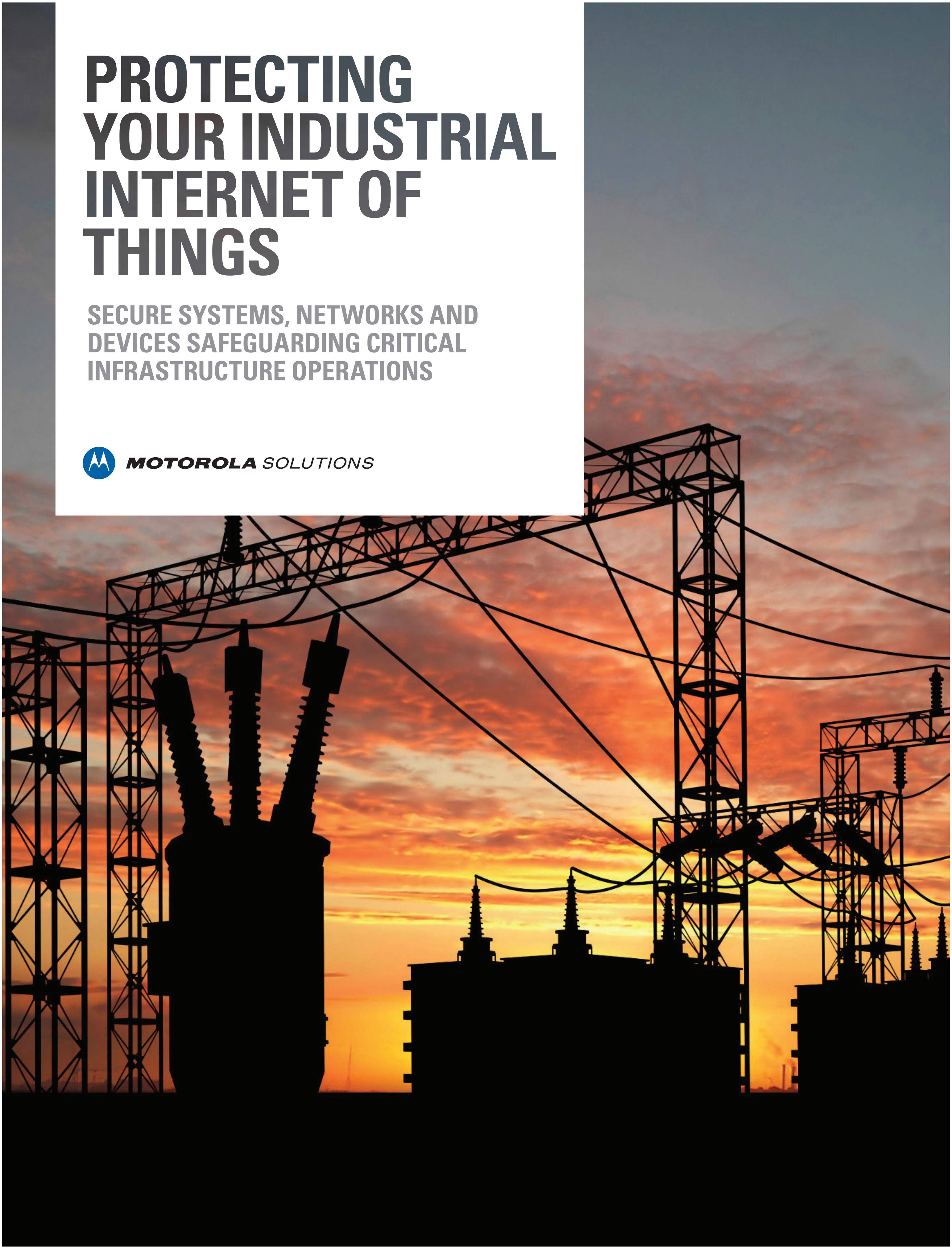
PROTECTING YOUR INDUSTRIAL INTERNET OF THINGS

SECURE SYSTEMS, NETWORKS AND DEVICES SAFEGUARDING CRITICAL INFRASTRUCTURE OPERATIONS

MOTOROLA SOLUTIONS



PROTECT YOUR DAILY OPERATIONS FROM BEING COMPROMISED

In today's data-driven society, connectivity comes with a cost. Your formerly isolated control and monitoring systems are now integrated with numerous enterprise systems and technologies to increase efficiencies. But, this also creates new vulnerabilities – from the computers in the control room to the mobile devices in the field.

