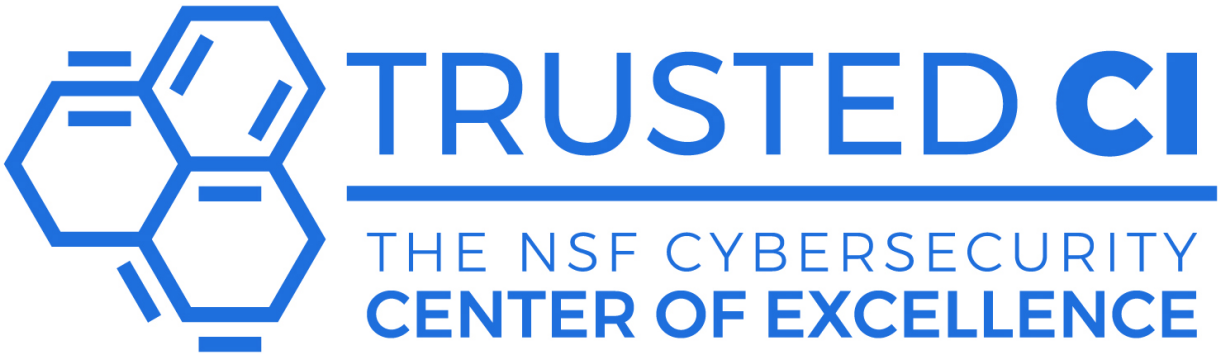

Findings of the 2022 Trusted CI Study on the Security of Operational Technology in NSF Scientific Research

July 13, 2022

Status: Draft Report v1.0

Distribution: Public

Emily K. Adams, Daniel Gunter, Ryan Kiser, Mark Krenz, Sean Peisert, Susan Sons, and John Zage

About the 2022 Trusted CI Annual Challenge Team

The 2022 Annual Challenge team is a collaborative effort of Trusted CI members from Indiana University, Lawrence Berkeley National Laboratory, and the National Center for Supercomputing Applications.

About Trusted CI

The mission of Trusted CI is to lead in the development of an NSF Cybersecurity Ecosystem with the workforce, knowledge, processes, and cyberinfrastructure that enables trustworthy science and NSF's vision of a nation that is a global leader in research and innovation.

Acknowledgments

In support of this effort, Trusted CI gratefully acknowledges the input from the individuals at the following NSF Major Facilities who contributed to this effort:

- IceCube Neutrino Observatory:[1] Ralf Auer, Steve Barnet, Francis Halzen, Kael Hanson, Benedikt Riedel
- NOIRLab:[2] Mike Fleming, Chris Morrison, Rod Rutland
- Ocean Observatories Initiative:[3] Jeffrey Glatstein, Paul Matthias, Craig Risien, Christopher Wingard
- United States Academic Research Fleet:[4] Pam Clark, Rose Dufour, Lee Ellett, Ken Feldman, Erich Gruebel, John Haverlack, Jim Holik, Robert Kamphaus, Jon Meyer, Chris Romsos, Laura Stolp, Kevin Walsh

The authors of this document are also grateful to Craig Jackson (Indiana University) and Drew Paine (formerly of Lawrence Berkeley National Laboratory) for their significant efforts in planning this study and contributing to initial aspects of the execution of the study. We are also grateful to Jim Basney (National Center for Supercomputing Applications), Kelli Shute (Indiana University), and Von Welch (Indiana University), who offered feedback on earlier versions of this report.

This document is a product of Trusted CI. Trusted CI is supported by the National Science Foundation under Grant #1920430. For more information about Trusted CI, please visit: https://trustedci.org/. Any opinions, findings, and conclusions or recommendations

[1] https://icecube.wisc.edu/
[2] https://www.noirlab.edu/
[3] https://oceanobservatories.org/
[4] https://www.unols.org/

expressed in this material are those of the author(s) and do not necessarily reflect the views of the National Science Foundation.

Using & Citing this Work

Cite this work using the following information:

> Emily K. Adams, Daniel Gunter, Ryan Kiser, Mark Krenz, Sean Peisert, Susan Sons, and John Zage. "Findings of the 2022 Trusted CI Study on the Security of Operational Technology in NSF Scientific Research," July 13, 2022. DOI: 10.5281/zenodo.6828675 https://doi.org/10.5281/zenodo.6828675

Executive Summary

Our study surveyed the practices of National Science Foundation (NSF) Major Facilities with respect to securing operational technology. *Operational technology (OT)* encompasses broad categories of computing and communication systems that in some way interact with the physical world. This includes devices that either have *sensing* elements or *control* elements, or some combination of the two. OT typically has the capability to be networked but may or may not be actually connected to a network at all times or at all.

