

***THE OT ZERO TRUST  
RISK ASSESSMENT***

**OTZT**

***K.O. CYBER THREATS WITH OT ZERO TRUST***





# **The OT Zero Trust** Risk Assessment

# Table of Contents

01 Introduction	4
<hr/>	
02 7 Steps Toward Zero Risk	5
03 Assess Threats	6
04 Analyze Risks	8
05 Prioritize Risks	10
06 Top ICS Cyber-attacks	11
07 Risk Assessment	12
08 Monitor Risks	14
09 Response to Cyber Incidents	15
<hr/>	
10 Conclusion	16

## 01

# Introduction

A system controlling the fabrication of integrated circuits stopped abruptly during routine operations, destroying wafers worth \$50,000. Another robot randomly swung its heavy metal arm around 180 degrees in an area regularly accessed by personnel. These were just accidents - imagine what a bad actor could orchestrate. To accurately decide which cyber defenses you need for optimum protection, look at your risk. Which devices are most vulnerable? What are the attack surfaces?

Arguably in NIST examples of adversarial incidents, **Risk 1. Denial of Control** has a high priority. The vulnerability is severe and the asset is critical. The likelihood this may occur is medium, but if it does, the impact is high. It may or may not be easy to detect. Therefore, defending against denial of control is important. In the past, executives often relied on security-by-obscurity. They isolated critical systems and posted perimeter defenses. Gartner recently punctuated the wake-up call that connecting assets to the internet also opens the door to ransomware, trojans, worms, and other nasty malware assaults. In the Market Guide for Operational Technology Security, Gartner identified the "Oh Wow!" moment - a polite term for the instant you realize that failing to invest in modern cybersecurity is creating a self-inflicted threat. The moment a ransom demand arrives, it is already too late.

**"Greetings! There was a significant flaw in the security system of your company..."**

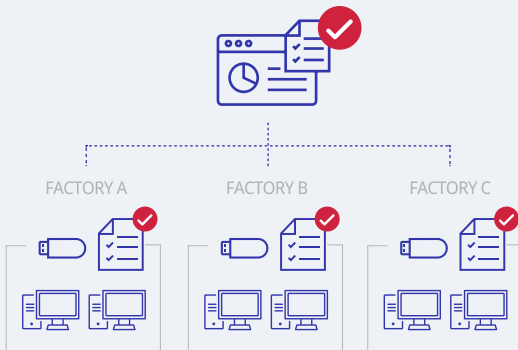
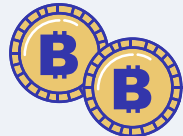

What will be attacked next? You realize that your OT network is one flat attack surface with lots of potential security holes. Unmanaged devices are connecting everywhere. Ports are open. Your teams are scrambling. Stop! You have a choice. Forego this "Oh Wow!" scenario and create your own superhero "POW!" moment. Smash the hacks by evaluating threats using this OT zero trust risk assessment toolkit.



# 02

# 7 Steps Toward Zero Risk

There is no guarantee of a risk-free world, but following these 7 steps can improve your protections.

<p><b>1. Take inventory</b></p> <p>OT zero trust portable security devices and endpoint protection automatically inspect and inventory of all types of devices from legacy to modern to air-gapped.</p> 	<p><b>2. Plan to cover your assets</b></p> <p>Devise a plan based on your tolerance for unexpected events. How much are you willing to risk?</p> <p>Cyber-criminals don't attack everyone. Why not buy insurance and bet that your systems will not be targeted? If you get hit, will you pay the ransom or rebuild your systems?</p> 
<p><b>3. Assess threats</b></p>	<p><b>4. Analyze risks to understand what is at stake</b></p>
<p><b>5. Prioritize risk and develop responses in case the risk event occurs</b></p>	<p><b>6. Monitor risks</b></p> 
<p><b>7. When under attack, activate your risk responses</b></p>	

# 03 Assess Threats

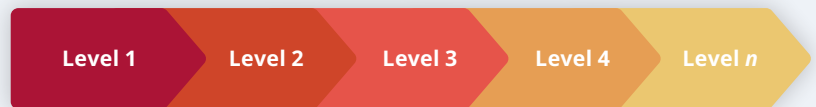
Hackers are constantly researching targets, developing or downloading hacking tools, looking for security holes, and attacking. Malware travels through your networks disguised as regular traffic. Personnel walking on-site often carry hidden cyber threats within their laptops and USB drives. Each type of attack has a different threat level, and attackers often mix and match attacks.

