from $655.8 billion in 2014 to $1.7 trillion in 2020, a compound annual growth rate of 16.9%. Modules, sensors, connectivity devices and IT services are expected to account for more than two-thirds of the market, with modules and sensors set to represent 31.8% of that total.

In July 2016, the Royal Society published a report on cyber security research challenges predicted to emerge over the next five to ten years. The research highlights the global impact of digitization and IoT, citing that as many as 15 billion devices are already online and up to 50 billion are expected to be connected by 2020.

The report prioritizes addressing any gaps in the security and reliability of cyber-physical systems, including IoT. Although greater connectivity within operations increases functionality and efficiency, it also heightens vulnerabilities in the system to a breach and the report recommends further engineering research to develop new defences against a cyber-physical attack.

Operations Technology interfacing with Information Technology

The independent U.K. think tank Chatham House conducted interviews on cyber security with civil nuclear industry personnel in the U.S., Canada, France, Germany, Japan, Russia, Ukraine and U.K. The 2015 report warned of a growing risk as nuclear facilities implement digital systems using commercial software, which is less costly than a customized solution but amplifies exposure to attacks.

The authors caution against relying on air-gapping to protect the ICS by isolating it from public networks. In realizing the commercial benefits of internet connectivity, the surface area vulnerable to threats expands, as other often undocumented or forgotten connections are installed by legitimate third party contractors.

The report identifies a number of industry-wide challenges including different working cultures and practices particularly evident between OT engineers and IT engineers designated as cyber security personnel. Difficulties communicating, limited interaction and conflicting priorities, often

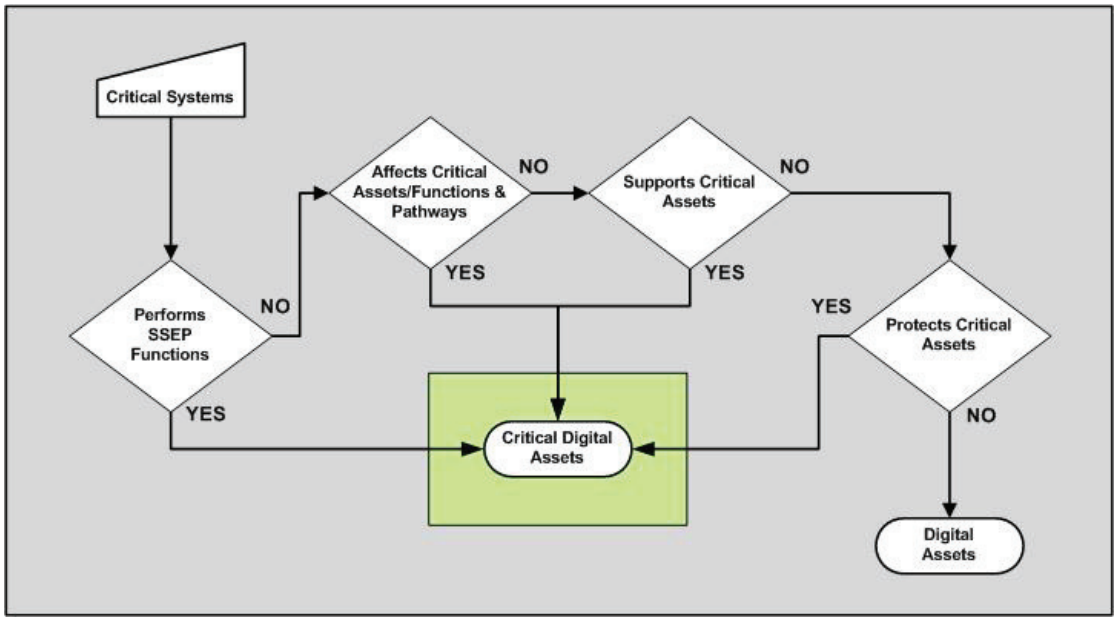
exacerbated by IT staff located off-site, have led to misunderstandings that escalate into continued friction.

