OPERATING PLANTS SECURELY IN A "NEW NORMAL" ENVIRONMENT

BY JAIME FOOSE

Manager, Security Systems
Emerson Process Management

Call it the "new normal." Cyber threats targeted to the power generation industry are growing in both frequency and complexity. Meanwhile, cybersecurity compliance obligations continue to evolve.

In this environment, there is increased urgency for utilities to secure their systems, establish security programs and comply with regulations. This can be daunting, as power plant staffing is often lean, with personnel facing many demands on their time. More and more, utilities are turning to control system suppliers for help.

With a staff that offers a rare combination of necessary skills, a blend of cybersecurity, control system and power industry experience, control system suppliers are uniquely qualified to help utilities identify areas of risk related to automation and control within their plants. While Emerson has always worked closely with customers on security matters, the company's Security Solutions group recently expanded its cybersecurity services portfolio, offering a best practices approach for helping power generators achieve a strong security posture. The portfolio includes: cybersecurity assessments, scheduled cybersecurity services, and security program & compliance services.

CYBERSECURITY ASSESSMENTS

Cybersecurity assessments are designed to assist power generators in identifying their cyber assets, assessing vulnerabilities, and providing recommendations to mitigate cybersecurity risks through the deployment of appropriate security controls and safeguards. The cybersecurity assessment service includes:

- Initial site walk down to identify targeted systems and key deliverables
- Detailed assessment plan
- Plant-wide cyber asset inventory and audit
- Network mapping of targeted systems
- Host-based vulnerability assessment with port, protocol, service and system scanning
- Network security analysis
- Risk mitigation analysis, review and reporting
- Mitigation and remediation recommendations

Assessments are recommended annually to evaluate and track continuous improvement of an organization's security posture.

SCHEDULED CYBERSECURITY SERVICES

Patch management, antivirus protection, and backup and recovery initiatives are often at the core of an organization's security program. Industry best practices suggest deploying patches monthly, updating antivirus definitions weekly, and performing frequent backups. Unfortunately, the work required to complete these updates adds to the workload of plant staff.

Scheduled cybersecurity services include regularly scheduled visits to customer sites to deploy patches; update and install antivirus definitions; and generate, verify, and archive backups – all without diverting essential manpower from other important assignments. This service can also be customized to include other cybersecurity or preventive maintenance tasks that require regular attention, such as review of overall heath and diagnostics for key control system components including servers, workstations, controllers and network equipment.

SECURITY PROGRAM & COMPLIANCE SERVICES

They say the devil is in the details, and that is certainly true for security programs and compliance – particularly in light of the ongoing evolution of the North American Electric Reliability Corporation's (NERC) Critical Infrastructure Protection (CIP) standards. This service area is focused on helping utilities evaluate, develop and implement security and compliance programs that meet compliance obligations while also following power industry best practices. This is an important distinction, as an established best practice followed in the financial or IT industry is not necessarily a best practice for the power-generation industry, and may in fact be detrimental. For example, in many office environments it is considered an IT best practice to lock users out of their workstations after a defined period of inactivity. However, this could have serious consequences in a control room, particularly if the operator forgets the password and cannot log back in. This is a good illustration of why common sense and power industry best practices should prevail.

Tasks related to security programs may include:

* Identifying compliance gaps
* Gathering evidence and supporting documentation required for compliance audits
* Developing and revising security processes & procedures as needed
* Conducting cybersecurity awareness training

NO SINGLE SOLUTION

Just as no two power plants are

(continued page 8)

