# Global System Integrator Report

## Convergence or overlap?

### Understanding the IT/OT relationship

A supplement to *CONTROL ENGINEERING* and *PLANT ENGINEERING* magazines

**By Katherine Elrod and contributing staff,**
*Sealevel Systems Inc.*

# Convergence or overlap? Understanding the IT/OT relationship

With the increasing number of industrial systems connected to the internet, operational technology (OT) is vulnerable to cyberattacks and stands to benefit from information technology (IT) experience

Until recent decades, operational technology (OT), which involves the monitoring and controlling of physical machinery and equipment, was manually managed by human workers. As information technology (IT) relies on computers for operation, its integration into cybersecurity has been swift compared to OT.

With the increasing number of industrial systems connected to the internet, OT is vulnerable to cyberattacks and stands to benefit from IT experience. Examples of OT systems include public services like power, water treatment or transportation applications. Cyberattacks on these systems can have devastating results.

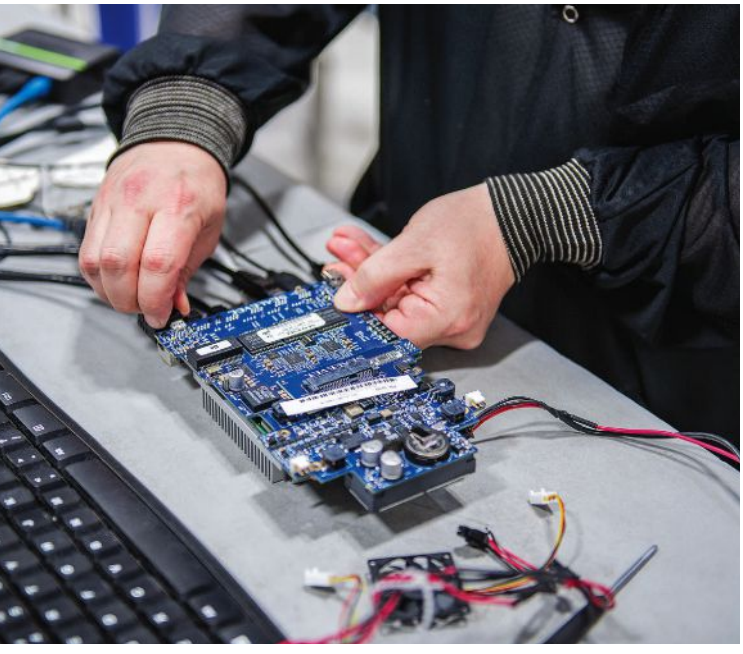
## Understand IT/OT convergence and security implications

***Key differences.*** IT operations exist within an office setting and involve data security, while OT exists on the factory floor and involves the reliability of mechanical functions. When it comes to transferring cybersecurity best practices learned from IT to OT, there are key differences to consider:

- **Environment.** IT operates over servers and the cloud, involving protocols such as HTTP, SSH and RDP. OT operates through machinery and uses protocols such as Modbus, EtherNet/IP and Profinet. The two operate on systems and protocols not seen in the other environment. Implementing security solutions directly from one to the other is not perfectly fitting.
- **Priorities.** IT focuses on data storage, retrieval, manipulation and transmission. Confidentiality and security are key concerns. OT focuses on the safety and availability of operational equipment and processes. When OT systems slow or break down, the physical implications to worker safety and public operations can be severe. An unplanned shutdown of IT processes can be managed with little harm beyond finances. Planned maintenance and security upgrades are more often scheduled in IT, whereas OT relies on keeping machines running at all costs and avoids software updates that require downtime.

***Benefits.*** Benefits include downtime and cost considerations, breakdown response and cost, productivity and safety, and security.

# Convergence or overlap? Understanding the IT/OT relationship



**Human error is the greatest security risk — cyber and beyond — often due to oversight or a lack of knowledge.**

Machine downtime and maintenance cost. IT systems monitor OT machines and equipment condition in real time. This allows a predictive maintenance model where repairs are performed only when conditions indicate a need. Predictive maintenance involves less downtime and maintenance costs than traditional preventive maintenance where machines and equipment are repaired on a schedule, regardless of condition.