OT engineers prioritize the safe, efficient and continuous running of the plant, whereas the main priority for IT engineers is security. Adding security to a device could invalidate its safety approval or show unexpected incompatibilities between the security and safety systems, especially if the device is connected to the network to facilitate access to the data it is generating. Implementing IoT solutions, with its throng of new devices, is likely to further complicate the relationship.

Cyber Security: Strategy and Implementation US Nuclear Regulatory Commission

In 2009, the Nuclear Regulatory Commission (NRC) published cyber security rules specifically targeting the protection of computer and communications systems and networks. The rules incorporated lessons learned form cyber security orders imposed after the September 2001 terrorist attacks.

All plant operators must implement an approved cyber security plan that is reviewed and inspected by the NRC. Regulatory guidance (RG 5.71) was issued a year later in January 2010, which included best practice notes from the U.S. Department for Homeland Security (DHS) and NEI.



Source: Regulatory Guide 5.71: Cyber Security Programs for Nuclear Facilities, Nuclear Regulatory Authority January 2010]

The guidelines highlight the need to maintain the approved cyber security program, performing continuous monitoring and assessment. The plan must be updated to reflect changes that could expose the plant and its systems to attack.

Cyber security and the Digitization of Nuclear Power Plants

Digitizing O&M by deploying innovative technology such as IoT and cloud computing could prompt a change to cyber security plan to ensure the plant remains protected from cyber security attacks.

David McIntyre, Public Affairs Officer: The staff is not planning on any new power reactors cyber security regulations at this time. We believe that the current regulations are already robust and broad enough to cover new IT developments and keep the licensees' systems secure.

If a licensee adopts a new IT development such as cloud computing, they will evaluate their implementation. If necessary, they will submit a cyber security plan change. At that time the staff will review the change and, of course, our inspections would cover any changes.

Enterprise Strategy Group, Inc.
Jon Oltsik, Senior Principal Analyst

Enterprise Strategy Group (ESG) is an IT analytical, research, validation and strategy firm that provides market intelligence to the global IT community. CISCO Systems, Inc, the world's largest networking technology company, commissioned ESG to research and assess the impact of IoT on large organizations from a chief information and security officer (CISO) perspective.

The research concludes that any enterprise engaging with IoT introduces new cyber security concerns. The vast array of non-uniform devices, new protocols and network traffic increases the overall threat surface and adds new risks that reach beyond IT assets and sensitive data.

Malware is already designed to penetrate traditional network security control such as firewalls. IoT could create more opportunities for networks to be compromised, as devices run embedded operating systems and applications that often have few malware detection or prevention capabilities.

Large organizations will not only have to manage these new risks, but also become more sensitive to how these threats are managed from both an IT and OT perspective. As already highlighted, there can be a disconnect between OT and IT that needs to be addressed to ensure robust cyber security.

	Information Technology	Operations Technology
Business role	Supply technologies for revenue generation and cost control. Tends to be fairly common across industries.	Control technology used to supply a "product" (i.e., electricity, refining, logistics, etc.) or manufacturing process. Tends to be very specific to an industry.
Focus	Discrete IT assets (i.e., servers, storage, endpoints), or functional services (i.e., application development, networking, security, etc.).	Physical equipment or process focus, typically across a "system" of technologies.
Security realm	Data and IT assets.	People and physical equipment.
Technology	Mostly modern equipment with regular replacement cycles. Standard systems, tools, and protocols.	Can include older technologies with long lifecycles. Often use specialized equipment, tools, and protocols

Source: Enterprise Strategy Group, 2014]

NUCLEARENERGY INSIDER

Cyber security and the Digitization of Nuclear Power Plants

OT and IT are intertwined and although IoT devices have different missions and protocols, they are all connected over a common internet protocol (IP). IT staff are trained to take immediate action if a potential breach is detected, which that can include placing a device in quarantine or taking it offline.