The surge in wireless Machine-to-Machine (M2M) technologies presents another challenge. The more data they collect from sensors, the better the decision-making, the smarter the use of resources and the safer the workforce. Yet, this increased integration and access – to technologies in the field, communication networks, devices, applications and personnel – can create new attack vectors, and contribute to increased attack vulnerability.

100%
INCREASE IN ATTACKS AGAINST INDUSTRIAL CONTROL SYSTEMS FROM 2013 TO 2014[2]

42.8 MILLION
CYBERSECURITY ATTACKS IN 2014[1]

85%
OF BREACHES TAKE APPROX. 5 MONTHS TO DISCOVER[3]

SECURE THE INDUSTRIAL IoT ACROSS YOUR ENTERPRISE

The Industrial Internet of Things (Industrial IoT) is a game-changer for organizations across critical infrastructure industries. It is transforming the way you work by moving from reactive to proactive decision-making, enhancing personnel safety, and enabling a real-time flow of information for more intelligent work processes and greater productivity gains.

The reality is, aging infrastructure and operational technologies are only as secure as the technology that supports them. Many were not designed with hardened security in mind, and as a result have inherent gaps, are easy to bypass, or provide open access to virtually any user.

That is why it is so critical to fortify your operations against cyber attacks across your entire enterprise. Control and monitoring systems and communication networks and devices must be protected so that data at rest and data in transit, does not become compromised.

83% OF ORGANIZATIONS SAY CYBER ATTACKS ARE ONE OF THEIR TOP 3 THREATS[4]

38% ORGANIZATIONS PREPARED FOR A CYBER ATTACK[4]

TIGHTEN SECURITY WITH THE RIGHT NETWORK, DEVICES AND SERVICES

Make sure your operations are virtually tamperproof with a highly secure, end-to-end Industrial IoT solution.

ASTRO® 25 NETWORK is trusted by millions of users everyday for always available, interoperable communications in mission-critical environments. Future ready and secure, this IP-based virtualized network is scalable and flexible to meet your needs today and into the future.

ACE3600 SCADA REMOTE TERMINAL UNITS handle large volumes of inputs and outputs for critical infrastructure automation and monitoring. With high processing power and enhanced security features, they help you operate safer and more productively, while seamlessly communicating valuable data across your enterprise.

MOTOROLA SOLUTIONS CYBERSECURITY SERVICES professionals work hand-in-hand with you to understand your risk posture, develop a prioritized plan focused on safeguarding your operational integrity, and identify the right tools and services needed to address on-going threats and vulnerabilities.

INSULATE THE INTELLIGENCE AT THE HEART OF YOUR OPERATIONS

THE CONTROL ROOM

Your control center is the heart of your critical infrastructure. Not only is this strategic locale an attractive target for malicious outsiders, it can become compromised either intentionally or inadvertently by insiders. With the convergence of IT and operational technology, any risk to your control room and the infrastructure it contains, can endanger your entire organization – jeopardizing the integrity and continuity of operations.

OUR HIGHLY SECURE INDUSTRIAL IOT SOLUTIONS PROVIDE CRITICAL LAYERS OF PROTECTION FOR ALL POINTS OF ENTRY BETWEEN YOUR COMPUTERS, SYSTEM SERVERS, COMMUNICATIONS NETWORK AND THE OUTSIDE WORLD.

WINDOWS HARDENING

Secure and lock down your Windows-based operating systems to minimize security threats and meet government standards (Federal Information Security Modernization Act of 2014 or FISMA certification).

SERVICE ACCESS ARCHITECTURE

Implement a secured line of communication between your ASTRO 25 mission-critical voice and data network and other enterprise IT systems to gain efficiency of connected systems and networks.

DEMILITARIZED ZONE (DMZ)

Tightly regulate traffic entering your system servers, such as your control center, with a combination of a firewall and intrusion prevention system. The DMZ eliminates common communication ports between the outside world and the internal controlled zone.

