WHITEPAPER

Information Technology and Operations Technology: Beyond Convergence

International Society of Automation
Setting the Standard for Automation™

Definitions and Priorities: Information Technology (IT) and Operations Technology (OT)

Information Technology (IT) is defined as hardware, software, and communications technologies that focus on the storage, recovery, transmission, manipulation, and protection of data. **Operations Technology (OT)** is defined as hardware and software that detects or causes a change through the direct monitoring and control of physical devices, processes, and events.

Key differences in the purpose and functionality of IT and OT are reflected in Table 1.

TABLE 1	Information Technology (IT)	Operations Technology (OT)
Primary Function	Process transactions, provide information, support people	Control or monitor physical processes and equipment
Focus	Programming, adjusting, augmenting, and re-programming to fit the evolving needs of networks, applications, and users	24/7, continuous, precise control and monitoring of machines and processes
Architecture	Enterprise-wide infrastructure and applications; generic	Event-driven, real-time, embedded hardware and software; custom
Examples of Systems	Office PCs, printers, web/app/ data/email servers, TCP networks	Industrial Controllers (PLC, DCS, SCADA) and I/O Hardened PCs and Servers Industrial Networks
Examples of Devices	IoT-enabled: tablets, smart phones, etc.	IIoT-enabled: sensors, cameras, embedded systems, robots, analyzers, etc.
Connectivity	Corporate network, IP-based	Control networks, hardwired and IP-based
Data Traffic	Converged network of data, voice, and video	Converged network of data, control, information, safety, and motion
Communication	User-centric	Machine-to-machine
Performance Requirements	High bandwidth, delay-tolerant Rebooting, Retrievable Back-up acceptable	Low bandwidth, real-time Outages unacceptable, redundancy is required
Update Frequency	High	Low
Interfaces and Networks	GUI, web browser, terminal, keyboard	Electromechanical, sensors, actuators, coded displays, hand-held devices

Traditional Security Priorities and Approaches

IT's focus is on protecting intellectual property and company assets, prioritizing confidentiality above integrity and availability. OT's focus is on productivity, maintaining 24/7 operations, and achieving high overall equipment effectiveness, prioritizing availability and control over integrity and confidentiality.

Simply put, IT strives to protect data first; OT strives to protect assets first. IT networks usually feature strict authentication protocols and access policies, while OT networks are simple to access but the physical machines are more closely guarded.

When cyber criminals target IT environments, they're typically after money—but when they target OT environments, they're working to disrupt operations. When a threat is detected in an IT environment, teams will shut down access to the area entirely. In an OT environment where productivity is king, however, teams typically keep operating and attempt to isolate the threat.

A comparison of security-related priorities and approaches is shown in table 2.

TABLE 2	Information Technology (IT)	Operations Technology (OT)
Security Priorities	Confidentiality, Integrity, Availability	Control, Availability, Integrity, Confidentiality
Access Control	Strict network authentication and access policies	Strict physical access but simple network device access
Cyber Criminal Motivation	Monetization	Disruption
Threat Protection	Shut down access	Isolate but keep operating
Maintenance	Multiple support sources; 3–5 year component life; Modular, accessible components; IT staff or contracted service in place	Single vendor support; 15–20 year component life; Remote components, hidden access; No full-time dedicated IT staff
Upgrades	Frequent patches and updates; Automatically pushed during uptime	Carefully planned and tested; Scheduled during downtime or not done at all
Primary Players	CIO and IT	Engineers, technicians, operators, managers

New Concerns for a New World

IT systems are historically used to manage complex data and information flow, but today's OT environments are leveraging them to manage complex physical processes. As a result, industries are safer, more efficient, and more reliable than ever before—but these technologies bring more security risks to facilities and operations.

