Mighty Guides®

Advice for CISOs:

How to Approach OT Cybersecurity

Sponsored by PAS®

INTRODUCTION

Kaspersky Lab's discovery of Stuxnet in 2010 turned the industrial world on its head. As the first known instance of malicious code specifically designed to seek out and interfere with industrial operations, Stuxnet was a serious wakeup call for OT operators, especially those in much of the world's critical infrastructure. So how has the OT/ICS community responded to the new reality of OT cyber risk?

With generous support from PAS, we asked 5 OT security professionals the following question:

What are the top three pieces of advice you would give a CISO to make the plant OT/ICS environment more secure from cyber attacks?

For OT and IT security people, this is something of a loaded question, largely because OT cybersecurity is still very much a work in progress. For instance, although many contributors stressed the importance of knowing your environment, that in itself is a big challenge that varies from industry to industry and plant to plant. "Asset knowledge" also means different things to different people.

The essays in this eBook provide a wealth of information and present an inside look at an aspect of cybersecurity that is still not well understood. I am certain that anyone responsible for critical industrial operations will benefit from the advice and experiences of those who have contributed to this eBook.

All the best,
David Rogelberg
Publisher,
Mighty Guides, Inc.

Mighty Guides®

Mighty Guides make you stronger.

These authoritative and diverse guides provide a full view of a topic. They help you explore, compare, and contrast a variety of viewpoints so that you can determine what will work best for you. Reading a Mighty Guide is kind of like having your own team of experts. Each heartfelt and sincere piece of advice in this guide sits right next to the contributor's name, biography, and links so that you can learn more about their work. This background information gives you the proper context for each expert's independent perspective.

Credible advice from top experts helps you make strong decisions. Strong decisions make you mighty.

© 2018 Mighty Guides, Inc. I 62 Nassau Drive I Great Neck, NY 11021 I 516-360-2622 I www.mightyguides.com

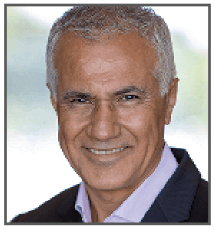
FOREWORD BY EDDIE HABIBI

Digitalization and Industrie 4.0 initiatives require tight integration between the complex, heterogeneous, and highly complex Industrial Control Systems (ICS) and the enterprise IT. However, the very components that enable digitalization—sensors, connectivity and smart applications—also increase risk. Digitalization enhances efficiency, improves safety, and optimizes production, but it also creates more opportunities for bad actors to penetrate operational technology (OT) environments and to wreak havoc.

To secure industrial facilities and ensure safe, reliable production, OT and IT security—traditionally two separate disciplines with different priorities—must come together to share cybersecurity and risk management best practices.

In this eBook, experts on the front lines of OT cybersecurity risk mitigation share their strategies for making control systems more secure. The firsthand experience collected here comes from experts across a diverse range of industries – including oil and gas, chemicals and refining, and power generation. Their essays illustrate the importance of understanding similarities and differences between IT and OT environments. They also share proven experience on adapting IT security controls and best practices to OT environments.

Apply the valuable insights provided in this guide within your own company to protect the endpoints that matter most in your company's industrial facilities—the proprietary industrial control system (ICS) assets responsible for safe and reliable production.



Regards,
Eddie Habibi
Founder & CEO, PAS Global, LLC

Founded in 1993, PAS is a leading provider of software solutions for ICS cybersecurity, process safety, and asset reliability to the energy, process, and power industries worldwide. PAS solutions include industrial control system cybersecurity, automation asset management, IPL assurance, alarm management, high performance HMI™, boundary management, and control loop performance optimization. PAS solutions are installed in over 1,380 facilities worldwide in more than 70 countries. PAS was recently named the #1 Global Provider of Safety Lifecycle Management by ARC Advisory Group including #1 rankings within Chemical, Power Generation, Refining, and Oil & Gas. For more information, visit www.pas.com. Connect with PAS on Twitter @PASGlobal or LinkedIn.

ADVICE FOR CISOs: HOW TO APPROACH OT CYBERSECURITY

In This Section...

