Certification Services: Built-In Security

exida, a leader in functional safety certification, is successfully applying proven tools and methodologies from the more mature functional safety certification program to independently verify a product's security protection. The result is Integrity Certification™, the only product certification that evaluates safety, security and reliability. Integrity Certification provides control system engineers with third-party validation and helps reduce the complexity of product selection and deployment. For equipment manufacturers, Integrity Certification provides a way to demonstrate that their product meets or exceeds their customers' safety, security and reliability requirements. It also represents an important opportunity for competitive differentiation.

Security Certification Process

exida's security certification process combines control system testing with formal, rigorous assessment criteria based on internationally accepted standards and processes. Embedded in the certification process is the system development perspective gained from the prior experiences of many of exida's employees. This means the certification process balances the highest standards of security verification with sensitivity to time-to-market and implementation costs. exida also leverages this experience to offer design consultation assistance prior to the certification process to help orient a manufacturer going through the process for the first time.

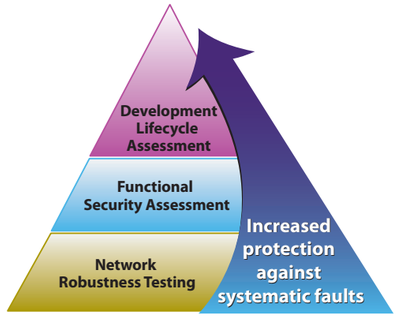
Comprehensive Security Product Certification

exida supports a comprehensive, three-tier approach to security certification that emulates other well-established product safety certification programs. It starts with a strong foundation of network stack robustness testing and layers in functional security assessment and development lifecycle assessment.

Network Robustness Testing Network Robustness Testing is based on Wurldtech's industry-leading Achilles Certification Program. Achilles Level I Certification identifies vulnerabilities in Ethernet enabled industrial components; assuring the security, reliability, and robustness of an implementation of OSI layers 2 through 4, including Ethernet, ARP, IP, ICMP, TCP and UDP. A component must pass each of the over 30 million individual tests to achieve Achilles Level I Certification with Pass/Fail criteria being specified in terms of key component functionalities such as continuity of process control.

A Functional Security Assessment detects errors or omissions in the security functionality of a product when audited against requirements for its target security level.

A Development Lifecycle Assessment detects and avoids systematic design faults. The vendor's software development and maintenance processes are audited against the security equivalent of IEC 61508, ensuring the organization follows a robust software development process.



Three-tier Approach to Security Certification

Functional Safety Services: Intersection between Safety and Security

Recognizing that weaknesses in control system safety and security can have similar consequences, exida gives plant operators a more efficient and more effective option for proactively avoiding unplanned incidents. As the only firm to offer consulting and certification services across both security and safety, exida provides a single expert resource for control system safety and security. For plant operators, this not only provides efficiencies in time and cost, it also ensures lower risk and higher availability solutions.

For equipment manufacturers, this means products can meet customer requirements for both security and safety while carrying the credibility and differentiation of Integrity Certification™, the only certification available for safety, security and reliability. In addition, exida works with you to minimize the impact certification can have on development costs and time-to-market. Many exida employees have prior system development experience, ensuring you have a partner who understands your needs and processes as an equipment manufacturer, as well as your customers' requirements.

Professional Services for Control System Security

exida for Control System Security

Protecting critical industrial processes from attack has become a growing priority for many companies. Power plants, refineries, chemical plants, and other industrial facilities have become more vulnerable as proprietary systems have evolved to open systems. Heavy use of commercial technologies, such as Windows, SQL and Ethernet, leaves control systems vulnerable to the same viruses, worms and trojans that impact office environments, and increasing remote and 24/7 system access translates to more connections. With both the number and the seriousness of security incidents on the rise, plant operators face increasing pressures to develop security programs for their plant, and equipment manufacturers need to meet growing customer demand for products that are "secure-by-design."

Supporting Equipment Manufacturers with Built-in Security

exida helps equipment manufacturers deliver intrinsically secure products through well-proven certification services, as well as design consulting services grounded in the system development experience of many exida employees. This experience means you get a partner who understands system development processes, the pressure to meet customer requirements within time-to-market schedules, and the opportunity to differentiate a system's security measures.