As recently indicated by NIST: "OT is critical to the operation of U.S. critical infrastructure."[5] Furthermore, there have been numerous incidents in recent years that have exposed significant security weaknesses in this often overlooked component of that critical infrastructure. In NSF Major Facilities, OT includes the same types of sensing and control devices used in critical infrastructure but also includes bespoke scientific instruments. NSF Major Facilities often exist to operate scientific cyberinfrastructure and would not be able to perform their funded activities without these assets.

We observed that Major Facilities took *safety engineering* extremely seriously. Likewise, all of the Major Facilities that we spoke with also took IT cybersecurity seriously as well. At the same time, we observed numerous places where OT security for those Major Facilities could be improved. When asked if there was one element of their organization that they

[5] NIST Guide to Operational Technology (OT) Security, SP 800-82 Rev. 3 (Draft), 2022. https://doi.org/10.6028/NIST.SP.800-82r3.ipd

could change, every facility we interviewed indicated that it would be that funding for at least one full-time employee (FTE) dedicated to IT and/or OT cybersecurity, independent of other responsibilities be made available. We believe this indicates a major concern regarding resources allocated to OT security.

In addition, we observed that while OT devices often have an operational lifetime of 15-30 years, there are often no cybersecurity requirements during the device acquisition process. This, despite the fact that much of the newer OT — that is, that which has been acquired in the past five years — is increasingly "software defined" and therefore containing exactly the same vulnerabilities as traditional IT systems. We also observed low amounts of documentation and little or no use of OT-related security policies once OT devices were installed or services reliant upon OT were in production use.

Many Major Facilities represent sole-source U.S. capacity for certain scientific disciplines. However, despite the outsized risks posed to the missions of Major Facilities by cyber attacks against operational technology, the portions of Major Facilities that operate operational technology are often disconnected from IT security. There tends to be a lack of communication between the teams that operate OT systems and the teams that provide IT systems and cybersecurity. This communication gap is not due to lack of interest in cross-team communication, but most often comes up due to the personnel structure, siloing those teams in different parts of an organization, and barriers presented by not fully understanding each other's technical domains. These challenges are amplified when teams managing OT deployments are geographically distributed or federated across multiple organizations.

Finally, we observed that Major Facilities rely a great deal on isolation (e.g., a physical air gap) for securing OT, rather than a defense-in-depth[6] strategy. As a result, security protections can succeed or fail with the efficacy of that isolation. In practice, there are times when the devices need to be connected to the network for updates and removed from an isolated state. There is a perception that only periodic reconnection keeps these systems secure, but that periodic reconnection can leave that equipment vulnerable while connected.

1. Introduction

In 2022, Trusted CI is conducting our focused "annual challenge" on the security of *operational technology* used in National Science Foundation (NSF)-funded scientific

[6] The U.S National Institute for Standards and Technology (NIST) defines "defense-in-depth" as *"an information security strategy that integrates people, technology, and operations capabilities to establish variable barriers across multiple layers and missions of the organization."* https://csrc.nist.gov/glossary/term/defense_in_depth

research. The goal of this year-long project, involving seven Trusted CI members, is to understand the state of the security of operational technology in science and then to develop a roadmap of clear, actionable recommendations toward sustainable improvement of the security of that operational technology.

Operational technology (OT) elements are sometimes called *cyber-physical systems*. These elements encompass broad categories of computing systems that in some way interact with the physical world. Roughly, this breaks down into devices that either have *sensing* elements or *control* elements, or some combination of the two. It includes industrial control systems, digital relays, programmable logic controllers, SCADA (supervisory control and digital acquisition), Internet of Things (IoT), and Industrial Internet of Things (IIoT).

In practical terms, in the NSF Major Facilities, we have found that OT used in science includes bespoke scientific instruments, such as

- controls for the motors that move telescopes in an observatory
- vehicle power and propulsion systems
- sensors and drones operating remotely and semi-autonomously in the field
- fixed sensors
- data acquisition systems (DAQs)
- winches and cranes on ships
- satellite communication nodes, including antenna controllers, modems, VoIP gear

OT in science also includes more mundane systems that in some cases are nonetheless critical to the science being conducted, including:

- heating and cooling systems
- electronic door controls
- environment monitoring

In addition to the OT devices themselves, there are supporting or auxiliary systems leveraged for maintenance and management of the OT environment, often with direct connections to the OT device : *i.e.* end-of-life machines, vendor "dial-in" access.

Trusted CI's approach to this effort has been to spend the first half of 2022 engaging with operators of OT in science to understand the range of operational practices and evaluate potential deficiencies that lead to vulnerabilities and compromises. In the second half of 2022, we plan to leverage our insights to develop a roadmap of solutions to sustainably advance security of scientific operational technology. This roadmap is expected to be used by Trusted CI in concert with Major Facilities to support improvements over a period of multiple years, given that the expected changes cannot all be introduced in one year for institutions that have equipment with installed lifetimes of decades.