Brian Foster
In Critical Infrastructure, Safety Comes First.. 5

Christopher Rey-herme
Security Awareness Is Key to
ICS Cybersecurity 8

Jose Mendez
There Must Be Standard Operating
Procedures for the OT Network..................... 11

Jacob Laas Glass
OT Security Begins with a Technical
Standard of Critical Security Elements......... 15

Gabriel Agboruche
Strategies for Securing Digital Assets
in Nuclear Power Plants................................ 18

BRIAN FOSTER

OT Cybersecurity Engineer
Portland General Electric

Brian Foster is an OT/ICS cybersecurity engineer. Having come to security from controls engineering, he possesses a deep understanding of the industrial equipment and processes he is securing. He builds security into OT systems as a function of safety, and uses quantitative math-based risk analysis to provide meaningful measurements to improvements.

LinkedIn

One of the great challenges in securing OT systems in the power generation and distribution industry is the age of system components. “The average lifespan of a typical ICS device is about 30 years,” says Brian Foster, OT/ICS cybersecurity engineer for Portland General Electric. “And, of course, 30-year-old equipment was not built with cybersecurity in mind.”

Although some vendors produce new equipment that is forward-looking when it comes to cybersecurity, many do not. “A few are building products on a well-made, secure PLC platform,” Foster explains. “They’re good about patching in ways that don’t mess up your controls. There’s a shift among ICS product vendors, but it’s definitely not across the board. I think because of the long lifespan of the equipment, vendors are not pushed very hard to come out with newer technology all the time. It just won’t be adopted very quickly.”

> “*Our number one concern is safety, and any security in our networks has to be designed in a way that is safe. We can’t have a machine fail and kill someone.*”

In this environment of critical infrastructure controlled by a large variety of new and older ICS, Foster believes there are three essential actions the person responsible for OT security must do: »

- **Take the time to understand your OT space.** It's essential to know what is in the environment before you can understand what it needs, but Foster points out that every environment is different. "It's never the same from place to place in OT, and there's going to be many different varieties of equipment," he says. Part of understanding your environment is having a comprehensive inventory of control system assets as well as asset configurations and their changes. There are solutions available to help discover and monitor OT assets, but they are different than those used in IT environments.
- **Recognize that safety trumps all other concerns in an OT network.** This is a fundamental cultural difference between OT environments and IT security, and it affects security strategy. For example, the traditional CIA model (confidentiality, integrity, and availability) is not meaningful in an OT network. "Our number one concern is safety, and any security in our networks has to be designed in a way that is safe. We can't have a machine fail and kill someone. That's just not an acceptable outcome. We approach everything with that safety mindset," Foster says. »

> "Passive tools are unlikely to affect anything. With active tools, you run more of a risk. Whether it's passive or active, these tools must be carefully evaluated before anything is put into place."

- **You must have visibility into the network.** This means being able to see data packets that are moving around and executing the many controls in an OT system. For critical networks like those in the power generation and distribution infrastructure, scanning tools are more likely to be passive than active because of the risk of active tools interfering with a process. “Passive tools are unlikely to affect anything,” says Foster. “With active tools, you run more of a risk. Could it cause traffic on your network that causes a control signal to be missed, which is completely unacceptable? Whether it’s passive or active, these tools must be carefully evaluated before anything is put into place.”

How you respond to suspicious activity is very important. In the IT world, it’s common to prevent suspicious packets from reaching their destination. But you can’t do that in critical infrastructure. “If I send a command to open a breaker, that breaker has to open,” Foster notes. “I don’t care if that command is malicious or otherwise, because someone’s life could be on the line. If we’re saying, ‘Cut the power,’ then regardless of where that command comes from, we’re cutting the power. But I want to know that command occurred. Where did it come from? What did the structure look like? Does it look like all the other times we’ve sent out commands to open the breaker? We have to look at a baseline to determine if this is similar or not. We already opened the breaker because that’s the safe thing to do, but we can look at it after the fact to see if that was the correct action.” ■

Reducing Industrial Risk:
20 Experts Share Strategies for Managing OT Cybersecurity

Download the full e-book: Reducing Industrial Risk:
20 Experts Share Strategies for Managing OT Cybersecurity

KEY POINTS

1 **Securing 30 year-old-equipment which was not built with security in mind is a great challenge in the power generation and distribution industry.**

2 **In the IT world, it’s common to prevent suspicious packets from reaching their destination. You can’t do that in critical infrastructure.**

CHRISTOPHE REY-HERME

Chief Industrial Information Security Officer
Total Marketing and Services

In his role as CISO at Total Marketing and Services, Christophe Rey-herme has defined his company's industrial cybersecurity strategy and policies, and rolled out a three-year program to improve the security level of its perimeter. He is also engaged in educating personnel about cybersecurity risks and solutions, conducting training programs, and making videos to raise awareness.

