KASPERSKY lab

KASPERSKY SECURITY SYSTEM

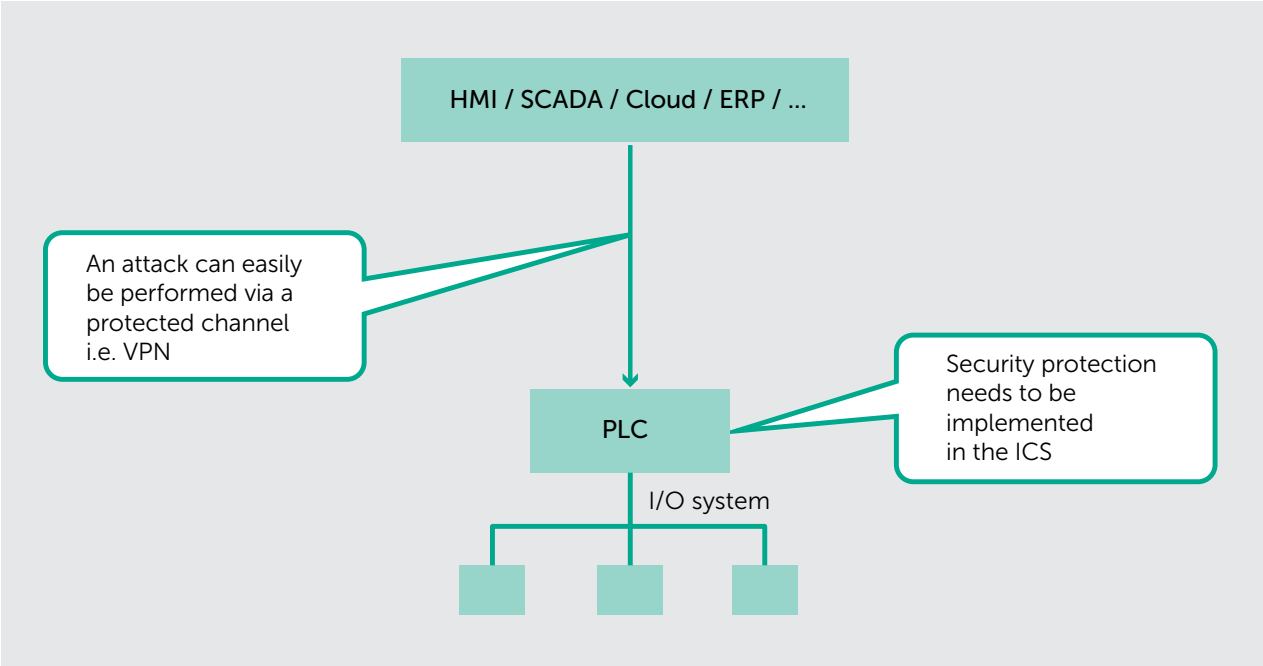
for Industrial Control Systems (ICS)

www.kaspersky.com

INTRODUCTION

Protecting a PC against threats is seen as common sense. However, the reality is that for every PC in the world there are hundreds of embedded systems, many of them being used in industrial applications and interconnected via Ethernet and other communication channels.

Even in the case of critical applications used for process automation in refineries, chemical plants, water and wastewater treatment, smart-grid automation, mobile automation systems and even in large production machinery in factory automation systems, the industrial control system (ICS) can be easily accessed, making these applications potential targets for dedicated attacks.



A secure communication channel is not enough to guarantee protection against attacks.

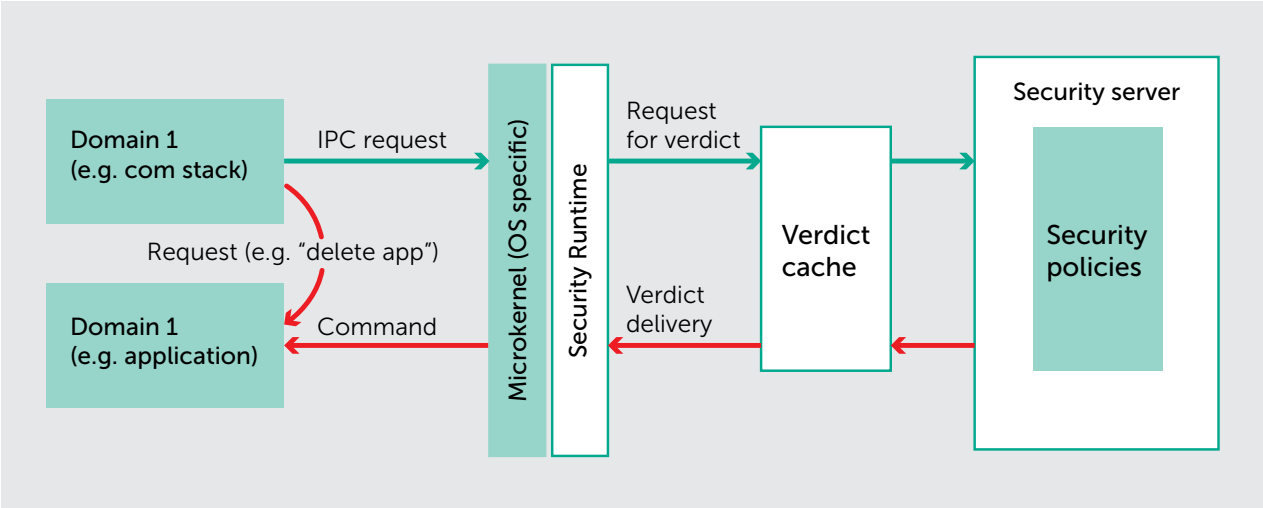
Some of these industries are very conservative and expect a control system to last for years, if not decades. As it's impossible to retrofit systems that are not secure-by-design and attack vectors can only be mitigated in this case, it is extremely important that manufacturers define a cybersecurity strategy as part of the specifications for new products.