Almost all of the NSF Major Facilities are funded by the GEO[7] and MPS[8] directorates. As a result, the findings reported in this document are the result of interviews with NSF Major Facilities in those directorates. It also contains the individual insights and experiences with OT operated by NSF Major Facilities from study team members, such as via Trusted CI engagements or the ongoing process of assisting Major Facilities with adoption of the Trusted CI Framework.

The intended audience for both the findings and roadmap documents include Trusted CI itself, so it can best support the NSF Major Facilities in securing their scientific OT, those operators of cyber-physical systems in science, and also NSF Program Officers, so that they understand those gaps in securing OT in science and can better understand the need for prioritization and committing of resources to improving the state of securing OT in science.

This report was written by team members of Trusted CI, the NSF Cybersecurity Center of Excellence. The team includes security experts from various parts of the discipline including operational security, scientific infrastructure development, and security research.

2. Why is Operational Technology Different?

Operational technology predates computer networks by a very long time and has a long history of being operated safely. In fact, there is an entire discipline called *safety engineering* that seeks to assure that proper engineering principles are used to ensure safety of individuals, equipment, and materials surrounding the use of OT, leveraging fault tree analysis, ensuring proper failure modes (fail safe, fail fast, fail slow, etc…).[9]

Very large amounts of OT in use today predates the use of modern computer networking and the Internet. Not only was it not designed with security in mind, it was not designed with networking in mind at all. Networking came later, and with it, exposure to attacks over those networks, be the OT local or remote, over the Internet. While it is also true that certain roots of today's computer operating systems also predate the Internet, including UNIX, Microsoft Windows, and macOS, all of those systems have seen robust improvements in security over the past decades — the core of Windows was wholly overhauled beginning with Windows 2000, and macOS with Mac OS X, for example — whereas the same is not true for a great deal of OT and the software that controls it.

---

[7] GEO is NSF's Directorate for Geosciences: https://www.nsf.gov/dir/index.jsp?org=GEO
[8] MPS is NSF's Directorate for Mathematical and Physical Sciences: https://www.nsf.gov/dir/index.jsp?org=MPS
[9] Chuck McParland, Sean Peisert, and Anna Scaglione, "Monitoring Security of Networked Control Systems: It's the Physics," *IEEE Security & Privacy*,12(6), pp. 32–39, November/December 2014. http://dx.doi.org/10.1109/MSP.2014.122

While operating systems and software written for traditional *information technology (IT)* purposes tend to be general purpose, software for OT is often custom-written according to the requirements of the device. For the manufacturer of the device or machine, the focus is usually more on the physical functionality than its software functionality. Companies developing such devices may have a long history of creating the device before the need for software control came about. For instance, a company that makes a winch or crane for a ship may be using basic electronic interfaces without the need for more sophisticated integrated computing or even networking. Later, due to demand from customers, the company may implement control of the winch or crane via a remote wireless controller or smartphone. While the company may have hired an expert to implement the functionality, that expert may not be ready to support the software infrastructure over time. Thus, vulnerabilities discovered in the software may unwittingly go unpatched by the company who may not even be aware that the system is still running or should be patched.

By its definition, OT interfaces — either via control systems or sensors or both — with the physical world and may be capable of affecting the physical world. This could include activities that put those close by in danger of being pinched, crushed, hit, electrocuted, and so on. In the scientific world, an example of this is in a control system for a telescope that needs to move a large telescope physically. If the telescope were to suddenly move unexpectedly, it could crush anyone in its path. This is in contrast to software that only deals with data and aspects of the virtual world, where physical safety is typically not a direct concern.

OT often can be easy to overlook, as its focus on operations often leads to it working in the background and blending in with the environment. A well-functioning system can easily be ignored. For instance, one may not consider that an Heating Ventilation Air Conditioning (HVAC) system in a commercial building (or on a ship) has a network connection for monitoring and control, but that is exactly how the company Target was breached in 2013.[10] Likewise, in a data center, an uninterruptible power supply (UPS) system for power backup may have a monitoring and control interface connected to a management network but is rarely utilized until there is an emergency. As with HVAC, vulnerabilities in networked UPS systems were exploited in March 2022 at APC.[11]

The reality is that there are many vectors into OT systems. Infamously, the Stuxnet malware that manipulated programmable logic controllers (PLCs) to cause uranium enrichment centrifuges in Iran to tear themselves apart jumped network air gaps by being