Helping Plant Operators Avoid Risk

A proactive security program provides the best protection against an incident. Developing such a program, however, comes on top of the existing requirements for system availability and safety. With its heritage in helping plant operators ensure high availability and functional safety for critical processes, exida is uniquely qualified to help you understand security issues, assess your risk and vulnerabilities, and explore your options to mitigate risk.

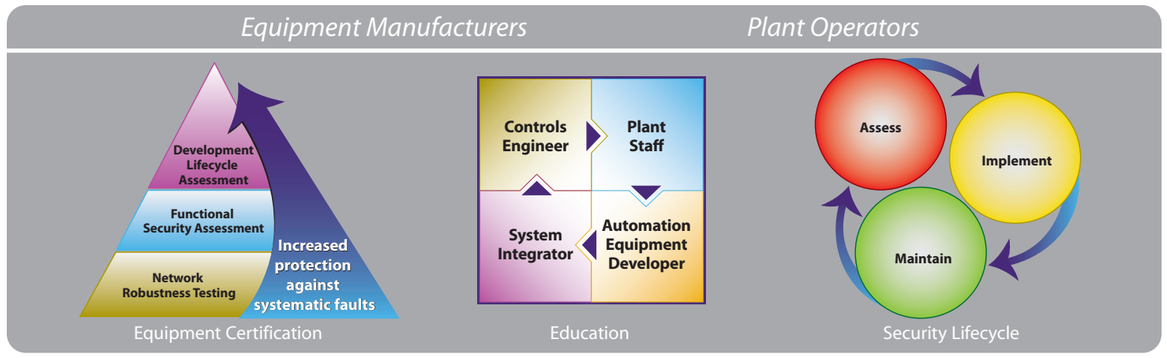
Security Breaches on the Rise

Not that long ago, the move towards "open systems" and the resulting incorporation of off-the-shelf technologies represented a huge step forward in control system design. System integration became easier, product development by manufacturers was accelerated, and training leveraged common tools and concepts. However, these "open systems" also opened control systems to security vulnerabilities for critical industrial processes.

While the off-the-shelf technologies now commonplace in control systems gain some security coverage with products like anti-virus software, the controllers and networks within those systems remain vulnerable. Here are some recent incidents that may have been avoided by implementing a proactive control system security strategy.[1]

- In March 2009, a Los Angeles federal grand jury indicted a disgruntled tech employee on allegations of temporarily disabling a computer system detecting pipeline leaks for three oil derricks off the Southern California Coast.
- A nuclear power plant in Georgia was forced into an emergency shutdown in March 2008 for 48 hours after a software patch was installed on a single computer.
- In 2008, a teenage boy hacked into a Polish tram system and used it like "a giant train set," causing chaos, derailing four vehicles, and injuring twelve people.
- A 2006 FBI report identified a foreign hacker penetrating security at a Harrisburg, Pennsylvania, water treatment plant, bringing the total recorded incidents against water systems to ten. An employee's laptop was compromised via the Internet and used as an entry point by hackers to access administrative systems and to install viruses and spyware.
- In 2004, the Sasser worm infected the distributed control system of a major chemical plant. The worm infection came through the firewall, causing loss of view and loss of control of the whole control system for the entire plant for over five hours.

[1]*Source: The Repository of Industrial Security Incidents database (www.securityincidents.org).*



Consulting Services: Expertise to Guide You

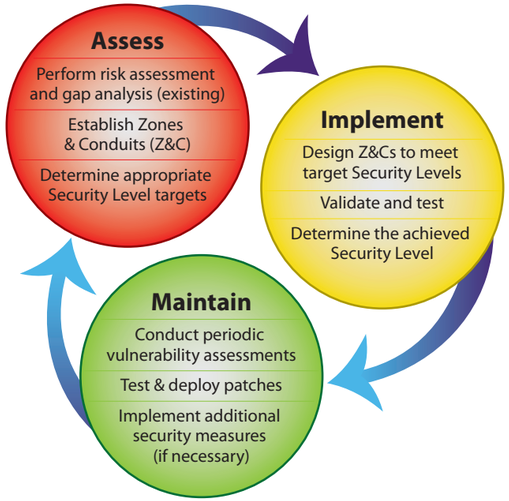
Control system security can be a complex additional requirement for many plant operators already faced with ensuring control system uptime and compliance with safety standards. exida recently acquired Byres Research to form a subsidiary dedicated to helping you understand your level of risk, proactively design appropriate control system architectures, comply with standards and regulations, and prepare for potential breaches.