OT has to have resiliency. If a nuclear power plant that is supplying power to a major city is being attacked, it cannot just be taken down and turned off. CISOs will need policies and processes to work around these IT and OT differences to ensure there is an appropriate response for the multiple and varied cyber security requirements across both areas.

The nuclear power industry understands there is a weak link in IoT, but there needs to be a greater understanding of the scope of that link, which stretches from devices to programmable logic controllers (PLCs) that control these devices and onto the internet.

Anything connected to the network is connected to the internet, which is a jumping off point for an attack. The variety of IoT device types, locations and security profiles will demand dynamic policy enforcement based on the trustworthiness of the devices and integrity of IoT data.

To support bridging a potential gap between OT and IT personnel, CISOs will need an IoT plan that addresses the new technologies, processes and cultural changes. Existing cyber security that is typically IT-centric will need to be balanced with a more OT-centric strategy.

Opportunities that use IoT to improve overall cyber security also need to be explored, as it may be the most suitable vehicle to integrate physical, cyber and industrial security into common standards, processes and technologies. IoT could drive an impetus to have tighter control over access to data generated by the array of devices on the network, as well as to have trusted authentication.

Segmentation of the network without disrupting access is also improving and as data are processed and analyzed more efficiently, security breaches are more likely to be identified more rapidly enabling a more timely response to limit any damage. Although there need to be standards set for IoT security and design, all these factors delivered by IoT could improve cyber security.

Owl computing Technologies, inc.
Scott Coleman, Marketing Manager

Owl Computing Technologies, Inc. is a provider of cyber security solutions that use data diodes to secure operational networks of critical infrastructure operators. Data diodes, which are installed in every U.S. nuclear facility, protect the plant by allowing data to only flow outwards so potentially harmful data cannot flow back in. Owl solutions are deployed in around 75% of U.S. operating plants.

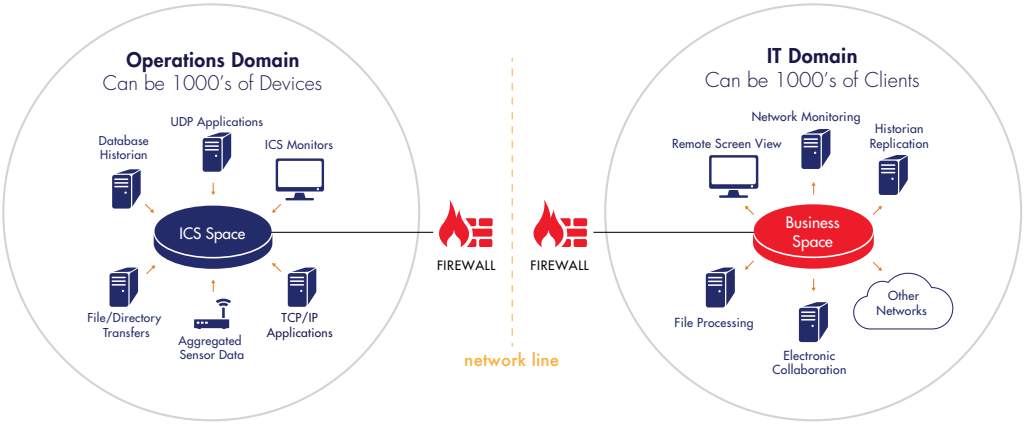
Cyber security threats broadly fall into two categories: external advanced persistent threats and insider threats, which can be further categorized as unintentional and intentional threats.