[10] Brian Krebs, "Target Hackers Broke in Via HVAC Company," February 5, 2014. https://krebsonsecurity.com/2014/02/target-hackers-broke-in-via-hvac-company/
[11] Eduard Kovacs, "Millions of APC Smart UPS Devices Can Be Remotely Hacked, Damaged," *SecurityWeek,* March 08, 2022 https://www.securityweek.com/millions-apc-smart-ups-devices-can-be-remotely-hacked-damaged

introduced to the facility through a compromised USB drive.[12] A single compromised password enabled attackers to shut down the Colonial Pipeline fuel distribution system.[13] In 2017, as a result of the NotPetya malware, (1) the radiation monitoring system at the Chernobyl nuclear power plant in Ukraine was disabled; (2) production was halted at Cadbury's chocolate factory in Hobart, Australia; and (3) shut down the shipping giant Maersk's entire computer network, including port operations.

The culture and traditions of many organizations often delegate the responsibility of installing, configuring, and maintaining OT to non-IT groups, vendors, or third-party contractors. These may include contractors brought in to do one job without an obligation to provide ongoing support. There is no guarantee that third-parties have adequate cybersecurity training or awareness of threats, the expectation or motivation to properly secure a networked device or adhere to fundamental cybersecurity practices such as strong passwords and per-user access controls. They may not be aware of the project's security policies. As a result, those individuals may be exposing OT control systems to an organization's IT network or even the broader Internet with minimal security protections in place. There may even be a misalignment of incentives for securing OT systems between contractors, and an organization's OT operators and cybersecurity staff. All this results in an increased risk of successful cyberattacks.

OT and IoT are often on separate networks and in unique physical locations, separated from traditional IT devices that might be found in a server room or network closet. Despite this segmentation, due to their operational requirements, OT might be more exposed to public access, such as a security badge reader, or in physically difficult to access locations, such as at the peak of a mountain. Their isolation or purpose might also require using less secure networks or exposing them on the public Internet for remote access. Some OT devices require that third-party personnel outside of the organization have administrative or operator access to the device to perform maintenance, which in turn may expose the device to external sources, thereby increasing the risk of exposure to network-based malicious activity.

OT and IoT devices are often running unique firmware or software that was developed for the specific purpose of the device. This means that if the vendor producing the software is out of business, there may no longer be support for the software even during the expected lifecycle of the asset. This is in contrast to more traditional computers where the operating

[12] Kim Zetter, "An Unprecedented Look at Stuxnet, the World's First Digital Weapon," *Wired*, Nov. 3, 2014. https://www.wired.com/2014/11/countdown-to-zero-day-stuxnet/
[13] Kim Lyons, "Hackers reportedly used a compromised password in Colonial Pipeline cyberattack," *The Verge*, June 5, 2021. https://www.theverge.com/2021/6/5/22520297/compromised-password-reportedly-allowed-hackers-colonial-pipeline-cyberattack

system (OS) was written by one of the major providers with a plan for providing security patching support and a long-term upgrade process.

OT often has different mechanisms for upgrading software or firmware of the device than traditional IT. In fact, the primary function of the device which a facility relies upon may need to be shut down for a significant amount of time, and can even require coordination with the manufacturer, or an additional purchase that must pass through an organization's procurement process.

An additional factor complicating the maintenance of OT is that it is often associated with more expensive equipment than commodity computers which are only meant to last 5 years before being upgraded. The organization's budget might only expect to buy the OT equipment once during the lifetime of the project. Furthermore, when OT equipment is able to receive security updates, the manufacturer will often only provide security updates on newer equipment. As a result, projects will often run equipment for decades without being able to patch security vulnerabilities.

3. Findings

Before we begin detailing our cybersecurity findings, we noted from our interviews that *safety engineering* is taken extremely seriously by all the NSF Major Facilities that we interviewed. Safety engineering is the aspect of operational technology that largely addresses safety of devices that are never connected to other networks or other computerized devices. Whenever potential damage to equipment or environment or safety of life was at question, OT operators at Major Facilities had a rigorous understanding of risks involved and policies and procedures in place to address them.

Likewise, all the Major Facilities that we spoke with also took cybersecurity seriously as well. Each had one or more individuals responsible for cybersecurity operations, typically from within the "IT" portion of an organization, which is typically, though not always separate from the OT operations portion. As we will discuss, it is this divided responsibility where many of our most noteworthy findings arose. At the same time, every facility indicated that if there was one element of their organization that they could change, it was that they would have at least one FTE dedicated to cybersecurity (including OT security) independent of other responsibilities.

Cybersecurity done properly requires scaffolding, such as people, policies and procedures, training, and maintenance lifecycles. Cybersecurity can seem to many like a highly technical domain, and indeed, there are many aspects of developing systems and operating systems in a secure way that are highly technical. At the same time, perhaps to an even

larger degree than the technical aspects is the human scaffolding around the technology. Given how central a role humans can play in the security or insecurity of a system in practice, human behavior is very important to security.

