

Overview: ALSTOM's Energy Management & Markets (EMM)* Business announces Security ServicesSM, a new suite of service offerings designed to ensure a secure energy infrastructure environment including defense against cyberterrorists, failproof backup systems and emergency procedures, as well as emergency backup and disaster recovery facilities. Implemented using state-of-the art audits, assessments, and alliances with knowledgeable security providers, Security Services enable energy industry customers to be fully knowledgeable of threats to their infrastructure and are offered a collection of services and capabilities to sustain and strengthen their current energy infrastructure security capabilities.

Why Partner with ALSTOM for Security Services?

Selecting ALSTOM EMM as an energy infrastructure security services partner makes sense. ALSTOM has...

- Strong knowledge of the energy industry - especially in the area of real-time energy network and market operations
- Extensive network of security providers in our own group of alliances who can be called to serve you - our customer
- Heightened customer focus, including customized services for individual customer needs

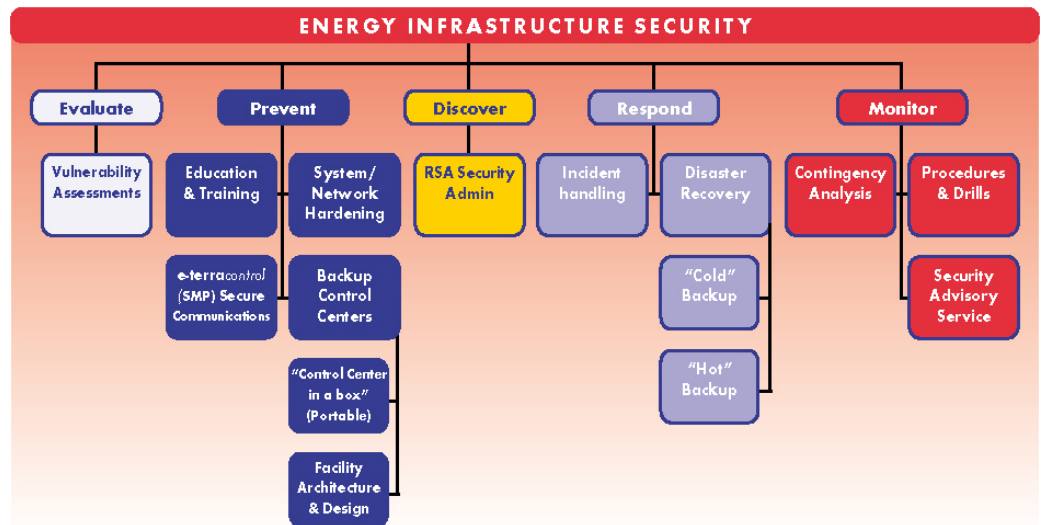
ALSTOM Profile

ALSTOM EMM is the leading Energy Management System (EMS) vendor in North America. In this role, the company develops and designs EMS systems, real-time communications, emergency backup and fail-over strategies, energy market rules, operating protocols and procedures.

ALSTOM EMM is the leading control system vendor and is ideally placed to review control systems for Independent System Operators (ISOs), Transmission and Generation Companies (TRANSCOs and GENCOs), and energy control area operators.

ALSTOM EMM has a wealth of expertise in both the set up and design of control systems and their interfaces, as well as the communications networks required to keep operations functioning in times of emergency resulting from equipment failure, natural disaster, and terrorism.

With over 80% of control areas in North America as clients, ALSTOM EMM is able to cost-effectively provide security services and solutions to meet the current needs of energy providers and service organizations.



Five Steps to Energy Infrastructure Security

The security of your operations are very important to your customers and to the integrity of your systems. In the five "steps" below, ALSTOM EMM and its key alliance partners provides support to its clients including:

- Evaluate
- Prevent
- Discover
- Respond
- Monitor

EVALUATE: Vulnerability Assessments

In conjunction with other industry IT security experts, ALSTOM EMM offers a security assessment process and program that provides on-site assessment of EMS-related IT systems. ALSTOM EMM can access its pool of alliances in the energy infrastructure security space and provide physical asset security assessments as well.

These assessments focus on some of the following:

- Identifying the assets and processes at risk
- Examining desktop security practices, password processes, key security, etc.
- Identifying security impacts of operations, facility and human resource policies
- Using automated tools for technical vulnerability scans
- Evaluating risk of system virus attacks

The deliverables from these assessments include a prioritized list of those areas needing attention as well as recommendations for future changes to processes, procedures, hardware and software arrangements.