NUCLEARENERGY INSIDER

Cyber security and the Digitization of Nuclear Power Plants

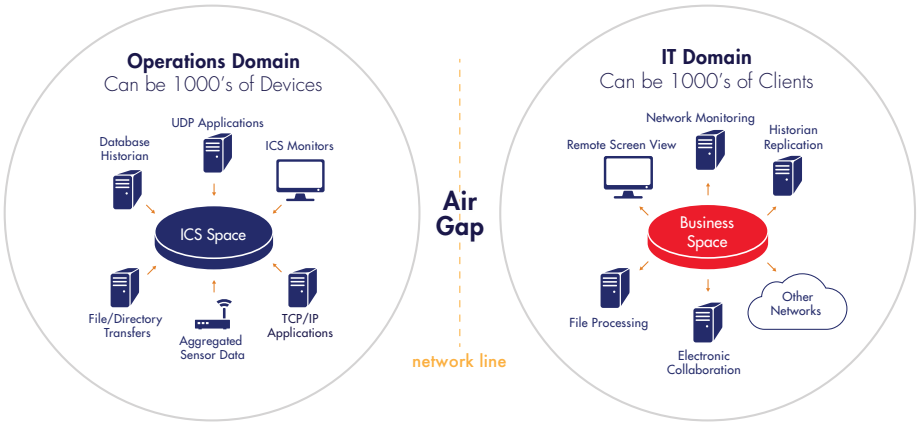
ADOPTING NEW NETWORK ARCHITECTURE SECURITY

1 TYPICAL VULNERABLE TWO-WAY NETWORK CONNECTION



- Two-way connections between the plant and business networks
- Network connection supports business efficiency
- Networks are vulnerable to cyber attack

2 NETWORK SEPARATION



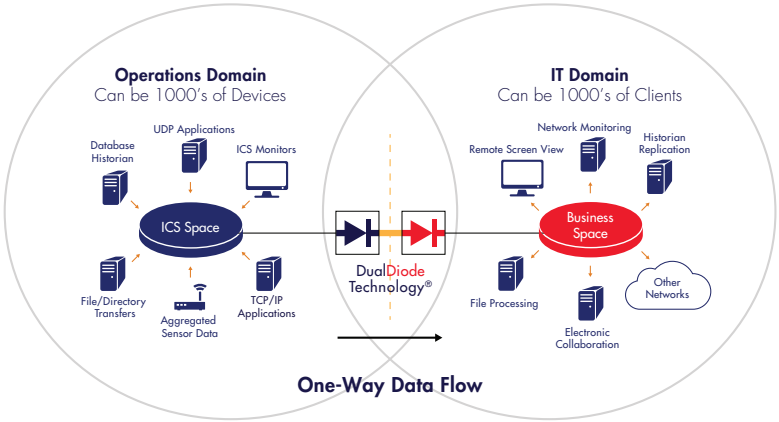
- Disconnection impedes business efficiency
- Not an operationally acceptable solution
- Need to strike a balance between security and efficiency

www.owlcti.com

External advanced persistent threats are ever-changing and progressing at unprecedented rates: today's zero day attack is tomorrow's cyber attack to be copied and deployed at an even more rapid rate. Ransomware is being deployed at alarming rates, with adversaries looking for small sums of money to provide keys to encrypted data.

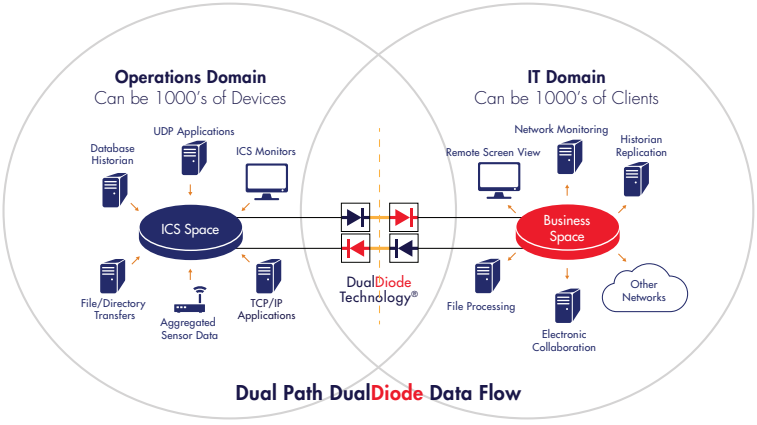
TECHNOLOGY ST ALLOWS OT AND IT EFFICIENCY