## Threat Actors

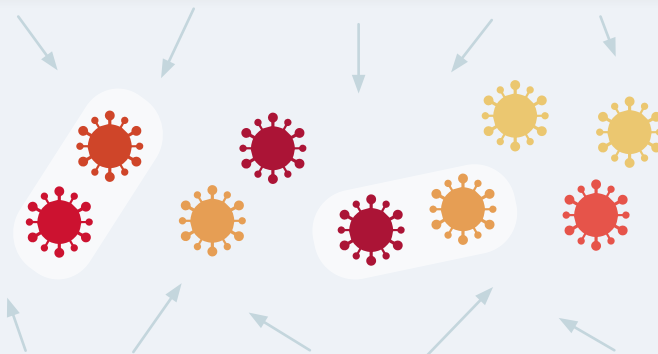
- Script Kiddies
- Hacktivism
- Commodity Threats
- Advanced Persistent Threats



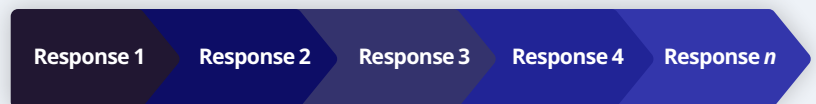
## Threats



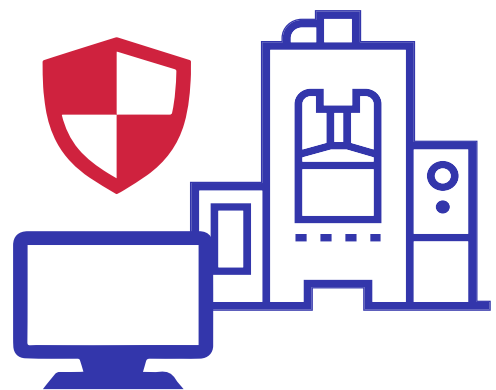
## Attacks



## Responses



Threat actors range from so-called “script kiddie” amateurs to state-employed, professional hackers. A script kiddie may just be a teenager randomly searching the web for hacking tools and other cybercrime-related resources, and hacktivists attack systems to bring attention to a cause. Most corporate threats begin with threat actors dedicated to the field of cybercrime or cyber espionage who would like to use ransomware to extract payments. Professional threat actors work collaboratively as Advanced Persistent Threat (APT) groups, which are the professionals of the cybercrime industry.\*



---

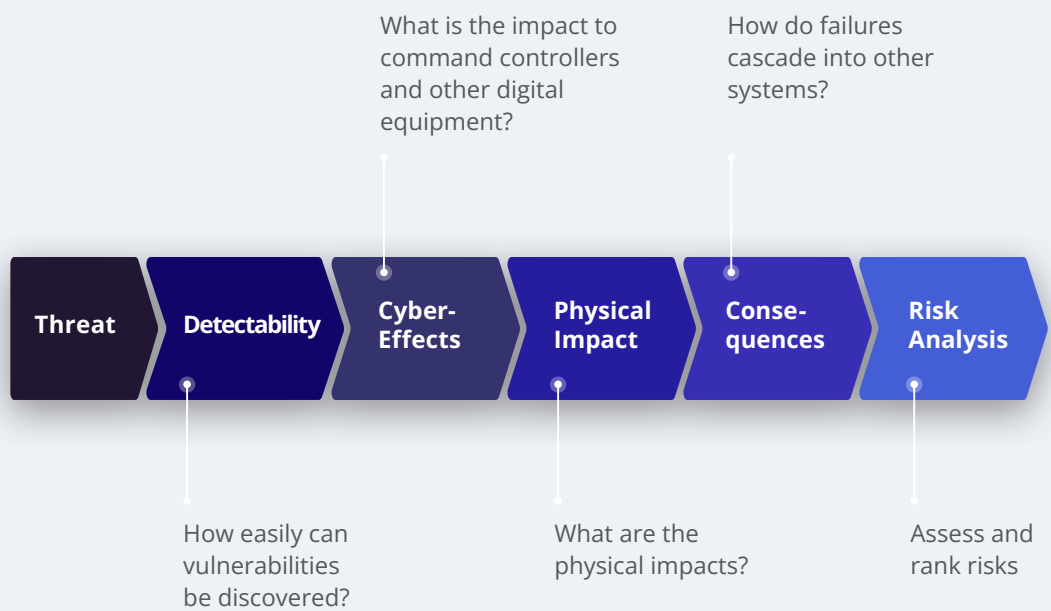
\* David P. Duggan, Sherry R. Thomas, Cynthia K. K. Veitch, and Laura Woodard, *Categorizing Threat: Building and Using a Generic Threat Matrix* (Albuquerque, New Mexico: Sandia National Laboratories Report: SAND2007-5791, 2007), 13.