To this end, in addition to technical aspects, our study also focused on the role of security of OT in the missions of Major Facilities and the organizational structure of personnel in charge of operating and securing OT. We also examined the processes and procedures in place to operate and secure technology and how those are developed, adopted, explained, followed, enforced, and revised and maintained over time. We also specifically investigated the OT procurement practices of Major Facilities given how important a role our early interviews found procurement to be. In the following sections, we describe our findings across these different areas.

3.1 Mission

Mission. From the "Trusted CI Framework Implementation Guide for Research Cyberinfrastructure Operators," the following is stated:

> *"Cybersecurity is not undertaken as an end unto itself: the ultimate goal of a cybersecurity program is to support the organization's mission. 'The mission' is the foundational motivating force driving decision making: it is made up of the task(s), purpose(s), and related action(s) that the organization treats as most important or essential. The program's implementation must account for the positive and negative impacts security can have on the organization's mission."*[14]

Many NSF major facilities exist to enable the generation of new knowledge through the operation of scientific instruments at a large scale. These instruments, and the data they produce, are a core component of the major facilities' ability to achieve their missions. The OT that enables these instruments to function is critical to the missions of these facilities.

In many cases, failure or mis-operation of a single large asset at a Major Facility could mean that the entire Facility and the science that it supports could be stalled for years due to downtime and damage. Many Major Facilities represent sole-source U.S. capacity for certain scientific disciplines and depend largely on the availability of their OT assets in order to perform their core activities. Consider, for example, the collapse of the Arecibo Telescope in late 2020. The Facility has been reduced to a skeleton staff and the science performed by Arecibo is not taking place. Even temporary disruptions in availability could jeopardize the scientific mission. Similarly, the loss — even temporary — of the U.S. Academic Research Fleet's (ARF) sole icebreaking vessel for arctic research, Research

[14] Jackson, Craig, Cowles, Bob, Russell, Scott, Adams, Emily K., Kiser, Ryan, Ricks, Ranson, & Shankar, Anurag. (2021). The Trusted CI Framework Implementation Guide for Research Cyberinfrastructure Operators (1.0). Zenodo. https://doi.org/10.5281/zenodo.4562447

Vessel (R/V) *Sikuliaq*, would have significant impact on Arctic research. Even aside from asset damage, consider the potential consequence of a major safety failure that led to loss of life: an automated telescope control that crushes a human or a ship's underwater sonar engaged while divers are in the water.

Findings. We found the *safety engineering* of OT to be front and center in the missions of Major Facilities. In addition, as mentioned earlier, IT security is typically taken very seriously. However, despite the outsized risks posed to the missions of Major Facilities by cyber attacks against OT, the portions of Major Facilities that operate OT are often disconnected from IT security. When this occurs, OT assets become a source of risks which are unaccounted for by the very parts of the organization whose roles are to account for and remediate cybersecurity risks to the organization's ability to carry out its mission.

Many of the facilities we interviewed expressed an increased awareness of the convergence and influence between IT and OT and are intentionally looking through a holistic lens when planning for the future. More than one facility has engaged in assessing the overall suitability of IT solutions with OT infrastructure needs in mind, including deploying similar devices across construction projects for greater uniformity in management and has planned a more rigorous device lifecycle and maintenance strategy than in previous deployments.

These information assets also have challenging and often poorly understood cybersecurity characteristics. For example, IT staff in the organization may be familiar with networks which communicate using protocols which offer integrity checking and authentication capabilities but not familiar with protocols which are in use in OT networks which do not offer those capabilities. Another example of these poorly understood cybersecurity characteristics is that OT-specific communication protocols which are not supported by common IT network monitoring tools can lead to gaps in security alerting and monitoring capabilities necessary to identify compromised systems. Because of these differences between IT and OT operations, the cybersecurity programs of NSF major facilities can miss key information necessary to identify risks to the very assets which these organizations rely on most to perform their missions.

These challenges exist for a variety of technical and administrative reasons. These include:

- limited security features of the associated communication protocols,
- limited information security staff expertise with OT,
- general staff availability and effort allocations,
- a lack of system-specific security hardening guidance, and
- a limited understanding of the risk characteristics of OT systems in risk acceptor roles compared to traditional IT systems.

This combination of issues makes it difficult for organizations to accurately tailor their cybersecurity programs to the mission of an organization which relies heavily on OT assets.

Organizations which are accounting for these challenges are often addressing them in respect to safety concerns. While this can be effective and accounts for what are arguably the most important category of risk, not all risks to the organizations' missions relate to safety concerns. This state of affairs still leaves gaps where categories of risk to the organization cannot be effectively accounted for.