Byres Research has been at the forefront of control system security since its emergence as a critical issue nearly a decade ago. Members of the Byres team have been responsible for numerous standards, best practices and innovations for control system security in industrial environments. They have provided security guidance to government security agencies and to major energy companies on cyber protection for critical infrastructures.

exida adds to this rich expertise a global service delivery capability and its own deep experience in control system availability and safety. Recognizing that weaknesses in control system safety and security expose similar consequences, the blending of these capabilities under exida gives plant operators a more efficient, more thorough option for proactively avoiding unplanned incidents.

The security life cycle, which in many ways resembles the safety life cycle, includes three main phases: Assess, Implement and Maintain.

- The **ASSESS** phase involves analyzing a new or existing design to determine the inherent risk in the system, to establish a Zone & Conduit (Z&C) model, and to establish security level targets for each Zone/Conduit.
- The **IMPLEMENT** phase involves designing and implementing the system architecture design as well as testing and validating that the design meets the security level targets established in the ASSESS phase.
- The **MAINTAIN** phase is focused on maintaining the security level targets through periodic vulnerability assessments and an effective patch management process.



Security Lifecycle

byres research inc
an exida company

Training: A Critical Foundation

Experience has shown that most companies benefit from training as the first step in implementing a security program. When you bring together the ever-changing landscape of automation technology with the inherently dynamic nature of security, embarking on a security program can seem complex and overwhelming. exida offers flexible training programs for all the stakeholders impacting system security, including plant operators, plant staff, automation equipment developers, and system integrators.

While plant operators face accountability for security, they rely on their equipment manufacturers and system integrators to deliver systems with security effectively built in. And once the system is in place, the plant staff needs to be prepared to add security to their list of priorities for productivity and safety. (Numerous security studies identify policy violations and social engineering, not malevolent intent, as significant contributing factors in most security breaches. Usually an employee or contractor did not understand the potential impact of his or her actions.)

exida is uniquely qualified to deliver training across all these stakeholders. For example:

exida adapts its training programs to meet your needs, with options for onsite classes, online courses, and programs at an exida location.

- Training materials developed by Byres Research formed the foundation for the ISA control system security training programs.
- exida instructors are active security professionals who participate in standards committees and provide professional security services, ensuring the training reflects the most current and pressing topics.
- exida's collective experience includes decades of control system development experience from many of its employees, providing a more relevant knowledgeable resource for equipment manufacturers and system integrators.

Standards Compliance and Regulatory Impact

The dramatic rise in incidents has created a sense of urgency in the development of industry standards and regulations addressing control system security. exida and its security consulting subsidiary, Byres Research, make it a priority to follow these developments very closely, including participating in standards committees and collaborating with government agencies. Being this steeped in current initiatives ensures expert guidance as you navigate emerging standards and regulations.

ISA99 The ISA99 committee Industrial Automation and Control System Security focuses on criteria and procedures for ensuring control system security. *Terminology, Concepts, and Models* (ISA99.01.01) provided an initial framework, and *Establishing an Industrial Automation and Control Systems Security Program* (ISA99.02.01) is currently with IEC65 WG10 for the IEC process. The ISA99 standards, along with the counterpart IEC 62443, form the most pervasive global guidelines for control system security.

NERC CIP Cyber security standards published by the North American Electric Reliability Council (NERC) ensure that all entities responsible for the reliability of the bulk electric systems in North America protect their critical cyber assets. Mandated in the U.S. by the Federal Energy Regulatory Commission (FERC), NERC CIP (Critical Infrastructure Protection) became effective 1 January 2007 and gives most entities until 31 Dec 2010 to be auditably compliant. The penalty for non-compliance can be up to US$1,000,000.

CFATS The Chemical Facility Anti-Terrorism Standards (CFATS) were issued by the U.S. Department of Homeland Security in April 2007 and require all chemical facilities to comply with regulatory requirements as detailed in 6CFR27 (CFATS). The process includes completing a screening process for potentially dangerous materials, identifying vulnerabilities through a security vulnerability assessment, and developing a site security plan.