MITSUBISHI POWER

WHITE PAPER:

POWER PLANT CYBERSECURITY IN A GLOBALLY CONNECTED WORLD

POWER PLANTS AND THE ENERGY TRANSITION

Energy markets around the world are demanding more and more from power plants as the energy transition accelerates. Thermal power plants originally built for baseloads are increasingly being expected to operate profitably at partial loads and start and stop much more frequently due to the unpredictability of different types of renewable energy and the need for economic dispatch. Ongoing grid reliability requires extraordinarily flexible support, including sustained reliability, faster and more reliable startups and very fast load change response while maintaining the online rotating inertia and spinning reserve the grid needs.

Emerging energy-storage technologies may assist in the longer term, but they will need new forms of coordination and cooperation among all forms of energy supply in an integrated grid.

Improved communication and connectivity between thermal power plants, renewable and distributed generation, energy storage and the grid are imperative to provide actual real-time data to support decision-making. Many critically needed thermal power plants will also be called upon to transition to newly available low-carbon or zero-carbon fuels,

in some cases expanding their mission to long-term energy storage as well. This makes it essential to eliminate an "island mentality" and make connections between geographically separated critical masses of information and knowledge in order for the energy transition to be successful.

The rise of digital communications and connectivity will improve the safety, productivity, accessibility and sustainability of energy systems around the world. But it is also raising new cybersecurity risks that must be proactively addressed.

RISING CYBERSECURITY AWARENESS AND REGULATORY REQUIREMENTS

With the increased need for digital communication and connectivity to maintain grid stability and improve plant performance, cybersecurity of data and infrastructure is critical. In fact, many U.S. executives now consider cyberattacks the number-one risk companies are confronting, according to a PwC Pulse survey in early 2022.

In many regions around the globe, standards and requirements for cybersecurity of power plants have been established. In North America, the North American Electric Reliability Corporation (NERC) is a not-for-profit international regulatory authority whose mission is to assure the effective and efficient reduction of risks to the reliability and security of the grid. NERC has established Critical Infrastructure Protection (CIP) standards and requirements that must be met, and there are severe penalties for noncompliance.

Also in the U.S., the U.S. Department of Homeland Security established the Cybersecurity and Infrastructure Security Agency (CISA) to coordinate government-level actions to reduce and eliminate threats to U.S. critical infrastructure.

Other regions around the world are creating their own standards, in many cases building upon the NERC CIP and CISA activities, to govern cybersecurity in their regions.

In addition to regional standards and requirements, there are also internationally accepted standards such as ISO/IEC 27001/2 Information Security, Cybersecurity and Privacy Protection; ISA/IEC 62443 Security for Industrial Automation and Control Systems, as well as best practices defined by resources such as the NIST Cybersecurity Framework.

These regulations and compliance resources help organizations understand and improve their management of cybersecurity risk, but that management is increasingly complex as well as critically important because of the growing need for connectivity driven by the energy transition.

THERE ARE CURRENTLY 13 CIP STANDARDS THAT ADDRESS CYBERSECURITY.

These are periodically updated, and additional CIP standards are expected. The NERC CIP standards require utility companies in North America to establish and adhere to a baseline set of cybersecurity measures.

STANDARD	DESCRIPTION
CIP-002-5.1a	Bulk Energy System Cyber System Categorization
CIP-003-8	Security Management Controls
CIP-004-6	Personnel & Training
CIP-005-7	Electronic Security Perimeter(s)
CIP-006-6	Physical Security of Bulk Energy System Cyber Systems
CIP-007-6	System Security Management
CIP-008-6	Incident Reporting and Response Planning
CIP-009-6	Recovery Plans for Bulk Energy System Cyber Systems
CIP-010-4	Configuration Change Management and Vulnerability Assessments
CIP-011-2	Information Protection
CIP-012-1	Communications between Control Centers
CIP-013-2	Supply Chain Risk Management
CIP-014-2	Physical Security

SECURE CONNECTIVITY IS REQUIRED FOR OPERATIONS & MAINTENANCE SUPPORT

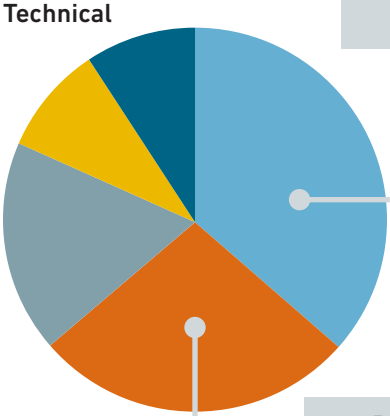
Compounding the challenges of cybersecurity compliance are staffing and expertise shortages. Many people have retired from the industry or have left due to the global COVID pandemic.