OPERATING PLANTS SECURELY

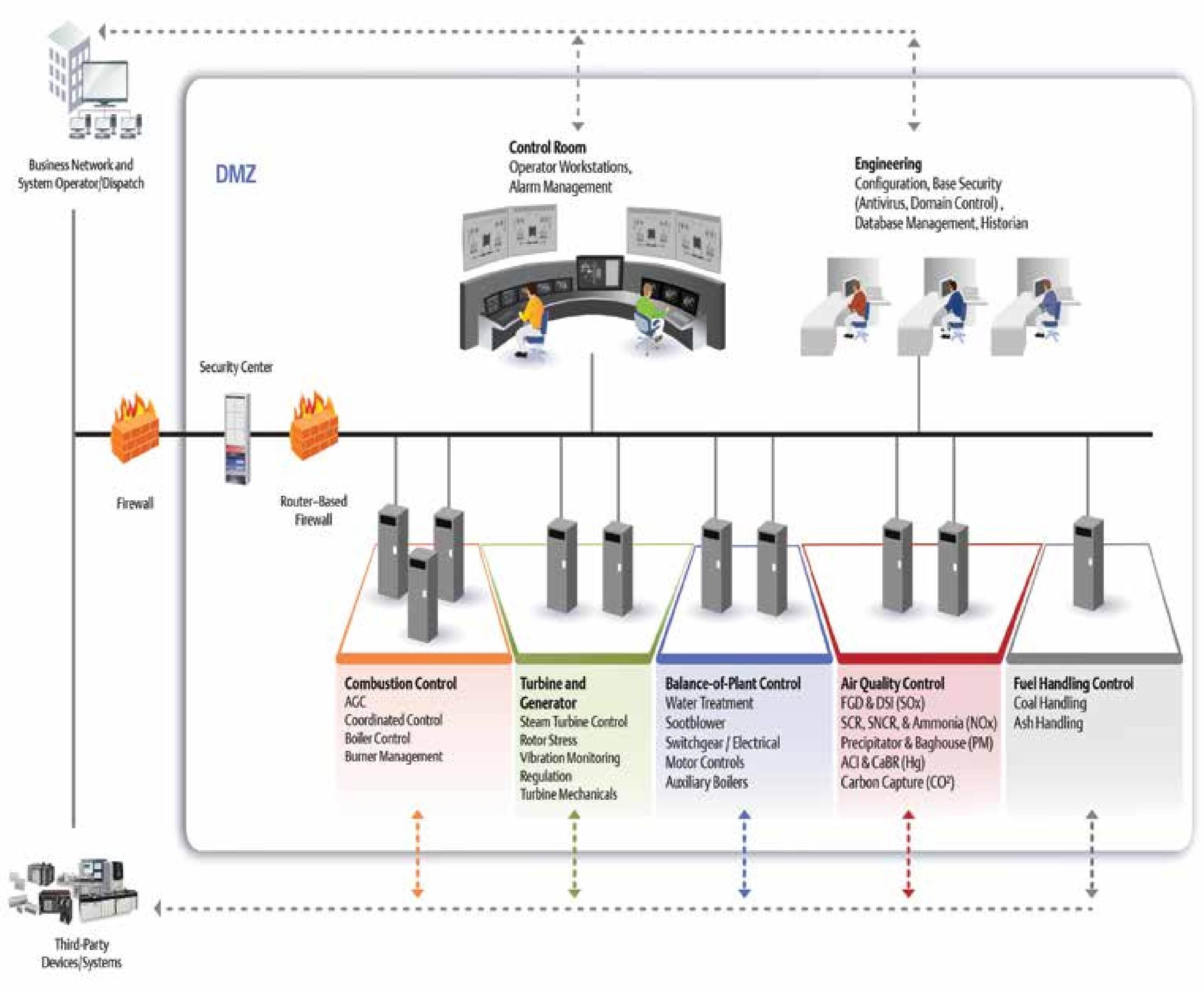
CONTINUED FROM PAGE 7

identical, there is no single solution for addressing evolving cybersecurity threats. As such, cybersecurity services should be customized to fit within the framework of an organization's existing programs and initiatives whether they are at a single location or across an entire fleet.

For certain, the power industry will continue to face increasing cybersecurity threats, as well as evolving compliance obligations. In the face of these pressures, it is prudent to develop security programs based on compliance obligations and security best practices. This is the best approach to ensure systems are truly secure, organizations are compliance-ready and reliable megawatt production is maintained.

JAIME FOOSE

Jaime Foose is the manager of the Security Solutions group at Emerson Process Management Power & Water Solutions. This group is focused on ensuring a strong security posture and supporting clients needs as they meet the challenges of NERC CIP compliance and cybersecurity in general. She has 14 years of extensive and varied experience in program and project management, project execution and software development, including work in the areas of cybersecurity/NERC CIP, digital bus technologies, SCADA, Ethernet and serial communication interfaces for power applications. Jaime holds a Bachelor of Science degree in computer science from University of Pittsburgh, as well as a Master of Science degree in information technology and project management and a Master of Business Administration degree, both from Robert Morris University.


Business Network and
System Operator/Dispatch
DMZ
Control Room
Operator Workstations,
Alarm Management
Engineering
Configuration, Base Security
(Antivirus, Domain Control),
Database Management, Historian
Security Center
Firewall
Router-Based
Firewall
Combustion Control
AGC
Coordinated Control
Boiler Control
Burner Management
Turbine and
Generator
Steam Turbine Control
Rotor Stress
Vibration Monitoring
Regulation
Turbine Mechanicals
Balance-of-Plant Control
Water Treatment
Sootblower
Switchgear / Electrical
Motor Controls
Auxiliary Boilers
Air Quality Control
FGD & DSI (SOx)
SCR, SNCR, & Ammonia (NOx)
Precipitator & Baghouse (PM)
ACI & CaBR (Hg)
Carbon Capture (CO²)
Fuel Handling Control
Coal Handling
Ash Handling
Third-Party
Devices/Systems