# 04 Analyze Risks

Operational technology functions in the physical world. The key difference between OT and IT cyber-attacks are the safety consequences:

- **Safety of your team and your community**
- **Safety of your property**
- **Environmental safety**

When evaluating risks consider what damage could occur if your sensors or actuators were hijacked. Think about what happens when an attack propagates through connected systems. If your digital controllers stop functioning, what happens to your non-digital assets? When setting risk thresholds, safety considerations are critical.



OT zero trust risk analysis allows you to identify the most important risks so you can focus your budget and your team on responding to the most critical threats first. When a threat is identified, consider these questions:

- **Which systems are vulnerable to the threat?**
- **What is the harm:**
  - Can this threat attack my command controllers?
  - What about my other digital equipment?
- **What are the physical ramifications of the threat?**
- **What if the threat cascades locally or beyond?**

While investigating whether a threat should be added to your risk assessment, you can use the MITRE ATT&CK matrix to understand the details of the threat. This is a curated knowledge base for cyber-threats against OT, whereby researchers have investigated common attack strategies for assets and systems that are routinely targeted.\*

---

\* The MITRE Corporation, "ICS tactics", accessed May 23 2022, <https://attack.mitre.org/tactics/ics/>

# 05 Prioritize Risks

Remember that lessons learned from IT may not apply to OT. IT cybersecurity assessments revolve around the CIA triad: Confidentiality, Integrity, and Availability. Because IT systems are often used for accounting, legal documents, and human resources, the highest priority is generally confidentiality. This is not true for operational technology (OT). Machines work all day, every day, 24 hours per day. Productivity is key. Safety is critical. For example, NERC-CIP defines a “bright-line” criteria for categorizing bulk electrical systems based on the impact if they were rendered unavailable for more than 15 minutes. Arguably, the first priority for OT is availability.\*

IT	Priority	OT
<b>Confidentiality</b>	<b>1</b>	<b>Availability</b>
<b>Integrity</b>	<b>2</b>	<b>Integrity</b>
<b>Availability</b>	<b>3</b>	<b>Confidentiality</b>

Detectability is also important. If you don’t know that a threat exists then you cannot respond. The environment plays an important role. Inclement weather is a risk to outdoor operations that may not affect IT systems located in an office or a data center. The criticality of an asset and the harm if an asset misbehaves must be considered. For example, what is the likelihood that a controller would activate a robot arm swinging it around 180 degrees? If that happened, would workers be hurt or would facilities or equipment be damaged?

Take a deep dive into the technical process for assessing and managing cyber-risks when using OT zero trust. First, time is valuable. Rank cyber-threats based on what is most critical so you can spend your time efficiently. Researchers ranked the most common types of cyber-attacks unique to ICS.

\* Qian Chen, F.T. Sheldon, and Robert K. Abercrombie, “Risk Assessment For Industrial Control Systems Quantifying Availability Using Mean Failure Cost (MFC)” Journal of Artificial Intelligence and Soft Computing Research 5(3):205-220 (Washington, DC: Government Printing Office, 2016), 207.