Attempts to disrupt operations, steal intellectual property, and affect the quality or safety of production are steadily increasing as more cyberattacks target critical infrastructure and industrial assets. Threat actors are using IT techniques to access OT systems, and they're using OT systems that are poorly defended to get access to corporate IT networks. In many ways, cyber criminals are taking advantage of the disconnects—and, in some cases, the distrust between OT and IT teams.

Historically, IT and OT cybersecurity have been considered separately, for several reasons:

- IT cybersecurity was the first focus area for threat actors
- OT environments used to be isolated and "off the grid"
- IT prioritized confidentiality and protection of data over availability and control of systems
- Upgrades and patches are handled very differently, because of access and uptime constraints
- IT teams are not experienced in the operations or control of OT systems
- Within many companies, IT staff and OT staff are functionally, and often physically, separate and uncoordinated

Today's interconnected world means that IT and OT can no longer consider security separately. This new dynamic has resulted in unfamiliar challenges for both areas:

- IT must now account for a greater scope of impact from attacks, including physical safety risks
- IT must learn how to manage outdated, and often custom-designed, systems that aren't easily updated, patched, or configured
- OT must now account for risks that aren't controllable by the machines or the processes
- OT must learn how to protect data as well as physical assets, as more and more

Five Trends Complicating Automation Cybersecurity

1. **Industrial Internet of Things (IIoT):** More connections and networked devices mean more security concerns, new scenarios, increased threat landscapes, different risk profiles
2. **OT/IT Convergence and Interdependence:** Server performance and cloud computing power is driving productivity, but now threat actors can leverage IT-based techniques to target OT networks—and historically effective IT defenses don't always work in operational environments
3. **Legacy Systems:** Difficult to update and maintain, legacy systems typically prioritize availability and integrity over security, and make supply chain integrity impossible because manufacturers no longer build spare parts
4. **Multi-Vendor Environments:** Without widespread compliance to industry-adopted standards, integration introduces risks and many products are not inherently secure
5. **Skill Gaps:** The aging population of engineers and technical specialists, especially in North America, has increased many industries' reliance on contract workforces, making consistent practices increasingly difficult to maintain without standardized competency assessments

traditionally closed systems like utilities and aviation come online

Because of the ever-increasing connectivity in industrial environments, and the resulting security complications, these are challenges that won't be solved quickly or easily. In fact, according to the World Economic Forum's 2019 Global Risk Report, cyberattacks causing disruption to operations and critical infrastructure are among the top five global risks.

Recent, high profile attacks have demonstrated the severe consequences of cybersecurity incidents. For example, the 2017 malware NotPetya spread from the servers of an unassuming Ukrainian software firm to some of the largest businesses in the world. Within a matter of hours, the worm had crippled the operations of several multinational companies, resulting in more than $10 billion in total damages.

Blurring Lines with Intention: Moving from Isolation to Convergence to Integration

Coordination, cooperation, and ultimately integration of IT and OT security can help to prevent or reduce the likelihood of cyberattacks.

A 2017 Gartner report estimated that about 60% of organizations are still in the initial research and sharing phases of their integration efforts between IT and OT. Most companies are just beginning to dialogue. They still need to align their practices and strategies, integrate their systems and infrastructures, and optimize their ecosystems for continuous improvement.

> "Coming together is a beginning. Keeping together is progress. Working together is success."
>
> 
>
> *– Henry Ford*

When IT and OT teams do come together to discuss enterprise security, many organizations find that these priorities emerge:

- Implementing industry-adopted standards and best practices across the enterprise
- Requiring devices and systems to be certified as standards-compliant
- Identifying and authenticating all devices and machines within the system—in plants and in the field—to avoid rogue or unverified devices being used to gain access
- Encrypting communications between devices to ensure data privacy and integrity
- Enabling remote upgrades with satisfactory protections in place to ensure integrity and safety

While these conversations are a good start, it's important to make IT and OT security integration a corporate priority. Increased collaboration—driven by intent and thoughtful strategy, or driven by risks and consequences—will be the only answer to the cybersecurity challenges of the future. ■