3 PLANT NETWORK PROTECTED BUT DATA FLOWS



- Security maintains "disconnected" plant network
- Information flows to support business efficiency
- Better security permits OT and IT to coexist

4 EFFICIENT SECURE ARCHITECTURE



- Security maintains a "disconnected" network
- Information flows to support business and plant efficiency
- Best security permits OT and IT efficiency

www.owlcti.com

This indicates a rise of "small time" attackers looking to make small sums of money for their efforts. Recent elaborate social engineering efforts to gain access and control of ICS via more sophisticated means also prove the real threat of other motivated adversaries.

The wide spectrum of threats puts a significant burden on nuclear security staff and their budgets. This burden also creates a threat within the industry if not planned for and managed correctly. Time

Cyber security and the Digitization of Nuclear Power Plants

and costs burdens are alleviated by Owl's one box solution that is simple to install and set up the data diode, as well as being simple and low maintenance to run.

At the convergence point of OT and IT is security technology (ST) and this is where operational challenges in adhering to NRC regulations exist everyday. Implementing changes that adhere to the guidance is a long-term process and cannot be completed within a few short years.

Regulatory reporting, insider threat protection and the deterministic isolation of critical cyber assets are a few examples of the continued challenges that asset owners face. Yet, nuclear asset owners, along with the NRC, are leading the way with creating a framework of best practices.

Cyber security strategies all have plant safety as their primary goal. Plant security is critical to plant reliability, which is a major aspect of plant safety so both physical and cyber security play an integral role in ensuring the plant remains safe to operate.

Cyber security systems need elements of system and cyber asset confidentiality, while maintaining very high levels of system integrity and providing for the availability of the systems to perform their functions. They also need to allow all plant staff to get their jobs done.

Beyond plant perimeter cyber security, additional efforts are needed to secure extra networks within the plants and critical cyber assets within the plant. Owl stays focused on developing and delivering the cyber security products needed to support these tasks.

Forward progress that ensures the continued cyber security of nuclear operations will be advanced by listening to the needs of and threats to the markets. Owl will continue to keep a pulse of advancing threats to the operators and the cyber security solutions needed at the intersection of IT and OT.

OSISOFT, LLC.
Steven J Sarnecki, Vice President of Federal and Public Sector
Christopher Crosby, Principal, Global Nuclear and Renewable Energy

OSIsoft, LLC. is a leader in delivering operational intelligence. Its PI System, an open enterprise infrastructure, connects sensor-based data, systems and people, and delivers real time, actionable insights that empower companies to optimize and transform their business.

The NRC selected OSIsoft to modernize its existing Emergency Response Data System (ERDS) with the PI system in 2006, and the company now provides centralized monitoring for all operationing U.S. nuclear power plants.

Cyber security is not a project; it is a process and one of continuous improvement. The use of portable media, personnel training and hiring, and bad actors are all examples of factors that must be accounted for in the overall program.

Cyber security and the Digitization of Nuclear Power Plants

The strategy must consider business networks interfacing with sections of the control system network (CSN), especially if IoT sensors are streaming data across the two systems. Access to the CSN must be secured against the threat of social engineering attacks such as phishing that target the data held on the business network.

Cyber adversaries will try to map out employee habits and work patterns that can be used to penetrate the business network and access the data. People with access to the CNS must be properly trained in cyber security protocols to ensure it remains protected.

The uniqueness of a control system is not, in itself, a secure system. Utilities can no longer hide behind isolation, as new systems are based on common text and common platforms. Everyone is using the same sensors and shared compatibility is the biggest threat to cyber security.