Breakdown response and cost. IT monitoring sends real-time alerts when OT equipment malfunctions and can even engage automatic remote shutdowns. An undetected mechanical breakdown can lead to extensive financial cost. The ability to know when a machine fails allows for quick repair and return to factory processes.

Productivity and safety. IT monitoring collects machine data to identify bottlenecks, overheating or other process inefficiencies. From this information, OT systems can be optimized to increase factory floor efficiency, improve safety and save energy costs. Through machine automation, certain processes can be performed without human intervention. This frees human workers to focus on other tasks, improving factory floor productivity and easing labor shortages.

Security. As OT systems migrate to the internet, IT systems keep factory floor data and processes safe from cyberattacks.

## Cybersecurity: Know your assets and vulnerabilities

***Managing OT cybersecurity with IT best practices.*** Despite their differences, OT can be secured by modifying IT security best practices:

- **Know your assets.** It's difficult to protect OT without knowing what need to be protected. A list should be made of every internet-connected device, and security vulnerabilities should be identified.

- **Segment networks.** Segmenting the OT network into smaller sections can prevent hackers from infiltrating the entire factory floor and keep operations safe. Furthermore, segmenting OT from IT can prevent attacks on one network from breaching the other.
- **Patch vulnerabilities.** OT equipment cannot undergo security updates as easily as IT devices. Some legacy equipment may not be updatable at all. However, managing security patches should not be overlooked. This means OT and IT must work together to manage acceptable downtime periods and reasonable patch delays.

- **Secure remote connections.** As more employees are working from home, steps must be taken in IT and OT environments to protect assets from increased security risks.

- **Open communications.** IT teams should work with OT teams in managing cybersecurity. As IT personnel are experienced in managing cybersecurity, it could be easy for IT teams to assume expertise. However, OT teams understand the unique needs of factory floor operations. IT and OT teams should work together in establishing a successful and trusted security plan.

***COVID-19's impact on cybersecurity.*** One of the security best practices mentioned here is the need to "secure remote connections." As the COVID-19 outbreak


forced many workers to operate remotely, security risks increased. Personal home networks are often insecure compared to business networks. Companies may not supply workers with portable business devices, which also have greater security implemented than personal devices. Operating from home may cause workers to feel more at ease using personal accounts or storage that are not as secure as company assets.

Cybercriminals are using COVID-19 to prey on personal fears like job security, economic security and basic needs like food and health care. The CDC and WHO saw a surge of impersonating phishing emails that offered COVID-19 updates, help links and requests for donations. Attackers created fake Skype and Zoom emails to steal personal login information and install malware. Google reported a 350% increase in phishing websites since the outbreak with many related to COVID-19.

The stress from the pandemic is likely to elevate human error. Stress can lead to increased judgment lapses, resulting in oversights that leave openings for cyberattacks. Worse, many workers are untrained in cybersecurity risks, making them unaware of how to spot and avoid attacks.

## Employees are the key to convergence and cybersecurity success

### *Adopting IT/OT convergence*

Companies that merge IT and OT systems will likely face growing pains. Successful cooperation results in a more knowledgeable and skilled employee base when it comes to keeping factory processes safe and efficient. IT/OT convergence can be more effective with a clear, widely communicated plan:

- Outline goals for IT/OT convergence: Personnel from both departments should understand the benefits and goals of convergence.
- Outline possible roadblocks: Personnel should understand challenges are expected. Personnel should be presented with steps for addressing potential issues and be encouraged to provide their own ideas.

- Break down departmental boundaries: This can take many different forms. Some businesses may co-locate IT and OT to give them opportunities to work side by side. Others may create an interdepartmental team composed of IT and OT personnel to oversee projects, roadblocks and solutions. Another option allows data convergence where data experts from IT and OT can view and work with each department's collected data, allowing for a greater understanding of how the two work together.

