SECURE AND FUTURE-READY SCADA CONTROL SYSTEMS

PREPARE YOUR CRITICAL INFRASTRUCTURE FOR WHAT HAPPENS NEXT

SCADA CONTROL SYSTEMS
YOUR FIRST LINE OF DEFENSE

SCADA systems control most of the vital infrastructure in key industrial and energy sectors including electric, oil and gas, water, transportation, manufacturing. They're your first line of defense against infrastructure failure. What happens if those defenses are compromised?

Failure could cost you money... disrupt or cripple operations... and potentially impact the health, security and economic well-being of the people who depend on you. Future events are unpredictable, but there's one thing you can be sure of – your systems will be tested. Only the most adaptable and robust equipment will see you through.

You can count on Motorola SCADA products for the security, flexibility and resilience you'll need to maintain control of your critical infrastructure in a risky world.

THE SCADA ENVIRONMENT IS CHANGING ARE YOUR SYSTEMS READY?

SCADA (Supervisory Control And Data Acquisition) systems play a vital role for utilities, enterprises and public agencies. They help improve service reliability, increase production efficiencies, reduce costs and minimize losses. However, yesterday's systems are frequently ill-equipped for today's challenges.

THE RISK OF CYBER ATTACK IS ESCALATING

Your infrastructure and control systems could be targeted by hackers or terrorists, making your SCADA systems vulnerable to enormous potential damage including:

- Malfunction of critical infrastructure
- Lack of system availability
- Damage to equipment
- Data loss
- Personal safety issues
- Revenue loss
- Penalties and legal action

Do your SCADA systems support the latest security practices to keep your systems safe from attack?

SYSTEMS ARE MORE COMPLEX – The facilities you maintain and the processes they perform are growing more sophisticated. Can your SCADA system keep up with demand for more data, more detailed analysis and integration with more advanced equipment?

REGULATIONS AND STANDARDS ARE IN FLUX – National, state and local regulations are changing, not always predictably, particularly in the area of cybersecurity. Will your SCADA system require modifications or even replacement to comply with upcoming standards?

YOU HAVE NEW OPTIONS FOR CONNECTIVITY – Wired or wireless, the networks that tie SCADA systems together are evolving rapidly. Will you have the freedom to make the best price/performance choice both now and into the future, or will compatibility problems prevent you from taking full advantage of emerging technology?

THE RISK IS INCREASING

Attacks on critical infrastructure around the world are growing quickly. The number of detected global vulnerabilities has increased by 20 times since 2010; in 2012, the number of security flaws found was far larger than those discovered during the whole previous period starting from 2005.[1]

A string of government reports detail the growing concerns of a cyber attack on critical US energy infrastructure. A June 2010 Government Accountability Office (GAO) report revealed that federal agencies cited an increase of more than 400% in the number of incidents reported to US-CERT compared to 2006.[2]

The ICS-CERT 2010 Year-in-Review reported that the number of cyber incidents in 2011 was up over 200% from 2010 and the vulnerability analysis and coordination rose a staggering 600%.[3]

The April 2012 GAO report, "Cybersecurity Threats impacting the Nation," noted that over the past six years, the number of incidents reported by federal agencies to the federal information security incident center (US-CERT) has increased by nearly 680%.[4]

STEP INTO THE FUTURE
WITH MOTOROLA SCADA

Whatever the age of your current SCADA systems, the equipment you choose going forward should be a bridge to tomorrow. Our products integrate seamlessly and cost-effectively with your existing systems. At the same time, they position you to leverage modern technology and mitigate tomorrow's risks. Secure and adaptable, these products will help you prepare your SCADA systems for what happens next.

- **ACE3600 RTU** and gateway products offer maximum flexibility and state-of-the-art security features so your investment will stand the test of time
- **MOSCAD-M** products are suitable for applications that require low-cost, low-power hardware
- **System Tool Suite (STS)** software makes it easy to manage field equipment and supports the full range of ACE3600 advanced security features

ACE3600
REMOTE TERMINAL UNIT (RTU)

RTUs deployed in the field collect data, execute local control and communicate with a SCADA control system. Motorola designed the ACE3600 RTU to support the most demanding applications while minimizing costs. For your most critical applications, it can be configured with a redundant CPU, power supply and battery backup for continued reliability in the event of equipment failure or power outage.

Modular design allows you to customize the ACE3600 to fit your specific needs. You can start small and grow, confident that the powerful processor can handle complex applications as your needs evolve.