ANTI-VIRUS SOFTWARE

Detect, prevent and remove damaging code, such as worms, viruses and Trojan horses on your computers. Workstations and servers that support system applications should have anti-virus software installed. Take special precautions when updating signatures and list management since these usually require an online connection.

APPLICATION CONTROL SOFTWARE (WHITELISTING)

Block unauthorized applications and code on your servers, workstations and field devices by allowing only pre-identified programs to run. The Motorola Solutions ACE3600 Remote Terminal Unit (RTU) and Gateway also have application control mechanisms that are tested with McAfee™ Solidifier.

STRENGTHEN YOUR COMMUNICATIONS BRIDGE

ASTRO® 25 MISSION-CRITICAL NETWORK

ASTRO 25 is the leading mission critical communication network in the world. This IP-based voice and small packet data network is the trusted platform that public safety, government agencies, the U.S. military and thousands more entities depend on for secure, interoperable, always available communications. Ensure protection of the people and technologies your ASTRO 25 network connects, with industry leading security enhancements, built from the ground up.

PROTECT YOUR ASTRO 25 COMMUNICATIONS NETWORK WITH SECURITY SOLUTIONS FOR PROACTIVE THREAT DETECTION, REAL-TIME RESPONSE AND CORRECTION.

ZONE CORE PROTECTION

Protects the ASTRO 25 core so only valid traffic traverses the network's boundaries with alerts for suspicious traffic.

SECURE PARTITIONING

Ensure exclusive database protection wherever you share resources.

DEVICE AUTHENTICATION

Tighten control of your digital radio network by preventing illegitimate users from accessing it and the valuable data it contains.

CENTRALIZED LOGGING

Log security events of interest reported by client devices such as log-in failures, changes made to hardware and software, and failures in security elements to gain visibility into system activity.

FIREWALLS

Ensure only legitimate traffic from external networks can access your ASTRO 25 communication system.

LOG CORRELATION AUDIT MANAGEMENT

Monitor your system more effectively by indexing and correlating log information in real time. Administrators gain fast and easy access to critical information in simple GUI formats.

INTEGRATED DATA ENCRYPTION

Protect data traffic from eavesdropping for integrated data applications on your ASTRO 25 trunked network.

INTRUSION DETECTION SENSING

Monitor all your inbound and outbound network traffic easily and proactively identify suspicious activity that could indicate an attack.

EXTEND PROTECTION TO THE EDGE

ACE3600 SCADA REMOTE TERMINAL UNITS

The ACE3600 RTU for your mission-critical control systems handles large volumes of data for more complex process automation and monitoring. Because it is at the edge of your Industrial IoT and controls and manages any number of operational technologies remotely, it is inherently designed with robust security from the start.

PROTECT ALL POINTS OF ENTRY, LIMIT POINTS OF VULNERABILITY AND PREVENT ATTEMPTS TO COMPROMISE ANY PART OF YOUR SYSTEMS AND DATA WITH THESE PROVEN SECURITY METHODOLOGIES.

SECURITY POLICY ENFORCEMENT

Ensure your users, devices and software tools adhere to the security policy settings established by your system administrators.

FIREWALL

Permit or deny data transmissions into your system, system segment or device based on rules and other established criteria. All IP messages must pass through a firewall which examines each one and blocks those not meeting specified security criteria.

ACCESS CONTROL

Verify access to an RTU is legitimate from both other RTUs or system users with authentication. A name, password and IP address are typical credentials to verify identity with a high degree of confidence.

The ACE3600 RTU offers the option of using a remote authority or authentication server to perform access control or relies on the device itself, such as a RTU or IP Gateway. A user account is required to access any part of the system, whether RTU, Gateway or software management tools.

ROLE-BASED ACCESS CONTROL

Assign specific roles and permissions to perform certain operations based on those roles. For example, a security administrator could define roles and assign a different combination of permissions to each role. Each user is given a role which defines his permissions accordingly.

INTRUSION DETECTION SYSTEM

Automatically monitor events in your control system, looking for activities that are potentially malicious or violate established security policies. The ACE3600 RTU will react in real-time to block that activity, while allowing legitimate traffic to occur. Unauthorized activity is logged and can be reported to a designated control center.

