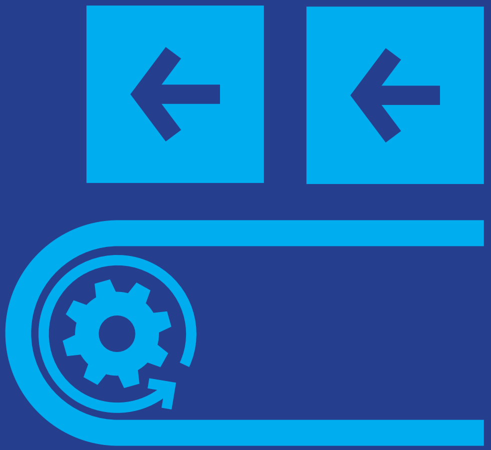
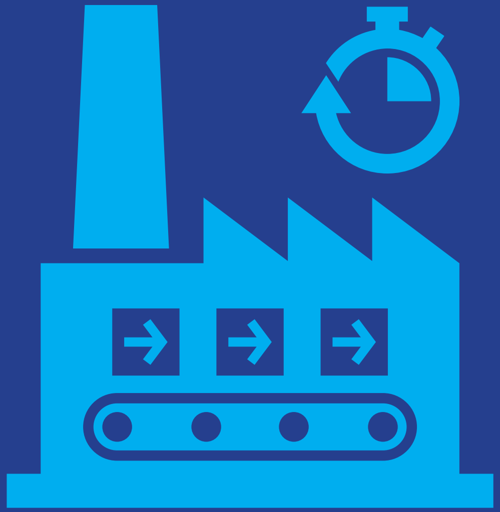


ENISA, the European Union Agency for Network & Information Security, is working together with stakeholders to identify pragmatic solutions to current Industrial Control Systems' security issues.

ICS SCADA AND SOCIETY

Industrial Control Systems (ICS) including SCADA (Supervisory Control and Data Acquisition) systems are the biggest part of the national and European Critical Infrastructures. In the last few years, ICS SCADA have passed through a significant transformation from proprietary, isolated systems to open architectures and standard technologies highly interconnected with other corporate networks and the Internet.

ENISA has recognised that the increased vulnerability to computer network-based attacks is an important weakness of intranets and open communication networks. Due to this increasing threat landscape, the agency has undertaken several activities to support ICS stakeholders by helping them to improve their security practices and by raising awareness to both industry and the public sector.



Industrial Control and SCADA systems are the heart of the European Critical Infrastructures. Action is needed. Follow ENISA's work and help us securing European industry.

To find out more about ICS SCADA systems visit www.enisa.europa.eu/scada

enisa

ENISA – European Union Agency for Network and Information Security

enisa.europa.eu

enisa

ENHANCING THE SECURITY OF ICS SCADA IN EUROPE

ENERGY
WATER
TRANSPORT
SHIPPING
CHEMICALS
MANUFACTURING

INDUSTRIAL CONTROL SYSTEMS

SUPERVISORY CONTROL AND DATA ACQUISITION

Information Sharing

ENISA organises and contributes to ICS SCADA workshops and initiatives about activities that aim at bringing together stakeholders to discuss ICS protection.

Examples of these initiatives are:

- The European SCADA and Control System Information Exchange (EuroSCSIE), which includes members of European Governments, research institutions, operators, industry that depend or are responsible for the security of Critical Infrastructures' industrial control systems.
- The European Reference Network for Critical Infrastructure Protection (ERNCIP) with a focus on Industrial Automated Control Systems and Smart Grids.
- The European Energy Information Security and Analysis Centre (EE-ISAC), aiming at sharing information and knowledge to increase the security of its members' infrastructures.

Community Engagement

In 2014 ENISA created the ICS Security Stakeholder Group. This group provides the opportunity for ICS SCADA experts to address important issues to ENISA in its work to enhance ICS security in the EU. It also gives the opportunity for ENISA to consult ICS SCADA experts and to listen to concerns and ideas.