VERSATILE CONNECTIVITY – You want every opportunity to save money and optimize performance. That's why we designed the ACE3600 RTU to use a variety of digital and analog interfaces so you are never locked into proprietary solutions?

- Connectivity options include conventional radio, digital MOTOTRBO radio, analog/digital trunking radio, MAS, TETRA, P25 , third party radios, cellular, fiber optics, dial-up, microwave, serial links and LAN connections
- Each RTU can easily and simultaneously communicate with other RTUs and to multiple control centers, sensors, intelligent electronic devices (IEDs) and programmable logic controllers (PLCs)
- RTUs can connect to SCADA control computer(s) using a variety of standard methods including MODBUS protocol, specialized drivers or M-OPC. The RTUs can use Modbus, DNP 3, and IEC60870-5-101 to communicate with intelligent devices.
- Every RTU in your network can act as a communication node and/or a store and forward data repeater to extend radio frequency coverage and save you the much higher cost of a dedicated repeater
- Each CPU module supports simultaneous communications on up to seven ports, including Ethernet, serial, radio modem and USB
- 24 different types of I/O modules are available, and each RTU has capacity for up to 110 modules, giving you great flexibility to configure large or small sites compactly and cost-effectively

PROCESSING POWER – You need your SCADA network to have the capacity to support sophisticated technology. That's why, at the heart of an ACE3600 RTU, you'll find a powerful CPU and substantial memory to perform complex tasks. Plus, you can add plug-in SRAM to expand storage capacity.

- The RTU provides local computing power to collect and analyze data from IEDs and other sources, performs local control as required and then presents consolidated data to your SCADA control center
- A 32-bit processor, running at 200 MHz, delivers very high performance, while the substantial Flash and DRAM memory capacity provides plenty of storage for alarms, events, live data, historical reports and files
- Both polling and event-based reporting are supported, peer-to-peer or RTU-to-host
- Remote maintenance allows administrators to efficiently and securely update configuration, application and control parameters; and make safe firmware upgrades

SECURITY ENHANCEMENTS – Now you can apply the same state-of-the-art security features that Motorola provides for military and critical enterprise networks to your SCADA systems. The ACE3600 supports a full range of best-practice security options including:

Security Policy Enforcement – Define and install a single, coherent, system-wide set of security configurations in every RTU.

Built-In Firewall – Filter IP communications by port, direction, protocol and IP address.

Access Control – User authentication tools, executed at the RTU or at the system server, verify specific user access and determine if use is legitimate and allowed.

Role-Based Access Control – The system administrator defines job roles and assigns different permissions so that each user is authorized to access only the parts of the system required for his or her job.

