# New revised guide to operational technology (OT) security published

September 28 2023

Credit: Smart Connected Systems Division, NIST

The impact of cybersecurity breaches on infrastructure control system owners/operators is more significant and visible than ever before. Whether you work for an infrastructure owner/operator or are a consumer of an infrastructure service, the events of the past few months/years have made it clear that cybersecurity is a critical factor in

ensuring the safe and reliable delivery of goods and services. For infrastructure control system owners/operators, it can be challenging to address the range of cybersecurity threats, vulnerabilities, and risks that can negatively impact their operations, especially with limited resources.

Operational Technology (OT) encompasses a broad range of programmable systems and devices that interact with the physical environment (or manage devices that interact with the physical environment). These systems and devices detect or cause a direct change through the monitoring and/or control of devices, processes, and events. Examples include industrial control systems (ICS), building automation systems, transportation systems, physical access control systems, physical environment monitoring systems, and physical environment measurement systems. OT can be found in all critical infrastructures.

To assist OT system owners/operators, NIST has published Special Publication (SP) 800-82r3 (Revision 3), Guide to Operational Technology (OT) Security, which provides guidance on how to improve the security of OT systems while addressing their unique performance, reliability, and safety requirements. SP 800-82r3 provides an overview of OT and typical system topologies, identifies typical threats to organizational mission and business functions supported by OT, describes typical vulnerabilities in OT, and provides recommended security safeguards and countermeasures to manage the associated risks.

SP 800-82 has been downloaded more than 3 million times since its initial release in 2006, and this is the third revision of NIST SP 800-82, with a new title reflecting an expanded scope. SP 800-82r3 was produced through a collaborative effort of the NIST Smart Connected Systems Division's Networked Control Systems Group and the NIST Computer Security Division.

Updates in this revision include:

- New title
- Expansion in scope from ICS to OT
- Updates to OT threats and vulnerabilities
- Updates to OT risk management, recommended practices, and architectures
- Updates to current activities in OT security
- Updates to security capabilities and tools for OT
- Additional alignment with other OT security standards and guidelines, including the Cybersecurity Framework (CSF)
- New tailoring guidance for SP 800-53r5 security controls, including an OT overlay that provides tailored security control baselines for low-impact, moderate-impact, and high-impact OT systems

In addition to SP 800-82r3, a collection of NIST resources for OT cybersecurity can be found at the Operational Technology Security website.

**More information:** Keith Stouffer, Guide to Operational Technology (OT) Security, (2023). DOI: 10.6028/NIST.SP.800-82r3

*This story is republished courtesy of NIST. Read the original story here.*

Provided by National Institute of Standards and Technology