



Cost-effective, system-wide services for NRC-mandated industries.

Keeping a security system up to date and performing optimally is at the top of the priority list for government-mandated critical infrastructure facilities. But it can also consume resources, time and budget, as well as require increasingly complex skill sets to manage in house. Allowing an experienced life cycle management (LCM) provider like Rockwell Collins to take on this responsibility can be the most efficient and reliable way to avoid disruptive events and costly fines.

Our LCM package includes everything from preventative and corrective maintenance for all hardware and software to spare parts management, cyber software patches and vulnerability remediation. Our focus is to help you maintain compliance with NEI 08-09 and other regulatory requirements while achieving a high level of responsiveness, peak operational efficiency and high system availability at all times.

PREVENTIVE MAINTENANCE

Maintenance prior to corrective action being required helps you stay ahead of and possibly avoid problems. We use documented and approved procedures on site and provide detailed reports of completed maintenance, issues noted and corrective actions required, including system wear and tear, patch-related issues and defective product failures.

CORRECTIVE MAINTENANCE

Corrective maintenance covers hardware and software issues for subsystems, including security access control and alarm monitoring multiplexer panels, network switches and routers, security computer equipment and security video head-end equipment.

KEY BENEFITS

- > Cost-effective LCM services that mitigate operational disruptions and fines
- > Proven critical infrastructure security expertise
- > Helps you achieve NEI compliance
- > Maintenance for all hardware and software
- > ISO-certified spare parts management
- > Cyber patching and validation



CYBERSECURITY LCM

A cornerstone of Rockwell Collins' LCM services is cybersecurity patch validation. Critical for on-going vulnerability remediation, cyber patches help maintain a Nuclear Energy Institute (NEI)-compliant, integrated, software-based system.

We evaluate patches biannually for the expected and unexpected to maintain applicability, usability and viability, soaking them for several weeks in a non-production environment to minimize the risk of negative impacts on your entire operational system. We validate system patches and other updates and release them in scheduled maintenance events, configuring settings to ensure preventive technical security controls are still intact as tested and delivered.

Regression testing on software components provides the updated patch set for installation to ensure that comprehensive testing and documentation can be completed. Preventative maintenance is performed on a periodic basis and includes system-level, operating systems, network switches and anti-virus applications.

SPARE PARTS MANAGEMENT

Spare parts in today's highly integrated systems can quickly become obsolete and costly. We ensure system maintainability and mitigate risks by taking a two-tiered approach, including on-site spares and vendor support on the entire inventory.

Our ISO-certified management program ensures the viability and usability of your spare parts inventory. We perform annual inspections of the inventory to verify that all parts are compatible with the current system configurations and are available for immediate deployment.

Building trust every day.

Rockwell Collins delivers innovative aviation and high-integrity solutions that transform commercial and government customers' futures worldwide. Backed by a global network of service and support, we are deeply committed to putting our solutions to work for you, whenever and wherever you need us. In this way, working together, we build trust. Every day.

For more information, contact:

Rockwell Collins
2551 Riva Road
Annapolis, MD 21401
866.633.6882 | +1.410.266.4000
criticalinfrastructure@rockwellcollins.com
rockwellcollins.com