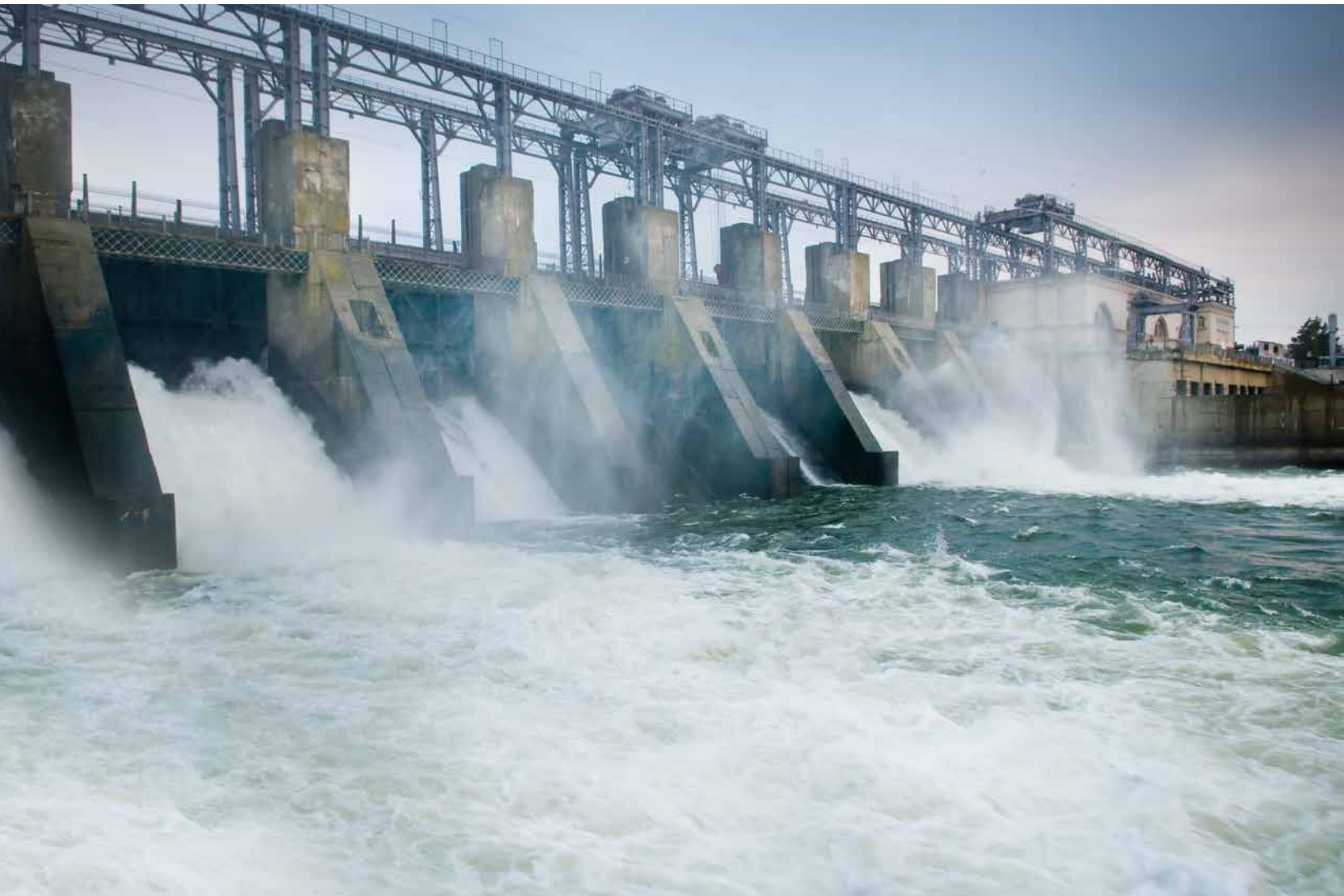
Intrusion Detection System – While allowing legitimate traffic, the ACE3600 identifies unauthorized access activities like an attempt to alter an RTU program or drop unauthorized data packets. It blocks these activities, logs the events and sends a report to the system administrator.

Application Control Software – Also known as "white listing," this software blocks unauthorized applications and code on PCs and RTUs. ACE3600 firmware protects user programs with this technique, and ACE3600 configuration management tools on PCs are protected with McAfee™ Solidifier.

Encryption – An algorithm makes data readable only by a device with a specific key to decrypt the message. Data stored within the ACE3600 is also encrypted using a 256-bit AES (Advanced Encryption Standard), meeting FIPS-140-2 Level 1 requirements.

Unused Port Deactivation – Disable communication for any ports that are unused, closing a point of access that could be exploited by attackers.

Time-Window Commands – When an application generates a command, it assigns a time window; after the time expires, system components will not execute the command. This can prevent replicating errors and commands of questionable origin from affecting the network.



MOTOROLA ACE3600
IP GATEWAY FEP

This gateway is a powerful and flexible option to facilitate network connections; it serves as front-end processor to interface between your RTUs and SCADA control center computer(s). Based on the same expandable, modular and secure hardware as the ACE3600 RTU, its enhanced software enables:

- Seamless connection between the Motorola Data Link Communication (MDLC) protocol and standard TCP/IP
- Instant access to all RTUs in the network, so the control center can collect real-time field data and manage the remote sites
- Client/server architecture to efficiently distribute data among multiple clients, control centers and RTUs
- Easy integration of the SCADA software using an API that works with virtually any master control center that uses an industry-standard operating system
- Redundant configurations for network survivability
- Security features including MDLC encryption, IP firewall and dynamic IP conversion table updates

MOSCAD-M RTU
FOR SPECIAL APPLICATIONS

This compact RTU has extensive power management features, making it particularly suitable for SCADA systems where low-power consumption is essential. “Sleep mode” operation allows the use of smaller and less expensive solar panels and batteries than the ACE3600. The MOSCAD-M is a low-cost option for monitoring and control in remote applications:

- Flood and warning systems
- Oil and gas leak detection
- Environmental and weather systems
- Detecting environmental pollution, chemical spill or radiation emission

SYSTEM TOOL SUITE
MODERN PROGRAMMING TOOL

Motorola System Tool Suite (STS) software reduces the cost and inconvenience of managing remote SCADA equipment. Administrators can configure, set up, program, debug and maintain the entire network, all through a graphic user interface.