Furthermore, the reduced energy sales generated by thermal power plants and more severe duty cycles caused by integration with renewable generation are challenging O&M budgets and making it increasingly difficult to maintain broad expertise locally at each power plant.

Due to these staffing-related challenges, real-time remote and online services and support are needed to replace declining on-site expertise at power plants. The real-time and online services require greater connectivity which, in turn, increases the need for robust cybersecurity.

A recent survey of power plant owners and operators with Mitsubishi Power gas turbine combined cycle (GTCC) systems showed that remote support of O&M activities is the second most important technical priority and the most important service & support priority.

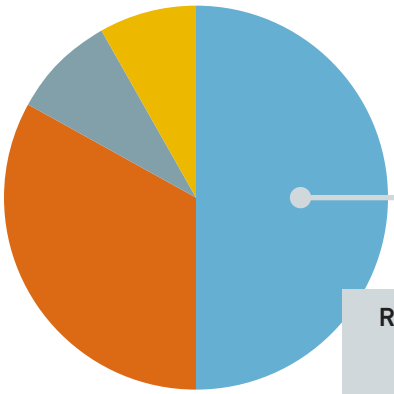
Technical



Flexibility is most mentioned technical key issue.

Remote support is second most mentioned technical key issue.

Service & Support



Remote support is most mentioned service & support key issue.