3.2 Organization & Governance

Organization and Governance. Organization and governance refers to institutional structures, hierarchies, and policies that govern OT operators. It includes definitions of roles and responsibilities for operators and other technical personnel, as well as the organizational guidelines and review procedures for assuring secure and safe operation. It also has an important role in long-term planning and decisions about resource allocation for both people and material.

The organizational structure within OT operators plays an important role in how cybersecurity is handled in relation to OT. Notably, as mentioned earlier, even where formal security roles exist, there is frequently "siloing" between information security personnel and OT operators. IT and OT personnel may talk to each other rarely, if at all. Communication between IT and OT personnel is further complicated by the more specialized and uncommon skill set involved in OT.

Findings. As befits the highly varied types of OT in use by Major Facilities, top-down governance of OT cybersecurity for Major Facilities is not dictated by the NSF. As a result, the structure of OT cybersecurity within the organizations studied varies, from highly decentralized to mostly centralized, including at the NSF level with some organizations reporting to multiple distinct NSF program managers. Policies applied across the organization were sometimes based on a broader set of common procedures designed to address regulatory requirements, such as those laid out in the Woods Hole Oceanographic Institution (WHOI) Safety Management Manual (SMM)[15] for shipboard cybersecurity. Notably, where other agencies are involved with the Major Facility, cybersecurity may be prescribed by agreements with that agency.

[15] WHOI Safety Management Manual, 7.10 – Cyber Risk Management (CRM) Instructions. https://www.whoi.edu/wp-content/uploads/2022/01/7.10-Cybersecurity-Instructions.pdf

In other cases, security policies were inherited from the lead institution, such as a university, which could also take on the role of coordinating OT security. All research universities have security policies, which should apply to Major Facility operations. In some cases, having and leveraging host university security can even be a requirement for certain non-NSF funding agency partners. However, host institution policies may not address all OT security requirements and host institutions often do not have the specialized skillset or personnel available to support OT security. When Major Facilities are able to leverage a host institution's security via specialized OT security support, we found that this can provide significant benefit to Facilities otherwise very limited by funding and expertise for security.

Another common organizational approach to physically distributed collaborations was to delegate the cybersecurity responsibilities to individual sites. Whether centralized or distributed, the projects studied did not have personnel dedicated to adapting or enforcing OT security policies across the project.

A common theme across all these organizations is a lack of available cybersecurity expertise *on site at remote locations*. Organizations that operate large and/or dangerous physical equipment have significant OT expertise focused on procedures related to that equipment, and significant consequences, e.g., via the International Traffic in Arms Regulations (ITAR) regulatory regime. No equivalent levels of enforcement or required expertise exists for OT threats. Decisions on the practices, training, and operational policies for OT are administered by delegation to individual sites or a body formed from committees from each institution.

To the best of our knowledge, nobody in the organizations we examined would describe themselves as an OT security expert. Interviewees recognized that this expertise was important. *Every Facility that we interviewed indicated that it is, or would be, extremely valuable to have a dedicated IT and/or OT cybersecurity specialist.* There was one Facility that we spoke with that did have such a single, dedicated specialist responsible for security; they described how having this specialist not only improved security but relieved the burden on other staff who had previously been supporting security in addition to their other responsibilities. We believe that the benefits of a dedicated cybersecurity specialist are not unlike those of having a dedicated safety specialist to ensure the safety of personnel and equipment. The latter is a role that most Major Facilities do have, and yet lack the resources to have the equivalent for cybersecurity.

While there are some efforts being made to hire additional cybersecurity expertise, the Facilities interviewed did not have more detailed long-term plans for organizational changes related to OT cybersecurity. At the same time, a cybersecurity position that requires both IT and OT technology expertise can be difficult to fill due to the extensive training required to be successful in the disparate technology domains.

We consistently found that interviewees were acutely aware of, and wanted to address, the gaps identified above. In particular, interviewees were aware that budget and personnel were below ideal levels, that they would benefit from increased representation of OT in cybersecurity groups in the organization, and that they needed enhanced authority to make decisions or have recommendations heard in the interest of OT. This speaks first to the high level of security awareness at each institution but also to the importance of providing organizational mechanisms to transform this awareness into action.

One Major Facility that we interviewed mentioned outsourcing as a way of addressing skill and personnel gaps. This includes outsourcing the security role itself, to the Research Security Operations Center (ResearchSOC).[16] It also included shifting technology providers from equipment that requires local expertise to equipment that is commercially supported, including via remote operation. While the latter provided a solution, it did so at somewhat greater cost and somewhat reduced flexibility than was provided when operating the more specialized, "home-grown" solutions.

