SECURE-ICS
Secure Critical Infrastructure Environments

CGI
Experience the commitment®

BE IN CONTROL SECURING CRITICAL INFRASTRUCTURES

Anyone integrating automation technologies these days is well aware of the pressure on the operators of industrial plants to increase productivity, reduce costs and share information in real time across multiple industrial and enterprise systems. Adding to these business pressures is the growing fear of cyber attacks as the world has become aware that the Stuxnet worm was specifically designed to disrupt an industrial process. Operators and engineers are under pressure to isolate automation systems at the same time as management is asking for greater interconnectedness.

How can CGI help your company deal with the conflicting requirements of more integration and more isolation? The SECURE-ICS™ security approach addresses the concepts of the "zone and conduit" model included in the ISA-99 / IEC62443 security standards supported by a cyber security management framework for helping deal with network & systems security threats that arise from both the "push for productivity" and the fear of the next "Son-of-Stuxnet" worm, with a **clear step by step approach**.

The past two years have been a wakeup call for the industrial automation industry. It has been the target of sophisticated cyber attacks like Stuxnet, Night Dragon and Duqu. An unprecedented number of security vulnerabilities have been exposed in industrial control products and regulatory agencies are demanding compliance to complex and confusing regulations. Cyber security has quickly become a serious issue for professionals in the process and critical infrastructure industries.

If you are a CISO, manager security, security architect, process control engineer, IT professional in a company with an automation division or a business manager responsible for safety or security, you may be wondering how your organization can get moving on more robust cyber security practices in your process control networks / critical infrastructures.

Devices which are directly connected to physical equipment and are responsible for controlling and monitoring the safe operations of real-world processes are the devices which are most vulnerable.

BASELINE OF CGI'S APPROACH

The ISA 99 / IEC62443 standard was the first industrial control systems security standard that defined the concepts of zones, conduits, boundaries and security levels.

The ISA standard defines security zones as:

'…A logical grouping of physical, informational and application assets sharing common security requirements.

This concept applies to the electronic environment where some systems are included in the security zone and all others are outside the zone.

There can also be zones within zones, or sub-zones, which provide layered security, giving defence-in-depth and addressing multiple levels of security requirements.

Defence-in-depth can also be accomplished by assigning different properties to security zones.'

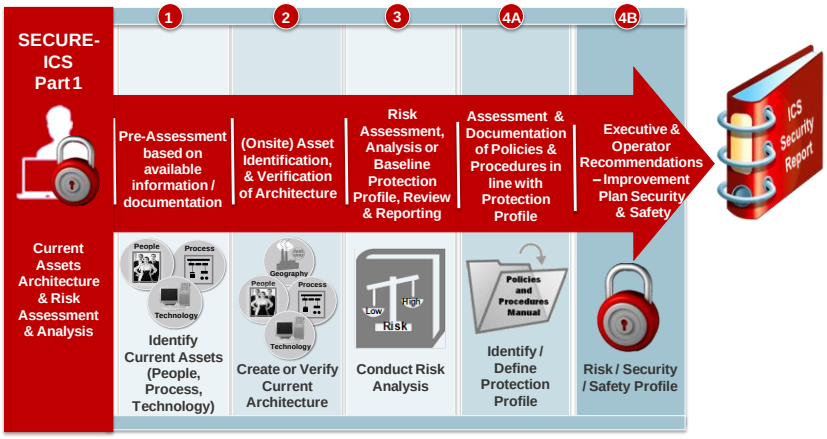
Why CGI?

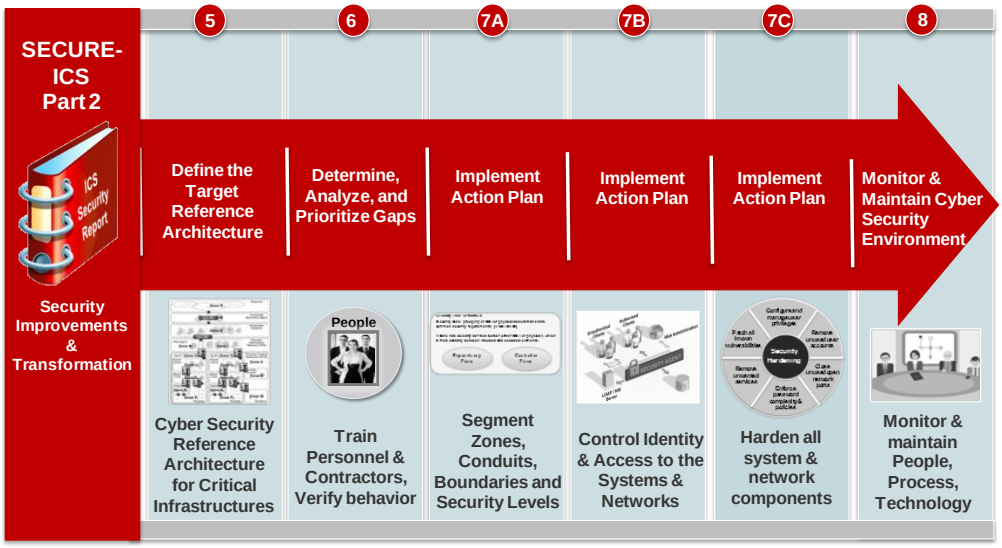
CGI's approach is based on material from numerous industry standards and best practice documents including the new USA NIST Cyber Security Framework, combined with our experiences in assessing / securing the security of industrial automation and control systems environments / critical infrastructures.

The result is an easy-to-follow 8-step process:

- Step 1 – Identify Current Assets (People, Process, Technology)
- Step 2 – Create or Verify Current Architecture
- Step 3 – Conduct a Risk (Self) Assessment
- Step 4A – Identify / Define Protection Profile
- Step 4B – Risk / Security / Safety Recommendations
- Step 5 – Define the Target Reference Architecture
- Step 6 – Determine, Analyze and Prioritize Gaps
- Step 7A – Implement Action Plan: Security Zones & Conduits
- Step 7B – Implement Action Plan: Identity Access Management
- Step 7C – Implement Action Plan: Harden All Components
- Step 8 – Monitor & Maintain System Security

The steps above are incorporated in CGI's overall Cyber Security Management Framework (CSMF) divided in the following phases: **Plan**/Identify; **Do**/Protect – Detect; **Check**/Respond; **Act**/Recover.





About CGI

CGI is a leading business and technology services company focused on helping clients achieve results.

Since our founding in 1976, we've operated upon the principles of sharing in clients' challenges and delivering quality services to address them.

With 68,000 professionals in more than 40 countries, we have the presence, expertise and complete IT services to meet clients' business needs anywhere, anytime.

We provide the responsiveness and accountability of a true local partner while offering the global scale, talent and services needed to meet your evolving needs.

For more information about CGI's Cyber Security Services & Solutions please contact your local CGI representative or visit www.cgi.com/cyber or email us at info@cgi.com.

Can you afford to wait? Eliminate the risk. Contact us.

cgi.com