

Critical Infrastructure Protection (CIP) – what does it mean and why Dessau is the industry leader

What we mean by Critical Infrastructure (CI)

The Canadian definition of CI includes ten sectors¹:

1. Energy and Utilities
2. Communications and Information Technology (IT)
3. Finance
4. Health Care
5. Food
6. Water
7. Transportation
8. Safety
9. Government
10. Manufacturing

Where Dessau Fits In

With the exception of Finance, Health Care, and Food, Dessau Engineering and Construction is a leader in all the other sectors both in Canada and Internationally (Africa, Central and South America). Dessau plans, designs, builds and manages infrastructures for clients in both the private and public sectors, covering 70% of the critical sectors identified by Public Safety Canada. The company is singularly well placed to pinpoint the weaknesses in all these systems that potential enemies might try to exploit. Furthermore, Dessau has the skilled staff and expertise to install countermeasures to ward off such exploitation, particularly in the fields of utilities (hydro, nuclear), IT, transportation, and water.

Pervasive to all ten sectors is the Cyber Security aspect which is a feature of the connectivity necessary for each sector to function effectively in the Internet age. Dessau has equipped itself to tackle the Cyber challenges by acquiring and fully integrating Elytra Enterprises Inc., a well known and experienced IT Security provider. By adding the security ingredient to all its historical offerings Dessau is one of the very few organizations to designate Cyber Security as a business imperative. What this means for the client is that Dessau takes care of all their security needs in the process of satisfying their business needs, be it a subway system, a telecom network, or a nuclear facility.

A CIP Primer

If there is one brief descriptive that captures the changing security world, post 9/11 attacks, it can be characterized as “completely open systems, where interconnections are

¹ <http://www.publicsafety.gc.ca/prg/em/nciap/about-en.asp>

omnipresent". Translated, this means that standards and their implementation are widely published and easily available to potential aggressors, and in any enterprise security is only as strong as the weakest link. If your Control or SCADA² system is connected to the corporate network, and the corporate network is accessible to your suppliers, then there are plenty of opportunities for an aggressor to neutralize security controls if the goal is to hijack a power substation.

This dangerous state of affairs has not descended upon us overnight, but is the offspring of the technology revolution brought to us by the Internet age. A few short years ago a SCADA system was discrete, well-controlled, and accessible to a few select operators who required a certain body of knowledge to do their job. Today's Control Systems allow managers real-time access to critical diagnostics and in the wireless world the person pushing the button could be at the end of his/her PDA³.

This is all very scary and baffling to the Control engineer whose purpose in life is the optimization of his particular process (refining, manufacturing, power generation, etc.). IT Security specialists, perhaps in the interest of increasing business, have not gone out of their way to ease the security burden on SCADA processes. This shortsightedness is slowly being rectified by progressive security specialists who see the CIP issues as challenges to be met head-on with time-tested and proven procedures and tools .

The PCS⁴/SCADA environment is pervasive across all aspects of CIP. Fortunately for SCADA operators, the security issues have been well understood in the IT Security field for the past decade, and an astute security professional can bring these lessons learned to the CIP world. At the same time the security professional is receiving a wake-up call to the traditional approach to security which for several years was overshadowed by the glamour field of IT Security and all its exciting tools. This traditional approach consists of the convergence of physical, personal, and technical (now referred to as IT Security) security into a unified security treatment for any enterprise⁵. We are slowly getting back to these three pillars of security which are of serious import if we are to have confidence in our CIP structures.

What's to be Done?

As mentioned in the previous section the threats to CI are well understood by security professionals, and every CI owner should make it their business to become familiar with those security threats, especially with the ones that apply specifically to their particular environment. The next step is to take logical measures to mitigate these threats so that the core business of operations can proceed unhindered and unabated.

² Supervisory Control and Data Acquisition: used in industry to monitor and control plant status and provide logging facilities; highly configurable

³ Personal Digital Assistant

⁴ Process Control System

⁵ For example, there is no point in spending millions of dollars on firewalls and Intrusion Detection Systems (IDSs) for the network if hiring procedures do not include a basic reliability check on that midnight operator who will be alone on duty.

Dessau/Elytra can provide a comprehensive Security Assessment of seven of the ten CIs identified by Public Safety Canada, and cost-effective recommendations to mitigate the major threats effectively. The client can then decide whether to implement these protective measures in-house or to call upon a Managed Security Services Provider to handle the security requirements. Dessau/Elytra can develop a security architecture tailored to any of the seven CI's that we specialize in, and we can help clients develop confidence in their security procedures.

For further information on our services and expertise, refer to

www.dessausoprin.com

www.elytra.com