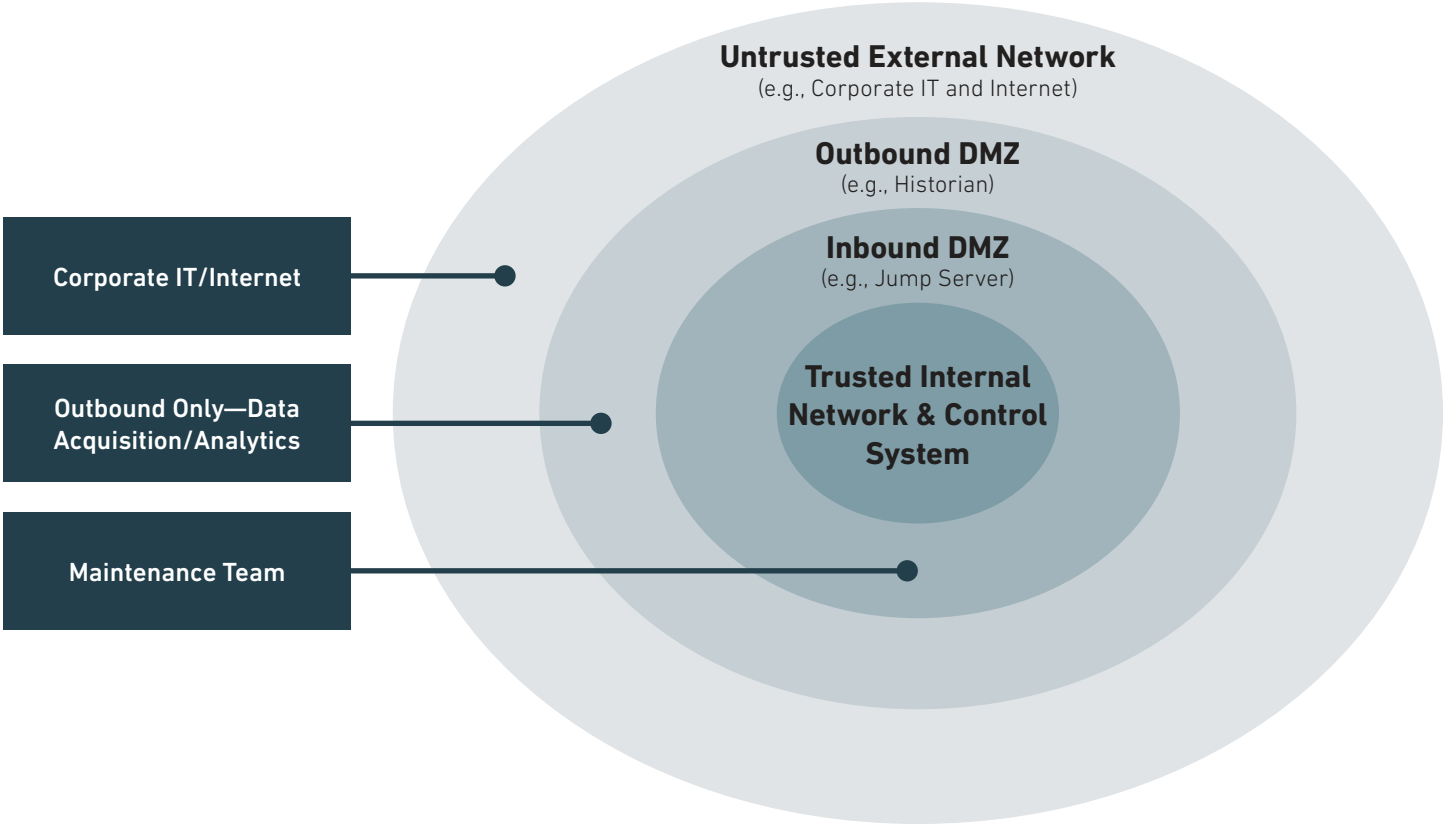
SECURE CONNECTIVITY IS DESIRABLE FOR COORDINATED ENERGY MANAGEMENT

The energy transition is also creating power-supply networks with increasing penetration of geographically dispersed renewables, distributed generation and energy storage. These networks of the future will be much more complex to operate effectively and efficiently than traditional power systems. Advancements in digital sensing, control and communication, along with advancements in machine learning and AI, are increasingly enabling optimal connections between physical equipment, digital systems and human activities. Those connections will be needed more and more to connect and dynamically manage generation sources and loads to assure the reliable and economically optimized energy generation, transmission and distribution required to support the energy transition and associated decarbonization objectives.

ENSURING SECURE CONNECTIVITY REQUIRES NETWORK SEGMENTATION

Effectively countering these threats requires a multilevel approach to network design and security. The trusted internal network and plant control systems must be carefully isolated from less trusted networks by segmented security zones with multiple levels of access control.

There should be "demilitarized zones" (DMZs) between security zones, and there should be multiple security controls within each security zone. There is a big difference in criticality between outbound data flows and inbound data flows. Outbound data is typically used for data acquisition, analytics and external awareness of system status. Inbound data is typically used for important management of automated grid integration, control settings updates and software patches.



DEFENSE IN DEPTH IS NEEDED TO FORTIFY PLANT CONNECTIVITY

Combating potential attacks on control systems and data flows while fortifying plant connectivity requires multiple security controls and protocols. No one technology or protocol can catch everything, which is why a multilayered approach is essential. Because of the diversity of threats, it's important to have more than one type of tool looking at threats from different angles. Such available technologies and protocols for cybersecurity include:

- **Antivirus and anti-malware software—**Including the latest antivirus and anti-malware software is an essential first line of defense. Antivirus software usually deals with older, more established threats, such as Trojans, viruses and worms. Anti-malware typically focuses on newer threats, such as polymorphic malware and malware delivered by zero-day exploits.
- **Protocols for source domain access—**Another critical layer of plant cybersecurity is to establish protocols around who has source domain access, with strict limitations and tight controls.
- **Explicit evaluation of threat vectors—**"Threat vectors" can be used interchangeably with "attack vectors" and generally describe the potential ways a hacker can manipulate a network or computer system or extract data. The number of vectors needs to be limited so any attack can be contained.
- **Automated intrusion detection and response—**Security automation is the machine-based execution of security actions with the power to programmatically detect, investigate and remediate cyberthreats by identifying incoming threats, triaging and prioritizing alerts as they emerge, then responding to them in a timely fashion.
- **Control of portable devices—**Attackers can use USB drives and other portable devices to infect other computers with malware, and organizations must restrict the use of such devices. If one is required, encryption on the device is essential.
- **Dedicated machines—**Establishing dedicated computers that are the only ones used for connectivity and digital communications limits access and cyberthreats.
- **Remote kill switches—**Connectivity should be established with remote kill switches that can be used in the event of a cyberthreat or unscheduled connection.
- **Systems with minimum attack footprint—**It is essential to design network and digital connectivity with a minimum attack footprint, thereby restricting the chances of an attack.
- **Apply principal of least-privilege access—**This means giving access to only those privileges needed for someone to complete a task. If a subject does not need an access right, the subject should not have that right, thereby reducing the prospect of cross-contamination from an attack.

ACTIONS OFTEN OVERLOOKED

The human aspect is the most difficult threat to manage, be it a clever intruder, malicious insider or just a careless operator.

Physical security is the most often overlooked part of cybersecurity and one of the most important. Physical security protects cybersecurity by limiting access to spaces where data is stored, control equipment resides and network communication takes place. In addition, peripheral components connected to the internet, such as RFID key card door locks, smartphones and video surveillance cameras, are common targets for hackers and need to be protected.