APPLICATION CONTROL SOFTWARE (WHITELISTING)

Block unauthorized applications and code from running on your RTUs in the field by allowing only pre-identified programs to run. The ACE3600 RTU or IP Gateway includes application control mechanisms that are tested with McAfee™ Solidifier.

ENCRYPTION

Make data unreadable except with a device that has a specific key to decrypt it. Prevent eavesdropping or spoofing where a person/program masquerades as another to gain illegal access and encrypt data stored in devices and applications to prevent attacks with the FIPS-140-2 certified, 256 bit AES (Advanced Encryption Standard) algorithm.

AUDITING

Monitor processing in each device and log any suspicious activity or deviations from policy. Any attempt of unauthorized access to a secure ACE3600 RTU will be blocked and logged in its internal security log. Based upon the severity, it can trigger an alarm to alert designated personnel. The security log is encrypted and saved in FLASH memory to prevent malicious alteration and can be retrieved for forensic purposes after the event.

UNUSED PORT DEACTIVATION

Communication in ports not in use can be prime targets for unauthorized access. The ACE3600 RTU enables unused ports to be disabled, reducing its vulnerability.

TIME-WINDOW COMMANDS

Add another layer of defense to limit the risk of replay attacks or other malicious activities, such as a disgruntled employee who has legitimate access. For critical control, a time stamp can be added to the command message. A subsequent "action" message must be received within a designated time window and contain elements that match those in the notification message or the action will be rejected.

SECURED PROGRAMMING

Eliminate vulnerabilities from common programming errors. By identifying insecure coding practices and developing secure alternatives, you can reduce or eliminate vulnerabilities before deployment.

Motorola Solutions implements extensive secured programming in our software development processes, including techniques such as code obscurification to disable reverse code engineering or eliminate encryption of data related to debugging and testing.

SAFEGUARD YOUR INDUSTRIAL IOT WITH TRUSTED EXPERTISE

MOTOROLA SOLUTIONS CYBERSECURITY SERVICES

Motorola Solutions helps customers worldwide with a proactive approach to address constantly-evolving cyber security threats and manage the complexity of regulatory standards, specified Information Assurance and IT security requirements. We can help your company achieve acceptable compliance levels and keep your networks fully operational.

As a global leader and innovator of mission-critical communication networks for over 85 years, we offer unmatched expertise and support for protecting your radio systems and enterprise networks. Our certified, security professionals stay actively informed of the rapidly-changing landscape of security threats and compliance technologies.

RELY ON OUR EXPERTISE TO HELP PROTECT YOUR OPERATIONS FROM DEVICES IN THE FIELD TO THE SERVERS IN THE CONTROL ROOM – AND THE NETWORKS THAT CONNECT THEM ALL TOGETHER.

SECURITY UPDATE SERVICE (SUS)

Pre-tested anti-malware definitions and applicable security patches for your ASTRO 25 system ensures operations are not disrupted when updates are installed onto your system. Choose from two delivery options:

- Self Installed Security Patches
- Remote Security Patch Installation

SECURITY MONITORING

A comprehensive methodology for monitoring your system for potential intrusions and detecting malicious outbreaks from external and internal vectors. Choose from two delivery options:

- Remote Monitoring from our Security Operations Center (SOC)
- On-Premise Security Monitoring

CYBERSECURITY PROFESSIONAL SERVICES

A comprehensive process for identifying, assessing and managing cybersecurity risk throughout your systems. Choose from two delivery options:

- Assessment Conducted By Our Cybersecurity Experts
- Joint Engagement with your IT Personnel

SOURCES

1. 2015 OAS Micro Trends Report on Cybersecurity and CIP in Americas
2. "Attacks against industrial control systems doubled last year," CSO Online, April 17, 2015
3. Raising the Bar for Cybersecurity, James Lewis, February 12, 2013
4. 2015 ISACA Global Cybersecurity Status Report

To learn more about Motorola's Cybersecurity Solutions for Industrial IoT, visit **motorolasolutions.com/industrialiot**.

Motorola Solutions, Inc. 1301 East Algonquin Road Schaumburg, Illinois 60196, U.S.A. 800-367-2346 **motorolasolutions.com**

MOTOROLA SOLUTIONS