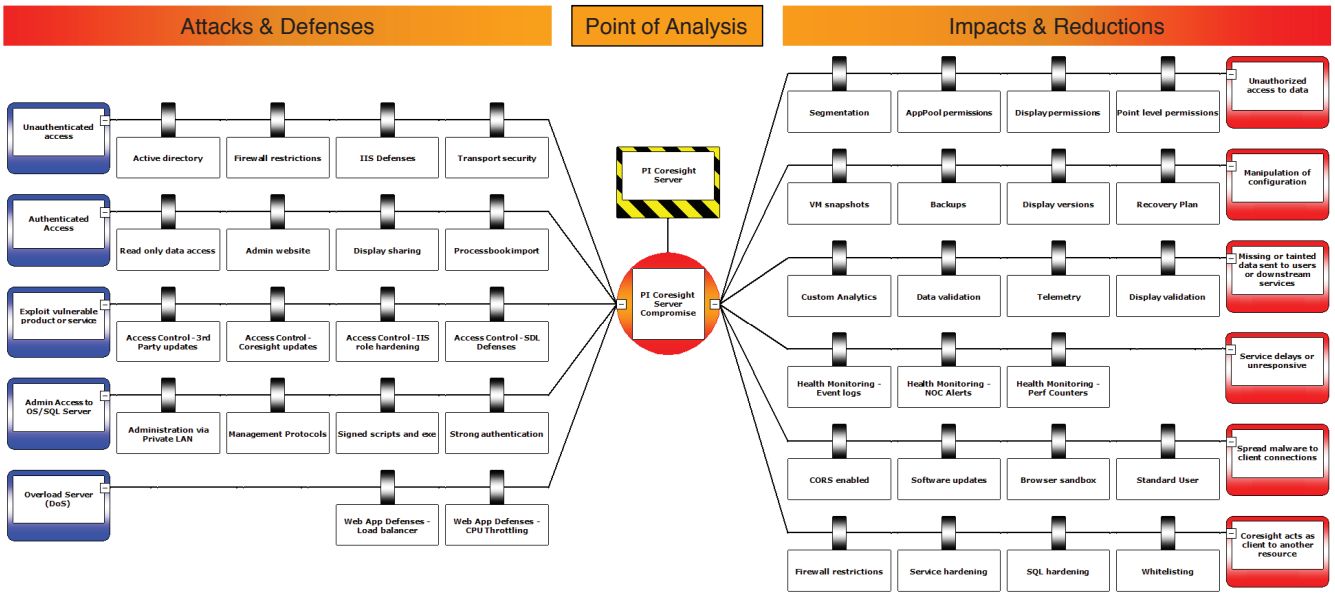
OSIsoft has increased the number of sensors in a plant, which has expanded the volume of data and decision points. This improves working efficiency, but every sensor becomes an exposure or a threat if not managed well.

PI software architecture is at the bridge between OT and IT with the ICS protected by mirror architecture, as well as data diodes supplied by security specialist partners. Data are streamed in real-time from operational sensors and relayed one-way to a replica PI System that is not digitally connected to operations, which enables the monitoring and analysis of data without the risk of breach.

Data traffic is also monitored for quality and consistent patterns, so atypical patterns that could point to someone or something interfering with the flow can be identified in real time. As breaches are often diagnosed after the event, sometimes months afterwards, real time awareness is crucial as it allows more immediate intervention and damage limitation actions to be taken.

The US is in a good place. It is challenging people to think about the supply chain and not just the physical plant. We need to be sure that operational procedures are in place and all the safeguards are being maintained and audited on a regular basis.