LinkedIn

As chief information security officer (CISO) for industrial control systems at Total Marketing and Services, Christophe Rey-herme is in charge of industry and cybersecurity for roughly 300 plants around the globe. A major part of his responsibilities is to increase his colleagues' security awareness and then to assist them in improving security for the business as a whole. When considering high-level ICS security priorities, Rey-herme recommends that security professionals keep these three tips in mind:

- **Make everyone aware of the importance of cybersecurity to themselves and the plant.** Rey-herme and his team have pursued a variety of strategies for raising security awareness among their colleagues, including making training videos as well as hacking and cybersecurity demonstrations that show their colleagues how easy it is to gain control over a system when it's not secure. "When people see the risk and what can happen if they don't secure the system, they become interested in the subject. Then, they begin to look for solutions for improvement," he says. "Once I have a partner at the plant who is interested in improving our solutions, that's a key point enabling me to move forward. I have too many plants to do everything on my own. »

> "*Part of our risk is coming from the connection of some of our plants to the enterprise network.*"

I absolutely need to have at least one or two people in each plant in charge of cybersecurity who are really aware of the risk. I get that through various awareness campaigns."

- **Cybersecurity has to be a business enabler.** This includes helping to acquire and deploy solutions that plant operators want and consider realistic for their real-world environments. When he first started working at Total Marketing and Services, Rey-herme noticed that the cybersecurity team tended to focus mostly on whether the company's plants were complying with the rules. "Now, we show the plants not only why and where they are not compliant, but we also provide a technical solution that ensures the business needs while complying with our cybersecurity rules," he says. To streamline the process going forward, Rey-herme and his team have built a catalog of solutions that can assist plants in fulfilling both objectives.
- **Collaborate with enterprise IT security people when determining risk exposure, especially in areas where there are connections between the plant and enterprise networks.** "Part of our risk is coming from the connection of some of our plants to the enterprise network," he says. »

> "I have too many plants to do everything on my own. I absolutely need to have at least one or two people in each plant in charge of cybersecurity who are really aware of the risk."

SECURITY AWARENESS IS KEY TO ICS CYBERSECURITY

> This presents a challenge because OT engineers are often unaware of the risk such connections pose to ICS systems, and IT people are often unaware of the connections, or they do not know how to evaluate the risks those connections create, or both. Rey-herme finds it valuable to collaborate closely with his colleagues in the enterprise IT security team so that they can effectively address both sides of the equation.

Ensuring adequate security is challenging in a plant environment, since OT tends to focus first and foremost on safety and operational continuity. As a result, OT engineers need to see security as a threat to operational continuity in order to take it seriously. This is why Rey-herme considers security awareness a top priority, as it enables the business to come together more effectively in support of a unified strategy. By raising awareness, communicating the importance of compliance, and collaborating with enterprise IT colleagues, he believes security organizations can go a long way toward achieving improved security. ■

Reducing Industrial Risk:
20 Experts Share Strategies for Managing OT Cybersecurity

Download the full e-book: Reducing Industrial Risk:
20 Experts Share Strategies for Managing OT Cybersecurity

KEY POINTS

1 **OT engineers need to see security as a threat to operational continuity in order to take it seriously.**

2 **When plants connect to enterprise networks, OT engineers are often unaware of the risk, and IT people are often unaware of the connections, or they do not know how to evaluate the risks, or both.**

GREG HALE

Editor/Founder
ISSSource.com

Twitter

Website

LinkedIn

> *You must understand what you have in your environment. I've talked to companies that thought they had about 500 control devices on the plant floor. It turned out they had more like 12,000. You have to know the devices and the device connections.*

THERE MUST BE STANDARD OPERATING PROCEDURES FOR THE OT NETWORK

JOSE MENDEZ

Director, Global
Cyber Security
CONFIDENTIAL

Jose Mendez is a professional with more than 20 years of IT experience, focusing on cybersecurity for the past 12 years. He has worked in multiple industries, including media, insurance, and manufacturing. In his current position as director of global cybersecurity, he was responsible for developing the entire cybersecurity culture from the ground up. Mendez is now responsible for formulating and deploying a cybersecurity strategy around the industrial networks in the mining industry.