06

# Top ICS Cyber-attacks

Cyber-attack	Description
<b>Denial of Control</b>	Control systems are disrupted by delaying or blocking the flow of data, creating bottlenecks
<b>Control Devices Reprogrammed</b>	Unauthorized changes to programmed instructions in PLCs, RTUs, DCS, or SCADA controllers that change alarm thresholds, change equipment behavior, or prematurely shutdown systems. Any of these could cause spills, fires, equipment damage, or other harm to workers and the environment.
<b>Spoofed System Status Information</b>	False data sent to control system operators could disguise attacks
<b>Control Logic Manipulation</b>	Untested changes to software or configuration settings could produce unpredictable results
<b>Safety Systems Modified</b>	Safety systems could be turned off or programmed to take incorrect actions that damage or destroy systems and threaten workers or the environment
<b>Malware injected into control systems</b>	Virus, Trojans, worms or other malware can disrupt production and may destroy equipment

Copied from Table C-8 in NIST Special Publication 800-82 Revision 2\*

These attack vectors often involve expert knowledge of systems, and expert hackers even develop apps so that others can attack without understanding all the technical details.

\* Keith Stouffer, Victoria Pillitteri, Suzanne Lightman, Marshall Abrams, and Adam Hahn, NIST Special Publication 800-82 Revision 2 Guide to Industrial Control Systems (ICS) Security Supervisory Control and Data Acquisition (SCADA) Systems, Distributed Control Systems (DCS), and Other Control System Configurations such as Programmable Logic Controllers (PLC) (Gaithersburg, Maryland: U.S. Department of Commerce, 2015), <https://nvlpubs.nist.gov/nistpubs/specialpublications/nist.sp.800-82r2.pdf>

## 07

# Risk Assessment

The goal of a risk assessment is to understand threats so you can deploy your cyber defenses where and when they are needed. You can use a risk assessment to evaluate protections for safeguarding a single asset to protecting your entire system. A risk assessment quantifies each risk so you can prioritize them. Risk scenarios are added to the risk assessment based on the results of the threat assessment and the risk analysis. Suppose, these evaluations reveal that both the denial of control and the malware injected into control systems are risks. To rank them, assign a value to each risk vector:

- **Vulnerability Severity** – On a scale of 0 to 10, if this threat occurred how severe would the damage be?
- **Asset Criticality** – On a scale of 0 to 10, how important is this asset?
- **Likelihood** – On a scale of 0 to 10, will this threat actually occur in your facility?
- **Impact** – On a scale of 0 to 10, what is the impact to productivity?
- **Detectability** – On a scale of 10 to 0, how will you know that you are under attack? Compared to other scores, detectability scores are reversed – a low detection scores 10, meaning that you are more vulnerable because you cannot defend against what you don't know about.
- **Risk Ranking** – We used this formula to determine risk ranking.  
$$\text{Priority} = (\text{severity} + (\text{criticality} * 2) + (\text{likelihood} * 2) + (\text{impact} * 2) + (\text{detectability} * 2)) / 5$$
- **Risk Priority** – **High priority risks** are those ranked from **18 to 12**, medium risks are ranked from 12 to 6, and low risks are under 6.

There are many quantification schemes more sophisticated than a scale of 0 to 10. For example, assigning Fibonacci sequences may prove more accurate for predicting future risks, and alternative risk formulas may better reflect your situation. Choose the method that quantifies risks based on your risk tolerance.

To quickly see which cyber defenses you need, sort by risk priority. You may even want to color-code your risk assessment. In this example, Risk 1. Denial of Control has the highest priority. The vulnerability is severe and the asset is critical. The likelihood this may occur is medium, but if it does, the impact is high. It may or may not be easy to detect. Red color coding is used to show high severity.