Cyber security and the Digitization of Nuclear Power Plants



Keep the bad guys out

But if they get in, limit the damage

NUCLEARENERGY INSIDER

Cyber security and the Digitization of Nuclear Power Plants

LIST OF ACRONYMS

CISO	chief information and security officer
CSN	control system network
DHS	Department for Homeland Security
ESG	Enterprise Strategy Group
IAEA	International Atomic Energy Agency
ICS	Industrial Control System(s)
IDC	International Data Corporation
IoT	Internet of Things
IP	internet protocol
NEI	Nuclear Energy Institute
NRC	Nuclear Regulatory Commission
O&M	operations and maintenance
PLC	programmable logic controller(s)
ST	security technology

REFERENCES

International Data Corporation, Inc.; Worldwide Semiannual Public Cloud Services Spending Guide. An IDC Database product, January 2016.

The Royal Society; Progress and Research in Cyber Security: supporting a resilient and trustworthy system in the UK, July 2016.

The Royal Institute of International Affairs (Chatham House); Cyber Security at Civil Nuclear Facilities: Understanding the risks. Caroline Baylon, with Roger Brunt and David Livingston, September 2015.

U.S. NRC: 10 CFR 73.54: Protection of Digital Computer and Communications Systems and Networks [74 FR 13970, Mar.27, 2009; 80 FR 67275, Nov.2, 2015].

U.S. NRC: RG 5.71: Cyber Security Programs for Nuclear Facilities

CISCO Systems, Inc. and Enterprise Strategy Group, Inc.; A White Paper: The Internet of Things: A CISO and Network Security Perspective. Jon Oltsik, 2014.

NPDC | NUCLEAR PLANT DIGITALIZATION CONFERENCE

Researched & Organized by: NUCLEARENERGY INSIDER

13-14 November, 2017 | The Hilton City Centre, Charlotte, NC, USA

Register by September 22nd and SAVE $400 on your pass

DIGITAL INNOVATION TO DELIVER COMPETITVELY PRICED NUCLEAR POWER

It's clear that if nuclear companies want to increase economic efficiency and be competitive, they need to understand and implement digital systems... and fast. The Nuclear Plant Digitalization Conference is North America's number one plant digitalization conference, where over 250 key decision makers gather from the most forward thinking utilities, innovative tech companies and integrated service providers.

- **Transform business operations through a holistic digital strategy:** Prepare for the new age of The Digital Plant and understand how digitalization is crucial in optimizing economic efficiency
- **Break down IT and Engineering siloes:** Drive cultural change throughout your business to ensure your workforce embraces the digital revolution and teams converge to adopt a holistic digital strategy
- **The latest predictive maintenance and I&C upgrades:** Discover how I&C upgrades are transforming production by making predictive maintenance, accurate forecasting and operational excellence a reality
- **Evolutions in records and configuration management:** Develop strategies to reduce labour costs through electronic work packages, remote monitoring and mobility working
- **Reduce cyber security threats:** Discover the objectives, requirements, model standards and regulatory expectations for transformation of cyber security in the nuclear sector

NEW AND EXCLUSIVE FOR 2017

- **BRAND-NEW** Cyber Security Strategy & Regulation Workshop: hear where best to place your ongoing cyber investment to mitigate risk and understand how regulations are evolving to meet new threats
- **BRAND-NEW** Interactive Roundtables sessions on driving cultural change within organizations to harness the digital revolution
- **BRAND-NEW** Executive Level Speakers including CIO's & VPs from the utilities leading the way in the digital transformation including Exelon and Southern Nuclear

ALREADY CONFIRMED TO SPEAK:

Susan Landahl
SVP Organizational Effectiveness & Integrated Performance Assessment
Exelon

Bradley Adams
VP Engineering
Southern Nuclear

Joe Donahue
VP Engineering
Duke Energy

Kristiina Soderholm
Lead of Digitalization
Fortum

Clint Carter
Director Advanced Monitoring & Diagnostic Services
Luminant

Waco Bankston
Director Information Technology & Cyber Security
STPNOC

Marek Derewonko
Division Manager for Engineering Support
Bruce Power

Janice Hoerber
IT Supervisor Development Operations
Ameren

Register by September 22nd to save $400 on your pass:
www.nuclearenergyinsider.com/nuclear-plant-digitalization/register.php