Cybersecurity is less regulated in the mining industry than in other sectors. "Power and banking each have had government regulations mandating levels of security," says Jose Mendez, who has worked in both IT and OT security. "They're seen as being ahead of the game when it comes to cybersecurity due to these government mandates. The mining industry does not have any of that." Yet the mining sector is just as vulnerable to cyber risk, not only to its operations, which must continue uninterrupted, but also to the miners themselves. Many miners working in hazardous environments depend on control systems to keep them safe. "Safety is incredibly important to the mining industry, and cybersecurity is part of that," he says.

Some aspects of mining provide opportunities to strengthen OT security. For example, whereas power distribution networks are built to last decades and can have very old industrial control systems, a typical precious-metal mine has a lifespan of 5 to 15 years. Also, because mining operations are often located in remote areas where it is expensive to move equipment, it's usually more cost effective to leave old systems behind and build a new mine with entirely new equipment. This gives mining operations more opportunity to upgrade OT systems than some other industries. »

> "*We found cases where OT brought in a vendor to install something that would send out telemetry over the Internet. This was happening without the control or knowledge of IT.*"

Sponsored by PAS

THERE MUST BE STANDARD OPERATING PROCEDURES FOR THE OT NETWORK

According to Mendez, the mining industry is starting to pay closer attention to OT security, due in part to a kind of “creeping” OT-IT convergence that is happening, often without IT’s knowledge. “In my experience, the OT network was independent from IT,” he explains. “The IT people never considered OT because there was this gap between OT and IT. They didn’t have to worry. But when we started documenting OT systems, we found cases where OT brought in a vendor to install something that would send out telemetry over the Internet. This was happening without the control or knowledge of IT.”

As mining operations focus more on OT security, Mendez recommends taking these steps:

- **Document everything.** “The IT network gets audited and you’re forced to keep and maintain a level of documentation about systems that you use, and the controls that you use to protect them. It should be the same for OT systems,” Mendez says. He suggests using a vendor who can make a complete assessment and report on all your PLCs and controllers, and then move forward from there. >>

> “You need to establish processes that are standard operating procedures, fine-tuned for the OT network.”

THERE MUST BE STANDARD OPERATING PROCEDURES FOR THE OT NETWORK

- **You need to have visibility into your assets and what's moving in the network.** "By visibility, I mean being able to see system detail, all traffic coming in and out, all the nodes that are there and their patch levels, and the types of communications that are happening. The ultimate goal is to have a service similar to an IT network SOC," says Mendez. "If you're not monitoring, you're leaving yourself exposed." But he also cautions that the monitoring constraints are different for OT. "You have systems controlling things at the nanosecond and microsecond level. Any type of latency introduced by monitoring could have a potential impact."
- **You must apply network controls to the OT network.** "What I mean by controls is applying the same type of processes that you have for your IT network into the OT network," says Mendez, who is passionately committed to improving OT security. "You want to have proper onboarding when it comes to new systems. You want to have proper patching, updates, backups, and antivirus. You need to establish processes that are standard operating procedures, fine-tuned for the OT network."

Doing all these things in a mining operation is challenging, because different mines within the business can be working off completely different generations of control systems. "In the OT network, it's obviously going to take a lot of finesse," concludes Mendez. ■

Reducing Industrial Risk:
20 Experts Share Strategies for Managing OT Cybersecurity

Download the full e-book: Reducing Industrial Risk:
20 Experts Share Strategies for Managing OT Cybersecurity

KEY POINTS

1 **One way to document everything is to start with a vendor who can make a complete assessment and report on all your PLCs and controllers, and then move forward from there.**

2 **OT network controls need to include proper onboarding of new systems, proper patching, proper updates, proper backups, antivirus, and standard operating procedures.**

OT SECURITY BEGINS WITH A TECHNICAL STANDARD OF CRITICAL SECURITY ELEMENTS

JACOB LAAS GLASS

Head of Industrial
IT & Infrastructure
Total TEPDK

Jacob Laas Glass's first position at Maersk Oil was instrument/automation engineer in 2006. Since then, he has been involved in many projects, including the installation of ICS systems on oil-producing platforms. He has also worked in the telecom and MES side of ICS, moving to OT security. He played a key role in establishing guidelines and corporate standards for the company. He currently leads a team of OT specialists dealing with OT security, critical infrastructure, and real-time data, analytics, and predictive maintenance.