PREVENT: Education and Training Services

Security Services includes standard and customized training in the area of energy infrastructure security with emphasis on the Information Technology space. This training is jointly offered by ALSTOM EMM and its alliance of security experts. The classes can be conducted at the ALSTOM offices or at the customer's offices and sites.

The training is intended to educate the clients at all levels - from executive leadership to the network administrators to the software developers.

The training includes safe computing and physical security guidelines, identifying prevention techniques, and activities ranging from simple to complex, and provision of a general "check list" for the executive/network administrator/developer to follow when focused on energy IT security issues.

PREVENT: System and Network Hardening

As a follow up to the assessments provided, ALSTOM EMM offers a service that provides system and network hardening. This service includes an inventory of the appropriate EMS IT hardware, software and interfaces. This is followed by identifying and installing updates, removing every possible component not used in normal operation, changing system defaults (especially passwords and file permissions), installing security software and performing penetration tests.

As an added service, ALSTOM EMM in conjunction with an alliance partner, can identify and in most cases perform control room / control center facility hardening activities (e.g., physical security system upgrades, etc.).

PREVENT: e-terracontrol (SCADA Management Platform) Substation Communications and RTU Data Processing

Vital to the overall operation of the electric network is the ability to "see" status of switches, breakers, transformers, substations, etc. from the control center. Unfortunately, due to the older SCADA communications technology, the raw data is sent from the infrastructure and is processed in the control center. Therefore, destruction of the stand-alone control center itself can result in "blind" operations which can be taken advantage of by terrorists.

For a reliable solution to this security concern, ALSTOM EMM offers its *e-terracontrol* [often referred to as SCADA Management Platform (SMP)]. Installing this simple but reliable data processing unit at the substation or infrastructure facility away from the control center, clients can be assured of reliable, *processed* data from the substations.

This data can also be directed to other facilities besides the control center such as other back up control facilities, emergency centers, or even to the Internet and wide area network for monitoring and executive oversight.

PREVENT: Backup Control Centers

The Security Services portfolio includes in-depth expertise on the design, architecture, installation, and testing backup control centers for primary facilities. ALSTOM EMM's experience includes installing the backup facilities with high-reliability failover capabilities for EMS systems as well as Market Operations Systems (MOS) where faulty operation can result in outages and losses of significant amounts of money.

The backup capability can range from elementary backup capabilities at a remote substation or other utility facility, all the way up to and including the design, architecture, construction, installation, testing and even full time operation – including staffing – of a Backup Control Center.

ALSTOM EMM can also design, deliver and operate a trailer-mounted "Control Center in a Box" to provide a mobile backup control center capability.

By discussing the individual needs and ideas of each client, ALSTOM EMM and the ALSTOM family of companies and alliance partners can provide a customized, reliable, effective and secure Backup Control Center.

DISCOVER: Monitoring and Detection Services

Security Services offers intrusion detection services as part of its portfolio. This service – offered in conjunction with Remote Site Administration (RSA) services, also offered by ALSTOM EMM – includes installation of network intrusion detection software. In addition to the software, the service includes network log reviews to look for intrusions and unauthorized "sniffing" as well as a process to send an alarm to ALSTOM EMM staff when a network intrusion is detected or unauthorized network access is identified.

RESPOND: Incident Handling

A responsive and effective security plan includes learning from the security incidents that occur and then revising or adding to the current policies and procedures to prevent this incident from recurring. ALSTOM, in conjunction with its world-class partners and alliances, can help answer questions such as "Exactly what happened?" "How did this occur?" "What do we need to do to prevent this in the future?" In a sense, one needs to stop the attack, learn from the attack, remove the virus or Trojan Horse, etc. from the system, repair the system, and ultimately ensure an effective reaction to the incident.

RESPOND: Disaster Recovery

The two primary features of a successful disaster recovery plan include 1) keeping an off-site copy of all critical data and 2) having access to a data center where the data restoration, configuration of network connections, and restoration of the IT infrastructure can occur with minimal downtime following a catastrophic event such as a natural disaster or terrorist attack.

For most energy providers, all active data should be backed up to a remote hot site, which has the capability to run all the applications generally found in the control center.

