



“Production environments are safe... aren't they???”

SCADA security

Currently there are many misunderstandings concerning SCADA Systems security. In the past most production networks were separated from other networks. However, today most of them are interconnected, meaning more and more vulnerabilities can be exploited on these production networks. Most of these environments are managed by the business itself. Keeping them running is more important than having them secured. However, when one of these systems is compromised, it can have a massive impact on the business.

SCADA systems control power, water, oil, gas, chemical, telecommunications and other critical and sensitive operational infrastructures that are absolutely vital to the machinery of our world and our day-to-day lives. Securing these networks was never an issue, since they were completely separated from other networks. Due to rapid changes of network topology and available technologies, securing these systems has become a huge concern for many companies.

Aszure can help you protect these vulnerable key infrastructures.

Aszure Assessment Program

The program has four pillars:

- Logical tests
- Physical tests
- Social tests
- Strategic tests

Logical testing focuses on the process network. Architecture review, system testing (internal, external, database systems, historians...) and system auditing (SCADA, OPC servers, servers, HMI's, network components) will be executed with extreme caution, minimizing the risk of system downtime.

In the physical test, we will try to gain access to your infrastructure, giving you a better view of the possible weak spots of your physical security.

During social testing, we will try to exploit the human factor to gain access to as much information as possible about your network.

Strategic tests are higher-level tests and can include risk analysis, Business Impact Analyses, High Level Risk Management Audits...

SCADA Security Consulting and Advice

Consultants working at Aszure have extensive competence in the field of SCADA security. Therefore, they are often hired for their specific knowledge and experience. Those assignments can be very short or can cover several months; they can be done once, or on a regular basis.

About Aszure

Aszure is specialized in operational risk management consultancy and staffing. Operational risk management, information security, business continuity and compliance to laws and regulations are major cornerstones of our services.

Aszure assists its customers with the incorporation of operational risk management at all levels and in all areas of their organization, including day-to-day operational decisions. No decision should be taken in any organization without applying proper operational risk management. It can be applied throughout the entire life cycle of any activity or project. In order to minimize risk, it is however preferable to apply operational risk management at the beginning phase of a project or operational activity.

About Aszure Academy

Aszure offers, through the Aszure Academy, an extensive education and awareness program, covering several open classes, events and customized education experiences.

Contact

For further and additional information, please contact us on Tel. +32 (0)9 243 10 20 or info@aszure.com

On all Aszure services our general terms of delivery apply.

Whether it is to address a particular problem, a wide range of problems, or the overall security of your system, our people can help you. We can assist your staff in attaining a secure environment while maintaining the much needed availability in process networks.

Security Implementation

Securing SCADA systems can be a sensitive operation. One mistake and your whole system can go down.

We can help in securing your system, minimizing the risk of unwanted and costly downtime. No need to spend many hours figuring out which product suits your needs.

Our personnel with in-depth knowledge of the latest security products will implement the required equipment and will provide you with all the necessary documentation.

Patch Management

Patching is a problem for many companies. In an industrial environment, patching is an even bigger problem.

The best way to start is to review your current policy. If there isn't one, we can assist you with the creation of a policy that is adapted to your specific needs.

By testing patches before implementing them, our team can be sure that patches don't affect the normal operation of your network.

Proper patch management limits the chances of a successful attack on your network.

Awareness

Having all the right tools and equipment in place just isn't enough. If your personnel think there is no need to secure your valuable assets, then why even bother securing them? Unlocked workstations, open doors, lost equipment, attaching infected devices to your network, rogue access points... These are just a few of the risks you may be facing.

Our team will make your staff aware of the possible risks your company may be facing, and thus further increasing security.



Hardening

Poor configuration of machines makes it easier for a hacker to intrude into your network. Getting access to one machine might be enough for a hacker to compromise your whole network. Have you closed all unnecessary ports? Have you changed all the default passwords? Is all unused software removed? Aszure can help you with hardening your systems, making your SCADA environment more secure.

WIB compliance

Higher security awareness has led to the birth of the WIB (Dutch workgroup for industrial security).

Now the question arises: are your vendors WIB compliant? Do they meet the security requirements described in the WIB? Or do they just say they are?

Aszure can help you, as an independent party, to assess whether your vendor really is WIB compliant. The vendors and their solutions will be evaluated with an extensive series of tests so that we can provide you with a detailed report about all the aspects of the WIB compliancy status.

Architecture review

In an architecture review, the Aszure Assessment team will look very closely at the deployed network architecture. They will investigate how the various network components are working together and if these are deployed in a secure way without posing unneeded risks to your information and assets.

Education

Our team teaches you, on a technical level, about SCADA security. What can you do to make your system more secure? And more important, how do you do it?

All participants will be provided with the appropriate training material, to assist them in their learning process.

“The most vital industrial systems in the world are supervised and controlled by SCADA systems. Why shouldn't the security of these systems be one of your main concerns?”

For more information, please contact:
Tel.: +32 (0)9 243 10 20
E-mail: info@aszure.com www.aszure.com
Bijenstraat 16-17, B-9051 Ghent, Belgium