Website I LinkedIn

Jacob Laas Glass, who is responsible for integrated operations and ICS security on six offshore oil platforms, knows what would make ICS security easier for him. "Vendors always think their system is the only system in the world that's going to install on a platform," he says. "But if they had the view that they are part of a much bigger thing, we would have a much simpler solution offshore. That would be my request. Please, vendor, consider you are not the only one in the world."

As the ICS industry gives more consideration to cybersecurity, vendors must develop a more holistic view. But for now, Glass must contend with an OT environment that is complex and difficult to secure. He has adopted several practices that have greatly improved cybersecurity in his environment. These include:

> *Every time we install something, we apply a Swiss cheese model against the standard. If there's something we can't do, we look for what we can do in the system to cover for that security element.*

- **Begin with a technical standard of critical security elements.** OT control systems often require multiple components to work together in order to perform a control function. Every device in that control system could have a critical safety impact on the overall system's function. When a device is installed, all the ways it could negatively impact the system must be evaluated. Glass recommends applying the same strategy to evaluate ICS from a security perspective. »

Begin with a technical security standard that the system and its components must meet. “Every time we install something, we apply a Swiss cheese model against the standard. We look at it to see what can be set up initially, what we can prevent, what we can detect, what we can respond to, and what we can recover. If there’s something we can’t do, we look for what we can do in the system instead to cover for that security element,” he notes. When something is added to the system, one way or another the system as a whole must still meet the standard of critical security elements.

- **When in doubt, assume a protection is not there.** In Glass’s environment, systems are pretty well documented from a cabling standpoint. However, documentation of device configuration is often poor. New technology that detects OT devices and their configurations has been a tremendous help in providing greater visibility, but there still can be areas of uncertainty. “For example, it might not be clear if a device is configured with a host firewall. In this scenario, we have to assume that it’s not there, and then develop a plan for hardening that device or network.” This involves a lot of work and help from vendors. >>

> “Someone could just sit in their security officer chair and say, ‘No, that’s not possible.’ But we have to make it possible. That’s the whole point with OT. We have to make it possible because there’s a lot of money involved.”

OT SECURITY BEGINS WITH A TECHNICAL STANDARD OF CRITICAL SECURITY ELEMENTS

“Some vendors know how to protect their own systems, but others do not get involved in industrial security. Then we do it ourselves,” says Glass.

- **Establish an OT department that works closely with the IT department.** This gives OT people access to IT people, who typically have more detailed technical knowledge about cybersecurity issues. In Glass’s organization, although the OT department resides in the IT department, it is still totally responsible for operations and OT security. But sitting next to the IT people has been a big help. “Every time we connect a device, we have different information from the vendor. ‘This is possible, this is not possible’ and so on. We get our network guy and the IT guy together and we apply our Swiss cheese model—what can we do to prevent, detect, and respond. That has helped us create good, secure solutions. “

Having a security standard for control systems, and working with IT to help implement them has been very effective for Glass. “Someone could just sit in their security officer chair and say, ‘No, that’s not possible.’ But we have to make it possible. That’s the whole point with OT. We have to make it possible because there’s a lot of money involved” he says.

Reducing Industrial Risk:
20 Experts Share Strategies for Managing OT Cybersecurity

Download the full e-book: Reducing Industrial Risk:
20 Experts Share Strategies for Managing OT Cybersecurity

KEY POINTS

1 **New tools detect OT devices and their configurations and providing greater visibility, but there still can be areas of uncertainty. When in doubt, assume a protection is not there.**

2 **When something is added to the system, one way or another the standard of critical security elements must always be met for the system as a whole.**

DALE PETERSON

Founder and CEO
Digital Bond, Inc.

Twitter

Website

LinkedIn

> *There's a tendency to focus ICS cyber risk reduction efforts primarily, or even exclusively, on deploying security controls to reduce the likelihood of an incident. Make sure you are also considering ways to reduce the consequence of an incident. This is often the most effective and efficient ICS risk reduction action, and it also caps the risk in a way that can be easily explained to executive management.*

STRATEGIES FOR SECURING DIGITAL ASSETS IN NUCLEAR POWER PLANTS

GABRIEL AGBORUCHE

Cybersecurity Specialist
Westinghouse Electric

Gabriel Agboruche is a cybersecurity specialist in the field of nuclear energy who is always looking for a challenge. As an engineer, he enjoys developing simple, easy-to-understand solutions to today's complex problems. As a person, integrity, character development, and commitment are the driving factors that heavily influence all aspects of his life.