3.3 Policies

Policies. Ideally, a "Policy" refers to a documented statement which is formally adopted as a norm within an organization to govern human behavior.[17] However, often, security "policies" are understood and adopted implicitly. For example, an organization may not have a security policy in place that says that only authorized individuals can access a system and then defines who is considered an authorized individual, who can authorize exceptions to that policy, et al.

In addition, well-defined *processes* are also key to cybersecurity. Without robust processes in place, the strongest technical controls can fail. For example, process guides *how* an organization identifies risk and decides to accept or mitigate it. It describes how people within an organization interact to inform the right people about risk and make decisions. Process may not say *which* technical controls to implement, but it will contain a methodology for how those controls are selected, how they are operated, and how they are maintained and updated over time.

Findings. In general, we found very low amounts of documentation and use of OT-related security policies. With a few exceptions relating to Major Facilities that have higher degrees of interactions with U.S. Government agencies outside of the National Science Foundation, or in some way brush up against export controlled areas, OT security practices tended to be implicit or assumed.

[16] https://researchsoc.iu.edu
[17] Trusted CI Framework Implementation Guide, Must 9: Policy

In addition, the largest process-related issue discovered in the team's interviews was the lack of communication between the teams that operate OT systems and the teams that provide IT cybersecurity. This gap means either that OT systems are not included at all in cybersecurity, or that OT systems do not benefit fully from the expertise of the IT security team, or, perhaps worst of all, are subject to edicts and requirements from IT security that are not appropriate or otherwise optimal for OT systems rather than IT systems.

We note that this observed IT/OT communication gap is not due to lack of interest in cross-team communication by those respective teams, but most often comes up due to the personnel structure, siloing those teams in different parts of an organization, and due to barriers in fully understanding each other's technical domains. This problem is particularly exacerbated with teams that are distributed or federated, in which case not only do OT operations and IT security not communicate adequately, but those teams may not even communicate adequately internally. Some Major Facilities even have scientific elements and technical elements that are operated by one contractor but building-type facilities operated by a separate contractor. This can cause communication to be virtually non-existent and increases the likelihood that there are assumptions about what one or the other is or is not doing, and is therefore likely to foster mistaken assumptions, misunderstandings, and gaps that could all lead to security issues.

Another huge issue for Major Facilities is that although a Research Infrastructure Guide exists, there is often no top-down governance of cybersecurity for Major Facilities by NSF. While this isn't necessarily a bad thing it does mean that each Major Facility is left to its own to determine operational policies, including cybersecurity. This includes not just the creation of policies, but the documentation and enforcement of those policies. Of particular concern is where cybersecurity can impact safety, such as when control elements are involved in manipulating equipment.

Many scientific OT systems have unusual and often unavoidable requirements. Among these include practical, physical limitations. For example, the amount of people that can be housed in a remote location may be very limited, thereby naturally precluding the ability to use preciously limited space (e.g., on a ship or in a polar facility) on additional IT security personnel, even if those personnel were otherwise available as part of a broader organization. Practical security issues for Major Facilities can also include potentially harmful devices and equipment that the scientists may bring to that Facility, such as personal laptops, smartphones, science gear, and telepresence gear that is connected to the Facility's network.

For example, a science party comes on board for a two or three week cruise with unmanned remotely operated vehicles and associated computers that are connected to the shipboard network. This would raise security issues such as how do different ship operators assess

such equipment that is connected to their networks, how are they monitored, and how would existing security policy apply to these assets.

3.4 Device Procurement & Maintenance

Device procurement & maintenance: The device procurement processes, and the nature of the device deployment, play a significant role in facilitating scientific research and organizations' facility operations. Most organizations have procurement policies that guide the decision-making process of device, software, and service acquisition. Considerations surrounding the acquisition of assets, and the lifetime maintenance of these assets, are a point-of-origin for an organization's function and can have a lasting effect on research and facility operations as devices may be in production for years or even decades.

Increasingly, procurement policies for many organizations, including scientific ones, are considering security in some fashion. For example, as a result of the National Defense Authorization Act (NDAA), as well as Build America, Buy America requirements, many organizations have banned the use of Huawei equipment or Kaspersky software due to the connections between those companies and adversarial foreign governments. In addition, in IT acquisitions, security is at least implicitly a requirement, if not explicitly — for example, new servers should be able to run current operating systems. But most organizations will take that even a step further with ensuring that security patches continue to be available through long term support contracts.

Findings. Considerations surrounding procurement, longevity of operations, and accepted risk over consistent operations surfaced as important issues in our discussions. While some scientific OT is "bespoke" and custom-built by academic engineering teams, other scientific OT deployed in their environments is commercially produced. However, in either case, the security properties of those devices tends not to be well understood by Major Facilities, and nor is security an element of OT procurement requirements, as it might be if it were a traditional computing or networking product or service.