- Protect your SCADA systems from unauthorized access using the latest security measures for access control, data encryption and authorization
- Write custom applications easily using the C language or a ladder diagram platform for development and debugging. You can also use industry standard packages such as IEC 61131 or 61850.
- Get a comprehensive, graphic view of the entire SCADA network, system sites and equipment. Extensive design and editing features make it simple to design and manage a large system.
- Save password-protected configurations and applications for RTUs, ports and I/O modules for later re-use so you can quickly reconfigure the network as events warrant

MOTOROLA SCADA SYSTEMS IN ACTION

AROUND THE WORLD IN MANY APPLICATIONS AND INDUSTRIES, THOUSANDS OF MOTOROLA SCADA SYSTEMS ARE ON THE JOB RIGHT NOW

SMART GRID

Electric utilities are modernizing their distribution grids to achieve greater supply reliability and to cut operating and maintenance costs. Motorola ACE3600 RTUs provide computerized remote control at medium-voltage substations and elsewhere on the grid.

Using reliable wireless links, RTUs connected to a variety of intelligent electronic devices – capacitor bank controllers, transducer-less AC measurement units, fault passage detection units and more – transfer information throughout the grid. Our RTU supports industry-standard interfaces, including MODBUS, DNP3.0 and IEC60870-5-101, giving utilities a wide choice of IED vendors and products.

OIL AND GAS

Oil and gas operations require remote control for production wellheads, long pipelines and valves located in difficult-to-access locations. The strictest safety measures are required to prevent and detect leaks and fires. That's why so many operators depend on Motorola RTUs to supervise remote sites.

ACE3600 RTUs can be used for the many gas installations that require flow calculations required by AGA (American Gas Association) standards such as AGA-3, AGA- 7 and AGA-8. RTUs along oil pipelines perform pressure monitoring and control using PID (Proportional-Integral- Derivative) based control routines, and control cathodic protection rectifiers and other industry equipment. We offer models certified to Factory Mutual Class 1, Division 2 standards for safe operation in potentially hazardous areas.

WATER AND WASTEWATER

Motorola ACE3600 systems perform continuous monitoring and control of water facilities, providing immediate problem detection and resolution. Well pumping can be automatically adjusted via water quality or energy costs. Reservoir volumes and system pressures are regulated to maximize the efficiency of the delivery system. RTUs alert operators to line breaks, equipment failures and possible unauthorized water use.

Motorola RTUs are routinely used to monitor and control the collection of waste water delivered to treatment facilities. They implement sophisticated pump sequencing operations to ensure the appropriate, most cost-effective pump is operating. The RTUs can interface directly to intelligent flow meters, and their large data storage capacity allows them to log data where few communication options exist such as combined sewer overflow (CSO) monitoring.