- Train personnel on security and factory floor operations: Having IT and OT personnel understand security and operational goals further breaks down boundaries and fosters understanding between departments. It also aids in ensuring the security and operational integrity of the factory floor, which is the goal of IT/OT convergence.

### *The greatest cybersecurity risk*

Human error is the greatest security risk — cyber and beyond — often due to oversight or a lack of knowledge. Fortunately, these risks can be alleviated with training and planning.

Train employees on security best practices: Effective cybersecurity starts with a knowledgeable workforce. Employee cybersecurity training should include:

- Password best practices. Passwords should be long, contain multiple character types (beyond letters), be changed regularly and not reused for other accounts.

- Social engineering attack recognition. Teach employees to spot fake emails and websites, which are common attacks hackers use to prey on human error.

- Cyberattack risks. Educate employees about the cost of a data breach to the company.

- Incident report procedure. Define how and to whom employees should report an attack.



# Convergence or overlap? Understanding the IT/OT relationship

- **Personal device policy.** If employees are employees permitted to access company resources on personal devices, establish actions to protect company data.

- **Company device policy.** Communicate the proper use of company devices, including the importance of security updates, if third party downloads are allowed, how devices should be secured and whether such devices can be carried home.

Cybersecurity training should begin with onboarding and be updated regularly for current employees. Mock attacks also can be practiced to train employees on practiced actions should a real attack occur. Companies should regularly share cybersecurity news, which helps employees recognize the commonality of attacks and keeps the importance of cybersecurity fresh in their minds.

Train users on their cybersecurity responsibility: For device manufacturers, training on cybersecurity best practices doesn't end with employees. Users of devices should be informed of their role in keeping devices and personal information secure:

- Dangers of social engineering and how to spot attacks.

- Risks associated with public Wi-Fi and how to alleviate.

- Location of privacy settings and guidance on use.

- Password management best practices.

- Importance of automatic updates and lock screens.

The first defense against cyberattacks is the person behind the device.

## How manufacturers are meeting IT/OT security needs

In response to the ever-increasing volume of cyberattacks, governing bodies are implementing proactive certification and requirements to mitigate risks. While the federal government is enforcing these standards with the primary goal of protecting controlled unclassified information (CUI), the same guidelines should apply to companies manufacturing devices used along the IT/OT convergence chain.

***NIST 800-171.*** NIST 800-171 is the National Institute of Standards and Technology Special Publication 800-171. The publication includes standards and guidelines to protect controlled unclassified information (CUI) — potentially sensitive information not regulated by the federal government. The following are security requirement families:

1. Access control
2. Awareness and training
3. Audit and accountable
4. Configuration management
5. Identification and authentication
6. Incident response
7. Maintenance
8. Media protection
9. Physical protection
10. Personnel security
11. Risk assessment.

***CMMC.*** The U.S. Department of Defense (DoD) created the Cybersecurity Maturity Model Certification (CMMC) as a standard to protect controlled unclassified information (CUI) that is handled by contractors. There are five certification levels, and each higher level incorporates security standards from the prior level. Within these five levels, the CMMC builds on and includes all NIST 800-171 guidelines as well as other cybersecurity standards and guidelines recognized by the DoD:

1. Basic cyber hygiene
2. Intermediate cyber hygiene
3. Good cyber hygiene
4. Proactive
5. Advanced/progressive.

## Final thoughts

Smart security strategy involves planning for and managing IT/OT cybersecurity needs and vulnerabilities sooner rather than later. Evaluation of each part of these processes, including users and devices, is a first step.

***Katherine Elrod*** *is director of marketing for Sealevel Systems Inc. With a foundational background in publishing followed by years in branding and digital communications, Elrod enjoys telling the story of trending tech and the resulting implications as it applies to Sealevel and beyond. She leads Sealevel's team of marketing specialists at Sealevel's headquarters in Liberty, SC.*