Many plants also have room to improve their IT and OT management practices and administrative controls. Simple things like closing the accounts of users who have left the company, applying least-privilege access protocols, conducting training and regularly testing the systems and plant practices are often not kept up to date. It also critical to keep operating systems and software up to date to ensure the latest upgrades and lessons-learned are in place.

It is important to have a core of experienced cybersecurity expertise at the power plant that knows the principles of cybersecurity and can be the first responder at the site when the system itself is under attack and the normal safeguards have possibly been broken through. These are also the people who would ultimately be directly responsible for keeping plant systems up to date. Steps to effectively establish this core expertise include:

1. **Determine needs.** It's important to first assess the organization's specific cybersecurity needs and requirements. This will help determine the type of cybersecurity personnel needed and the skills and experience they should have.
2. **Look for relevant experience and certifications.** Look for candidates who have experience in the cybersecurity field, particularly in the energy or utility sector. Experience in these areas can be particularly valuable, as it suggests a familiarity with the types of systems and challenges commonly found in power plants. Also look for cybersecurity professionals who hold certifications, such as Certified Information Systems Security Professional (CISSP) or the Certified Ethical Hacker (CEH).
3. **Consider hiring a managed security service provider (MSSP).** If a full-time cybersecurity team isn't feasible, consider hiring an MSSP to handle your cybersecurity needs. MSSPs can provide a range of services, including monitoring and protecting your systems, as well as responding to security breaches.
4. **Foster a culture of security.** Most important is to foster a culture of security within the organization, and this should extend to hiring practices. Look for candidates who demonstrate a commitment to security and are able to effectively communicate the importance of cybersecurity to their colleagues.

COMPREHENSIVE CYBERSECURITY SOLUTIONS INTEGRATE MULTIPLE STRATEGIES AND TECHNOLOGIES

Managing the different aspects of cybersecurity is a very difficult task, even with significant staffing and budgets. As a result, many power plants supplement their internal expertise with outside products and services to help manage cybersecurity.

For example, the TOMONI® Security Suite from Mitsubishi is a comprehensive suite of cybersecurity solutions that offers the latest technologies and upgrades of edge- and plant-based control systems for the highest level of OT cybersecurity. Its Netmation Protect Pack, paired with the Mitsubishi Netmation control systems that many power plants utilize, is NERC CIP compliant, including firewalls and available two-factor secure password authentication. It provides an industry-leading benchmark for cybersecurity best practices.

Netmation Protect Pack operational testing for multiple power blocks at Mitsubishi Power Cyberlab, Orlando,

Important features of a comprehensive cybersecurity solution should include:

- **Managed control logic updates and software patches—** It is essential to manage any control logic changes and patches and, in particular, to verify the authenticity and compatibility of patches prior to deploying at any power plant site. Encrypted hard drives should be provided to plant operators, and secured remote communications should be utilized during updates and patch deployment. A system designed for proper cybersecurity must also support proper disaster recovery.
- **Virtualized HMI—**Human machine interfaces (HMI) are access terminals that give plant personnel and other end-users a way to visually monitor and adjust automated operations, machine controls and output functions. HMI virtualization provides a smaller attack footprint than physical multi-workstation implementation, and it is easier to maintain the physical security of server-based systems than multiple individual systems. It also provides much better access control because it is centrally managed. Integrated intrusion detection systems and failover capability for HMI and OT network components are more robust, resilient and reliable when compared to current physical systems. In addition, it provides centralized disaster recovery with automated backup systems.
- **Dedicated circuits and encrypted VPNs—**An encrypted VPN should be created between two or more firewalls and set up with private dedicated circuits. The firewalls should be set up to only talk to one another and confirmed through a code. When the firewalls pass traffic back and forth, they should encrypt the traffic so no one else can read it, creating a virtual tunnel between the locations.
- **Multifactor authentication—**Multifactor authentication is increasingly considered to provide added layers of password security. For future application, biometric authentication, a security process that relies on the unique biological characteristics of individuals to verify they are who they say they are, is increasing in reliability and provides an even higher standard that should be considered.
- **Configuration and change management—**Configuration and change management are vital, and this extends beyond software version and patch management. The configuration of hardware, virtual machines, virtual networks, containers and storage all need to be closely controlled, and specific configurations need to be evaluated for vulnerabilities, including intrusion testing. It is also important to review the histories and previous threats to better understand the type of attacks that might be coming. For example, knowing what is installed in the system at all times allows the security team to quickly evaluate emerging threats such as those contained in CISA emergency directives.
- **Incident, log and event management—**Access and activity logging as well as intrusion detection logs are required to produce the documentation and reports important to regulatory compliance.