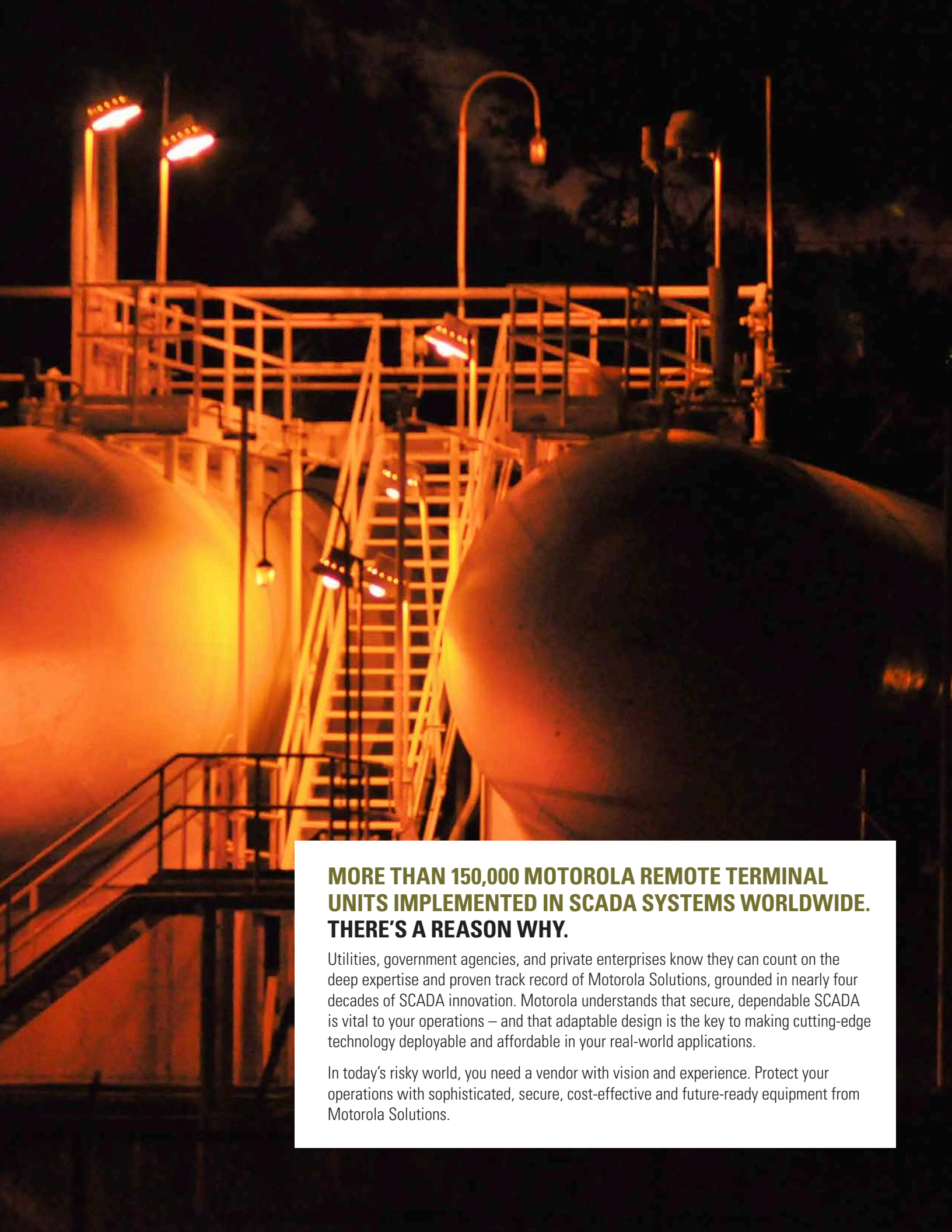
EARLY WARNING SYSTEMS

Our siren warning systems deliver critical messages to small and large municipal populations as well as nuclear power facilities, refineries and chemical plants. Motorola RTUs can be integrated with a range of siren equipment to enable many activation options. Secure and encrypted communications minimize the possibility of false alarms or system intrusion. The system supports combinations of tones or pre-recorded voice messages. It supports multiple control centers and offers flexible functions such as siren activation in selected groups, backup control, silent test, download of pre-recorded public warning messages, and redundancy. ACE3600 siren-based systems are certified for P25 or TETRA infrastructures.

PUBLIC SAFETY AND FIRE STATION ALERTING

Motorola Fire Station Alerting systems alert first responders with a tone, followed by an incident-specific voice message to help dispatch the appropriate apparatus and personnel as quickly as possible. When station RTUs receive an alert, they can automatically turn on lights, connect the voice dispatch message to specific areas in the station, open the station doors, identify the vehicles assigned to the task, turn off kitchen appliances, send a message to dispatch when all vehicles have left the station, and finally close the station doors.

Fire Station Alerting integrates with Computer Aided Dispatch (CAD) for easy selection of regional fire station(s), activation of vehicles in those locations, voice dispatch capability and redundant two-way communications.



MORE THAN 150,000 MOTOROLA REMOTE TERMINAL UNITS IMPLEMENTED IN SCADA SYSTEMS WORLDWIDE. THERE'S A REASON WHY.

Utilities, government agencies, and private enterprises know they can count on the deep expertise and proven track record of Motorola Solutions, grounded in nearly four decades of SCADA innovation. Motorola understands that secure, dependable SCADA is vital to your operations – and that adaptable design is the key to making cutting-edge technology deployable and affordable in your real-world applications.

In today's risky world, you need a vendor with vision and experience. Protect your operations with sophisticated, secure, cost-effective and future-ready equipment from Motorola Solutions.

SOURCES

1. Positron Technologies, SCADA Safety in Numbers v1.1, 2012
2. Cybersecurity: Continued Attention is Needed to Protect Federal Information Systems from Evolving Threats, GAO, June 2010, page 3
3. CSSP Year in Review: FY 2011, DHS, January 2011, page 6
4. Cybersecurity: Threats Impacting the Nation, GAO, Testimony before the Subcommittee on Oversight, Investigations, and Management, Committee on Homeland Security, House of Representatives, April 24, 2012

To learn more about how Motorola SCADA systems can provide the security, flexibility and resilience you need to control your critical infrastructure, contact your Motorola representative or visit **motorolasolutions.com/scada.**

MOTOROLA