ALSTOM EMM provides these services. For example, disaster recovery services includes periodic data collection and secure storage away from the control center proper.

A "cold backup" capability is also provided, where servers are set up at ALSTOM EMM's secure application service provider – Qwest – to be brought on line in a few days following a catastrophic event at the control centers.

ALSTOM EMM's premier disaster recovery capability includes a "mirrored" facility – also at Qwest – which includes servers, EMS and MOS applications, and systematically backed-up data on a "hot site." In this case, the data can be encrypted and sent over the Internet to the "hot boxes."

The "hot" and "cold" disaster recovery facilities can be set up as redundant operations with automatic failover capabilities.

MONITOR: Contingency Analysis

Using ALSTOM EMM products – such as grid network analysis tools and the Dispatcher Training System (DTS), detailed contingencies for the client's network can be developed covering a range of feasible and extremely remote events. ALSTOM EMM has expertise in the development of realistic scenarios as well as the systems to run these contingency analyses. These analysis tools can be run for clients to provide vulnerability analysis of key equipment and energy infrastructure (i.e., substations, etc.).

MONITOR: Procedures and Drills

ALSTOM EMM and its alliance partners can develop and/or consult on preparation of detailed operating and emergency procedures for control centers and other energy operations facilities. These procedures are developed with the clients planners and system operators to ensure accuracy, completeness, understanding, and most importantly, "ownership" by the operators. These procedures will be developed using appropriate human- factors authoring techniques and will be validated either through actual use on a simulator or walk-through with the operating crews.

Besides developing the procedures for use, it is imperative that practice casualty and failover drills be held and closely monitored to ensure that the crews know their roles in the event of a major catastrophe. These drills also ensure that the switches, equipment, and software are functioning properly and continue to be valid as systems are upgraded and changed. ALSTOM EMM offers independent service to not only assist with these drills but also to provide detailed critique of the drill results and specific recommendations for client improvements and enhancements to the crew's performance, procedures and/or equipment.

MONITOR: Security Information Clearinghouse

ALSTOM EMM has developed a deep and substantial collection of alliance partners who work to provide effective, vigilant, and reliable security solutions to the clients energy infrastructure. Requests for assistance can be handled not only by ALSTOM EMM and the ALSTOM family of companies, but also solved in partnership with our highly capable and expert partners.

ALSTOM EMM is actively developing new security partners every day. Areas where ALSTOM EMM has access to expert solutions include:

- IT security – assessment, detection, prevention, response, and awareness
- Physical plant security – including vulnerability assessments, remote monitoring
- Biometrics
- Visualization techniques
- Emergency equipment replacement

MONITOR: Security Advisory Service

ALSTOM EMM offers its clients a security advisory and consulting service using its top echelon staff of IT security experts in conjunction with its security service alliance partners.

This service includes:

- A fixed number of hours of advisory response to IT security questions – essentially a retainer - this is provided on a Time and Materials Basis.
- A monthly electronic newsletter identifying news items of interest regarding energy infrastructure security, IT security issues, etc.

*ALSTOM Energy Management & Markets (EMM) is comprised of USA-based ALSTOM ESCA Corporation in Bellevue, Washington, and ALSTOM EMM Massy near Paris, France.

ALSTOM ESCA Corporation is certified by Underwriters Laboratories, Inc.® to the International Organization for Standardization ISO 9000 Series Standards for Quality.

ALSTOM EMM Massy has obtained an ISO 9001 certification for its activities: "Engineering and integration of management and telecommunication system for electrical networks."



ISO 9001: 1994
A3991



Copyright ©2002 by ALSTOM ESCA Corporation. All rights reserved.

The information in this document is subject to change without notice.

ESCA and HABITAT are registered trademarks. The e-terra family of products and services are trademarks and/or service marks of ALSTOM ESCA Corporation.

Other product and company names in these materials may be trademarks or registered trademarks of other companies, and are the property of their respective owners. They are used only for explanation and to the respective owner's benefit, without intent to infringe.

security_03'02

ALSTOM

ALSTOM T&D Energy Management & Markets

www.tde.alstom.com

11120 NE 33rd Place • Bellevue, WA USA 98004 • +1 425 822 6800

ALSTOM EMM AMERICA ALSTOM EMM BRAZIL ALSTOM EMM EUROPE ALSTOM EMM INDIA