DITS.center e.V.

ICS-S Industrial Control System Security

Industry 4.0 and the "Internet of Things (IoT)" promote the networking of systems for process control and factory automation. The design, development and operation of robust and secure systems will result in new challenges that are better addressed across companies. The aim is to promote SME networks.

The IT landscape of manufacturing and process automation companies is divided into the components Office IT and the Industrial Control System (ICS). ICS controls the physical processes and is an integral part of the value chain in most manufacturing companies. ICS consists of a large number of IT components at all levels of the automation pyramid with various vulnerable interfaces.

In office IT, sophisticated and mature security mechanisms, processes and regulations (e. g. password policy, endpoint security, firewalls, security of mobile systems) are already available. However, the maturity of information security in heterogeneous automation systems and networks, which have grown over decades, still needs to be greatly improved. The responsible persons involved often lack experience in the field of information security - the IT security experts, on the other hand, are faced with the particular framework conditions of automation engineers such as real-time, safety, firmware, machine control software are not very familiar.

There is no standard for ICS components to fight against attacks, although serious economic damage, risk of injury and supply failure are threatening. The systematic exclusion of hazards requires training, measures in development and operation. The exchange between users (production companies), IT experts and governmental institutions (BSI) is necessary to integrate both the special industry know-how and the security understanding.

Through funding and research, ICS-S establishes a network that develops sustainable solutions in the security environment of mechatronics and implements them in line with market and application requirements.

The ICS-S network activity is driven by the constantly changing requirements and the resulting need for action. Industry 4.0 increases the potential danger with new goals and technologies. Stricter requirements of the IT security law, as well as the international series of standards IEC 62443 on industrial communication networks have to be taken into account.

In the past, the firmware of automation technology could be developed and operated by the developers as a proprietary solution outside of generally accepted standards. Today, transparency and traceable compliance with standards and norms are mandatory. There is a need to adapt products and establish new standards for developers and operators.

The loss of data as well as the attack on processes and facilities in the areas of production, supply and distribution define threats with serious economic and social consequences. The ICS-S initiative promotes awareness of the topic both in the development of components, production and management on the operator's side. Practitioners and users are supported and encouraged by an information forum for processes, methods and measures to detect attacks and defend themselves.

The complexity of the possible attacks in the areas of automation, digitization, industry 4.0 and the Internet of Things is manifold. Especially the medium-sized manufacturers and operators of automation technology are challenged with identical questions. There is a risk that ICS-S could have a lasting effect on competition between large industry and SMEs to the detriment of SMEs. It is only reasonable to secure or increase the effectiveness and efficiency of the measures and competitiveness by acting jointly and in a coordinated manner. The following concrete measures are envisaged in the ICS-S project:

- Systematic analysis of the problem areas (use cases)
- Analysis of threat scenarios and case studies
- Analysis of legal framework conditions, data protection etc.
- Cooperation with research institutions
- Cooperation with authorities (BSI) in the area of IT security
- Cooperation with security agencies to create situation reports
- Cooperation with system integrators
- Integration of software, hardware and consulting companies
- Implementation of projects on individual questions and topics
- Realisation of information events and training courses
- Development and maintenance of an internet-based knowledge platform
- Pointing out possible solutions
- Promotion of cooperation.

Technology	Software, viruses, digitization, IT and Cyber Security, IEC 62443, civil security, data protection, data security.
Markets	Production engineering, automation technology, process engineering, software, firmware.
Remarks	Industrial Control System, Industry 4.0, Internet of Things, Networking, SME, synergy, cooperation.