LinkedIn

Unlike some OT environments, nuclear power plants are heavily regulated. Nuclear Regulatory Commission (NRC) inspections, which include an evaluation of cybersecurity, typically occur every two years during scheduled outages for plant refueling. This is also when other plant maintenance occurs, such as updating and re-engineering control systems.

But even in this tightly controlled environment there can be devices that introduce vulnerabilities. "When systems are out there in the plant, they often stay there until they fail. One thing we evaluate is the health of those particular assets," says Gabriel Agboruche, who has spent much of his career as a cybersecurity engineer and specialist.

> *Having rogue devices in your OT environment that you don't have control over is a big problem.*

The OT environment in a nuclear power plant is made up of layers of criticality, each one separated from the others by an air gap. One of the challenges in securing these systems while using modern ICS components is preserving those air gaps. Agboruche follows these practices in securing the plant's OT systems:

- **Have a correct, accurate account of all digital assets within your plant.** This includes knowing what you have, understanding how and what those devices control, and working with IT people to understand the data inside those control systems. This is important for safe and secure operation of the plant, and it also helps with NRC inspections. »

"Having rogue devices in your OT environment that you don't have control over is a big problem," Agboruche notes.

- **Assess critical vulnerabilities immediately.** "As soon as we learn of any vulnerabilities or any possible threats that might be coming from anywhere, we have to evaluate our systems to make sure the plant is not at risk," says Agboruche. These might be alerts from control system vendors, or information about a new kind of ICS attack such as Stuxnet. "We don't just hear about things and say we're OK. We need to be able to evaluate our systems to make sure that we're not vulnerable to the same type of attack with the same issues," he comments.
- **Carefully evaluate every piece of equipment that goes into the plant.** This is a continuous process that not only involves looking at new equipment, but it also means evaluating existing systems and comparing those to similar systems in other plants. Agboruche notes that an important part of nuclear power plant cybersecurity is sharing information with other plants. "Sometimes we'll hear from another plant that may have a more mature cybersecurity program. We'll evaluate our systems compared to theirs. We'll do our own evaluation too on the back end, so we have a thorough look at the different vulnerabilities," he says. »

> "As soon as we learn of any vulnerabilities or any possible threats that might be coming from anywhere, we have to evaluate our systems to make sure the plant is not vulnerable to those things."

Agboruche points out that there is no way to completely eliminate cyber risk, but people often don't recognize there are risks when you open up your network to certain types of technologies or even vendors. He cites as an example one type of handheld communicator used to wirelessly configure different devices within the plant. It sends and receives proprietary communication protocols. The newest versions of that device now have Bluetooth capabilities. "There's a new vector of interest for somebody who might have malicious intent. Are we comfortable with this? There needs to be an evaluation. If we're comfortable with it, what are we doing to protect against it?"

Agboruche believes that inside an OT operation, data itself is ultimately the most critical asset, but not because of the intrinsic value of the data. "Data is your primary asset because that is what is interacting with the physical world," he says.

Reducing Industrial Risk:
20 Experts Share Strategies for Managing OT Cybersecurity

Download the full e-book: Reducing Industrial Risk:
20 Experts Share Strategies for Managing OT Cybersecurity

KEY POINTS

1 **People often don't recognize there are risks when you open up your network to certain types of technologies or even vendors.**

2 **Know what you have, all the current configurations of those devices, understand what those devices control, and understand how the data is actually working inside those ICS systems.**

ERIC COSMAN

Co-Chair, ISA99 Committee
ISA

Website

LinkedIn

The most effective asset discovery is accomplished using a combination of automatic and manual methods. It should begin with a simple query or survey of those most familiar with the operations environment, asking them to share diagrams or other records of their configuration. If records are inaccurate, incomplete or nonexistent, some sort of scanning may be required; but it must be as passive or non-obtrusive as possible in order to avoid accidental tripping of equipment. Under no circumstances should scanning be performed without knowledge, permission, and involvement of operations personnel.