**Cyber Security: ENISA White Paper: Can we learn from Industrial Control Systems/SCADA security incidents?**

**The EU’s cyber security Agency ENISA released a white paper today, giving recommendations regarding prevention and preparedness for an agile and integrated response to cyber security attacks and incidents against Industrial Control Systems (ICS)/SCADA. Increasing numbers of recent security incidents against industrial control systems/SCADA raise questions about the ability of many organisations to respond to critical incidents, as well as about their analytical capabilities. A proactive learning environment through ex-post analysis incidents is therefore key, the Agency underlines.**

ICS are widely used to control industrial processes for manufacturing, production and distribution of products. Often commercial, outdated off-the-shelf software is used. Well-known types of ICS include supervisory control and data acquisition (SCADA), where SCADA systems are the largest ICS subgroup. Recent ICS/SCADA incidents underline the importance of good governance and control of SCADA infrastructures. In particular, **the ability to respond to critical incidents, as well as the capacity to analyse the results of an attack in order to learn from such incidents is crucial, the Agency underlines.**

The goal of an ex-post incident analysis is to obtain in-depth-knowledge regarding the incident. This gives you the ability to:

* rely on robust evidence in order to respond to the changing nature of domestic and alien threats;
* ensure that enough learning takes place in order to deploy resilient systems.

We identified four key points for a proactive learning environment which will in turn ensure a fast response to cyber incidents and their ex-post analysis:

* Complementing the existing skills base with ex-post analysis expertise and understanding overlaps between cyber and physical critical incident response teams;
* Facilitating the integration of cyber and physical response processes with a greater understanding of where digital evidence may be found and what the appropriate actions to preserve it would be;
* Designing and configuring systems in a way that enables digital evidence retention; and
* Increasing inter-organisational and interstate collaboration efforts.

The Executive Director of ENISA [Professor Udo Helmbrecht](https://www.enisa.europa.eu/about-enisa/structure-organization/executive-director) commented: “SCADA systems are often embedded in sectors that are part of a nation’s critical infrastructure, for example power distribution and transportation control, which makes them an increasingly attractive potential target for cyber attacks, ranging from disgruntled insiders and dissident groups, to foreign states. Such systems should be operated in a manner which allows for the collection and analysis of digital evidence to identify what happened during a security breach.”

**For** [**full report**](https://www.enisa.europa.eu/activities/Resilience-and-CIIP/critical-infrastructure-and-services/scada-industrial-control-systems/can-we-learn-from-scada-security-incidents) **and recommendations;** <https://www.enisa.europa.eu/activities/Resilience-and-CIIP/critical-infrastructure-and-services/scada-industrial-control-systems/can-we-learn-from-scada-security-incidents>

**Background**: <http://ec.europa.eu/digital-agenda/en/news/eu-cybersecurity-plan-protect-open-internet-and-online-freedom-and-opportunity-cyber-security>

**For interviews;** Ulf Bergström, Spokesman, Mobile: ulf.bergstrom[at]enisa.europa.eu, mobile: + 30 6948 460 143, or Adrian Pauna, Expert, resilience[at]enisa.europa.eu