Contrary to the rapid lifecycle of IT devices and support, Facility devices are expected to sustain a number of years or decades of service. In the case of an interviewee's Facility new-construction, device installments are expected to operate for 30 years with mid-life refresh occurring at the 15-year mark. In cases like these, some Facilities, such as the ARF, when building new ships, are taking a proactive approach in planning for the limited windows of opportunity to establish or enhance cybersecurity in their OT infrastructure and deployments.

In general, the Major Facilities we interviewed acquired some amount of commercially available OT devices to meet the function and purpose of their mission. However, that acquisition process typically had little if any aspect considering device origin or

cybersecurity protocols as part of it. Those Major Facilities that have higher-degrees of interactions with U.S. Government agencies outside of the National Science Foundation may be required to follow domain-specific regulatory requirements to guide the decision-making process of device, software, and service acquisition, and in those cases cybersecurity and OT lifecycle management tend to have higher consideration.

The support and maintenance of devices deployed in Facility operations often are impacted by "vendor lock-in" due to either limited availability in the market for specialized equipment, or currently deployed equipment support available only from a single vendor. In some cases, devices deployed in Facilities had continued operation even after the device vendor had gone out of business. In many OT installments, device hardware sourcing and the subsequent vendor support was proprietary, resulting in little or no local access to maintain device configurations or the state of device security in local installations.

More than one Facility expressed concern with vendor transparency regarding cybersecurity practices, uncertainty surrounding the integrity of device firmware updates, and unrestricted remote vendor access to a device, especially for those devices *only* able to be serviced by a vendor. Some Facilities had implemented technical controls to secure vendor access to devices such as dedicated communication channels for vendor "dial-in" or by leveraging dedicated, offline laptops to perform device updates. Others employed various levels of security defense-in-depth (*i.e.,* multiple layers of SSH connections to reach a device), relied on IT-OT network separation for security, or cited low-value of the device as a risk reduction. (*i.e.,* assumption the data or function of the device was not worthy of malicious activity).

3.5 Networking

Networking. Networking aspects of securing OT refer to network isolation of OT, monitoring of networks containing OT, and having the expertise available to analyze traffic to and from OT for suspicious activity.

In general, the proper technical approach to securing OT can look a lot like securing an otherwise unsecurable computer system, such as a computer running an operating system that is no longer receiving security updates from the vendor. In fact, the OT may well be controlled by such an operating system.

Findings. The technical needs of each facility regarding OT operations vary. OT expertise from one type of device does not necessarily translate to another. Fortunately, there are some categories with similarities, such as sonar from ship operations OT and scientific OT.

Firewalls and segmentation are employed by all interviewees explicitly to protect and isolate OT. In theory the network isolation of critical systems is a fool-proof method of

maintaining the operational status of OT devices. However, in practice, there are times when the device needs to be connected to the network for updates. There is a perception that only periodic reconnection keeps these systems secure. Some systems are required by the vendors to periodically connect to update systems or upload metrics. Some of these systems are kept isolated through a simple on-off switch, which could easily be left on accidentally. Another method of isolation through router configurations allowing one-way communications from an isolated device can leave the potential for misconfigured settings, allowing bidirectional communications. Specifications of the isolation process and security checks on its isolation don't have a standardization.

There appeared to be an assumption that the geographic isolation of some sites and bandwidth limitations provide a measure of security. These defining features of some large facilities however, may only change the landscape rather than increasing its security. Compromising an isolated location may or may not be any more difficult than a more easily accessible location.

Another challenge many large facilities deal with due to their isolated locations involves providing connectivity at these remote locations. Connections are often provided by satellite services, which involves limitations to bandwidth due to technical limitations and high costs. For example, placement of satellite dishes on ships and some remote sites must account for vessel hull features or geography that may block satellite connectivity. Additional challenges can occur when individuals at these scientific sites demand Internet access, stressing shared, limited bandwidth.

Due to the limited bandwidth, common security activities such as security monitoring are often not practiced at all. Security monitoring involves a constant connection to upload current logs for remote monitoring and analysis. In situations with limited bandwidth supporting a moderate user base, even a small constant connection can be unaffordable. Alternatives such as storing logs to analyze later is possible but is a large hurdle to accomplish when potential time windows in which to perform these activities are already filled with other necessary maintenance tasks. Another alternative is having staff assigned to monitor the networks in person, but remote sites often also have limited bunking space for personnel.

4.0 Next Steps

This document is intended to present the findings of Trusted CI's investigation into the security of operational technology used in science. In the coming months, Trusted CI will be developing a "solutions roadmap" aimed at presenting a multi-year plan for addressing key gaps in the security of OT in major facilities both in initial installation as well as operation.