- **Intrusion testing and third-party assessment—**Testing and third-party assessment are essential parts of creating a strong cybersecure plant.

  It is important to conduct intrusion testing, sometimes called security testing or penetration testing, to scan the system for vulnerabilities such as security holes, open ports and other issues with the security of the network or system.

  A third-party risk assessment is an in-depth examination of each vendor relationship a business has established. This assessment looks to identify possible security risks associated with the vendors, and how these pitfalls can be mitigated.

SUCCESSFUL EXPERIENCE

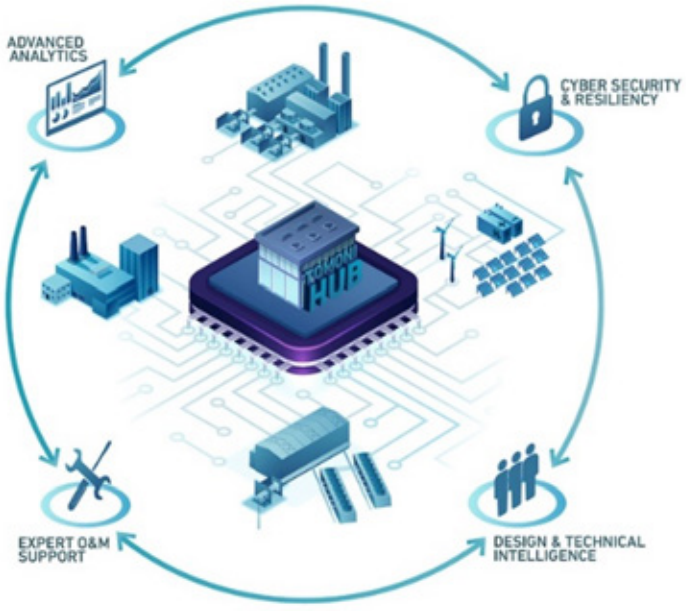
Remote connections to provide monitoring and diagnostics (M&D) of power plants have been common in the industry for more than 20 years and provide a good baseline of experience to demonstrate the feasibility of and requirements for cybersecure external data, analytics and control connections.

One example of long-term successful and cybersecure connectivity for M&D is the network of TOMONI HUBs, which has already become an integral element in the support of many power plants' successful O&M results. The name "HUB" conveys the central role these facilities are increasingly playing in channeling expert O&M support for on-site personnel and an evolving workforce.

New technical capabilities introduced in recent years include remote inspection and maintenance via virtual presence technologies, as well as remote operation. Many of the technologies were validated at Mitsubishi Power's T-Point 2 power plant, the smartest power plant in the world, which is currently being operated remotely from the Takasago, Japan, TOMONI HUB.

The TOMONI HUBs use a combination of point-to-point dedicated and encrypted VPN communication and the most secure aspects of the Microsoft Azure Cloud technologies along with firewalls and data diodes to prohibit data flow from outside to inside more strictly than standard firewalls. There have been no penetrations or other adverse security issues reported with these connections in thousands of unit-years of operation.

Additional experience is being confirmed by the extensive and growing fleet of GTCC and steam power plants being successfully protected by the TOMONI Security Suite, further demonstrating that cybersecure connections are possible for any power plant with the right level of technology, experience and focus.



CONCLUSIONS

For power plants taking an active and enduring role in the energy transition, connectivity and digital communication are required. Safe, secure connectivity and digital communications have been proven possible with knowledge, understanding and the right attention.

As energy needs diversify, regulations increase and new threats emerge, identifying the right solution is more challenging than ever. There are many organizations promoting power plant cybersecurity solutions with varying degrees of complexity and comprehensiveness—which is why having the right partner by your side is crucial. If you have an issue or question related to power plant cybersecurity, you have a team at Mitsubishi Power that can help with practical real-world advice.

TOMONI® is a suite of intelligent solutions that accelerates decarbonization with power plant design, O&M and system knowledge, together with strong customer and partner collaborations. TOMONI leverages advanced controls, artificial intelligence and machine learning with multilayered cybersecurity to make energy systems smarter, more profitable and, ultimately, more autonomous on the road to a sustainable future.

TOMONI®

- Data Foundation & Enablers
- O&M Optimization
- Performance Improvement
- Flexible Operations

METP-11DS45E2-A