In a highly competitive market like industrial automation, manufacturers can no longer afford to only use proprietary software and it is now common to use third-party technologies for the operating system, real-time engine, communication and field bus protocol stacks as well as the logic engine. These technologies come with vulnerabilities that turn the ICS into an easy target.

Most of the embedded software technologies, such as logic engines executing code in a development system (i.e. IEC 61131 tool), are not secure by design. They weren't and still aren't developed with cybersecurity in mind. Quality, reliability, performance, time to market and openness of the software remain the priority of tool manufacturers.

Monolithic systems do not provide a secure basis against incidents and attacks. Moreover, many manufacturers lack knowledge in security and are largely unaware of the threats as well as the techniques and technologies necessary to make their ICS secure.

For manufacturers to meet the security requirements of an ICS, they need to start with a system redesign in combination with specialized software. The embedded software needs to be separated in different domains and run as different processes. All communication between processes must run through a dedicated security system that can control all communications in accordance with predefined security policies.



Process for communication between domains using KSS

Kaspersky Lab and BE.services GmbH have joined forces to help manufacturers create secure ICS equipment and provide solutions and services to address embedded security issues. BE.services supports the integration of KSS in the firmware.

Kaspersky Security System is a versatile security engine that enables the definition and checking of custom security conditions for ICS applications. This is not just about malware protection; it's also about preventing common violations of security rules. The solution adds security without harming production safety. Kaspersky Security System is embedded in the firmware of the ICS, computing security verdicts that are defined and configured by authorized personnel.

APPLYING KASPERSKY SECURITY SYSTEM

- Defining security policies:
  - Identifying untrusted software in the information
  - Decomposing this software into the components
  - Determining the set of privileges required by every component to run properly
  - Classifying application data and system resources used by components
  - Defining rules for interaction between system components and for data access
- Enforcing security policies to prevent both accidental errors and unauthorized access attempts
- Event logging and reporting

COMBATING CYBER-PHYSICAL RISKS

Security violations can be the result of a simple misuse of the industrial network, or an advanced targeted attack that exploits diverse vulnerabilities on different ICS network layers. Whatever the cause, these incidents can lead to significant financial and reputational damage, a halt to critical processes and other adverse effects that must be prevented.

The main goal of the collaboration between BE.services GmbH and Kaspersky Lab is to create a solution that protects the most critical ICS assets against security violations.

About BE.services GmbH

BE.services GmbH's core competence is the support of ICS manufacturers in the development of their automation systems by providing both software solutions and embedded software services, from architecture design consultancy to complete embedded software development.

As Kaspersky Lab's distributor and integrator of embedded cybersecurity solutions, BE.services provides a complete offering for Industry 4.0 & IIoT compliance. While ICS are required to be SMART, REAL-TIME and CONNECTED, the real challenge for manufacturers is to make their control systems SECURE. This is exactly what BE.services provides based on the technologies from Kaspersky Lab.

About Kaspersky Lab

Kaspersky Lab is a global privately held cybersecurity company founded in 1997. Kaspersky Lab's deep threat intelligence and security expertise is constantly transforming into security solutions and services to protect businesses, critical infrastructure, governments and consumers around the globe. The company's comprehensive security portfolio includes leading endpoint protection and a number of specialized security solutions and services to fight sophisticated and evolving digital threats. Over 400 million users are protected by Kaspersky Lab technologies and we help 270,000 corporate clients protect what matters most to them.

BE.services GmbH
Heisinger Strasse 12
87437 Kempten – Germany
Tel.: +49-831-9606-9991
Fax: +49-831-9606-9990

AO Kaspersky Lab, 39A/2 Leningradskoe shosse,
Moscow, 125212, Russian Federation,
www.kaspersky.com
All about Internet security: www.securelist.com
Find a partner near you: www.kaspersky.com/buyoffline