	<p><b>Risk 1. Denial of Control</b></p> <p>Control systems are disrupted by delaying the flow of data and creating bottlenecks</p>	<p><b>Risk 2. Malware injected into control systems</b></p> <p>Virus, Trojans, worms or other malware can disrupt production and may destroy equipment</p>
Vulnerability Severity (Low 0-High 10)	10	1
Asset Criticality (Low 0-High 10)	10	5
Likelihood (Low 0-High 10)	5	1
Impact (Low 0-High 10)	10	10
Detectability (Low 10-High 0)	5	5
<b>Risk Priority</b>	<b>14</b>	<b>8.6</b>
<b>Risk Mitigation or Response</b>	<p>Mitigation 1. Use a defense console to monitor status from all assets and report incidents</p> <p>-----</p> <p>Mitigation 2. Segment the network so you can quarantine infected machines</p>	<p>Mitigation 1. Inspect devices to scan and destroy malware on modern endpoints and legacy or air-gapped devices</p> <p>-----</p> <p>Mitigation 2. Reinforce protections with virtual patching</p>

# 08

## Monitor Risks

The four cornerstones of OT zero trust support continual monitoring of your systems. OT zero trust devices can be set to monitor-mode so you can observe or to defend-mode so they take action on your behalf.

Inspect assets, take inventory, and destroy supply chain malware using portable security devices. These devices do not interrupt production so you can scan legacy and air-gapped assets, as well as perform routine or surprise inspections.

Lockdown assets by determining your trust policies so OT zero trust can enforce them. Your assets are armed with monitors that discern the situation and take the best course of action depending on what's happening at any given time.

Segment your network into zero trust zones and only allow trusted messages from trusted devices to enter a zone. Once inside, only trustworthy messages can be sent outside. Set up zones to run efficiently and set up honeypots to lure cybercriminals away from your critical assets.

Reinforce cybersecurity by using endpoint protection with machine-learning threat intelligence and virtual patching to reduce risk until a vendor-supplied patch is released and tested. Continually monitor your systems, assessing threats and activating your risk responses when under attack.

OT zero trust shows the status of your system on a single pane of glass. All security devices report in real-time to one cybersecurity defense console.



# 09

## Response to Cyber Incidents

Risk thresholds are unique to every company. For each risk you identify you decide what response meets your comfort level. Risk responses are generally grouped into these categories: avoiding, transferring, sharing, mitigating, or accepting the risk. The most important feature of any risk response is the ability for your system or your team to execute the response and stop the attack. OT zero trust locks down assets, monitors network traffic using trust lists that stop most attacks before they start.



# 10

## Conclusion

The seven steps toward zero risk are based on guidance from years of experience by industry leaders who have documented their lessons learned in NIST and other standards along with researchers who are solely dedicated to finding better ways to protect your operational technology. Using OT zero trust, ARM yourself with a tried-and-true process that is summarized in the NIST Guide to Industrial Control Systems (ICS) Security: continually **A**ssess risks, **R**espond to threats, and **M**onitor vulnerabilities.\*



\* Keith Stouffer, Suzanne Lightman, Victoria Pillitteri, Marshall Abrams), Adam Hahn, SP 800-82 Rev. 2 Guide to Industrial Control Systems (ICS) Security, (Gaithersburg, Maryland: U.S. Department of Commerce,2015).

While there is no guarantee of a risk-free world, this 7-step OT risk assessment will improve cybersecurity at your operations.

### **1. Take inventory of your assets**

OT zero trust-based portable security devices automatically inventory every asset during inspection, making it easy to confirm the defensive status of stand-alone assets, newly-arrived onboarding assets, and any devices brought onto the work site.

### **2. Develop a security plan to protect your assets**

Use your inventory and your unique tolerance for the unexpected to inform your cybersecurity plan.

### **3. Assess threats before analyzing risks**

OT zero trust-based threat intelligence is always working for you, finding new trends that sock it to any malware lurking in the shadows of your systems and network.

### **4. Analyze risks to understand what is at stake**

An ounce of prevention is worth a pound of cure – OT zero trust matches up protections with your assets to put dependable, easily-maintained defenses in place before your network gets hit and your assets are in danger.

### **5. Assess risks to prioritize managing the risk and to develop responses in case the risk-event occurs**

Quantifying risks gives you a POWERful weapon to prioritize and justify your budget for cyber defenses.

### **6. Monitor risks using automated or manual controls**

OT zero trust is a valued technology partner following your lead using your criteria to carry out the critical mission of tackling the 24x7x365 challenge of safeguarding your systems around the clock.

### **7. When under attack, activate risk responses**

Forego the “Oh Wow!” chaos and prepare your team and your cyber defenses to respond with your superhero partner in cyber protection, OT zero trust.