Support Policy Making

ENISA's report on "Protecting Industrial Control Systems" aim to identify threats, risks and challenges in the area of ICS protection as well as to recognize national, pan European and international initiatives on ICS security. The report concludes with a set of recommendations for Europe that focus on three pillars:

- The creation of a pan-European Strategy for European ICS Security activities and the development of a National Strategy for ICS Security in each Member State.
- The creation of a common test bed(s) at European level, as a Public-Private Partnership.
- The establishment of National ICS-computer emergency response capabilities.

Lessons Learnt

Good governance and control of critical infrastructures and the ability to respond to cyber security incidents. ENISA's white paper on "Can we learn from SCADA security incidents" calls the security experts to:

- Facilitate integration with existing reporting and analysis structures.
- Safeguard systems and configurations.
- Review key roles and responsibilities.
- Pursue inter-organisational public and privately held and cross country cooperation.

Good practices on Testing

Security testing is a very crucial aspect for the acceptance of a product.

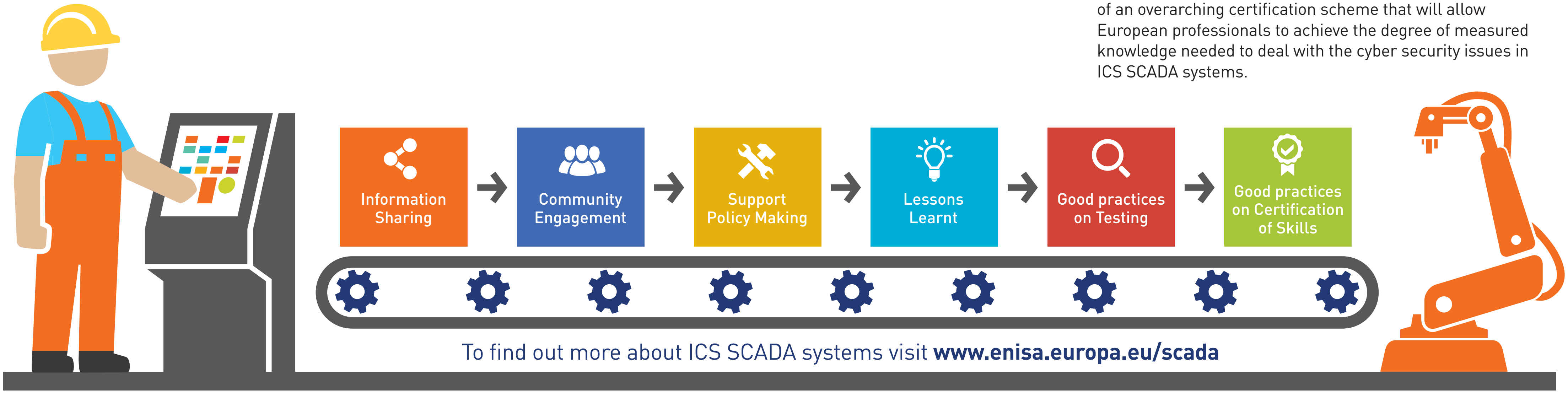
ENISA issued a study aiming to improve several areas of ICS security, not only by identifying the challenges to good security testing practices of ICS and SCADA systems but also providing key recommendations to the involved stakeholders:

- A Testing Coordination Capability under public European leadership should be created.
- Working groups of experts should define the testing methodologies and criteria that are more closely aligned with the testing strategy.
- The working groups involved will identify potential sources of funding and develop a business plan.
- CERTs should be contacted for specific cooperation, including Vulnerability Disclosures and incident response.

Good practices on Certification of Skills

Securing ICS SCADA from cyber threats requires to handle the confluence of contents, objectives and needs of two very different topics such as cyber security and industrial automation. Moreover there is the need to cover a skill gap from the lower operative levels to the top management. For this reason ENISA published a report on certification of Cyber Security skills of ICS SCADA professionals.

This report highlights the importance of the development of an overarching certification scheme that will allow European professionals to achieve the degree of measured knowledge needed to deal with the cyber security issues in ICS SCADA systems.



To find out more about ICS SCADA systems visit **www.enisa.europa.eu/scada**