Embedded Security Shield (KasperskyOS edition) by Kaspersky Lab and BE.services GmbH

KasperskyOS®

www.kaspersky.com
os.kaspersky.com

BE. services

www.be-services.net

The industrial control system (ICS) is the core of industrial automation and, with the advent of Industry 4.0 and the Industrial Internet of Things (IIoT), it will retain its role at the heart of smart manufacturing. However, as industrial environments evolve, security considerations increasingly come to the fore. The proliferation of connected devices and the complexity of managing IT / OT convergence in a smart manufacturing era make industrial control systems increasingly susceptible to cyberattacks.

Challenge

Kaspersky Lab views ICS cybersecurity as one of the most important aspects of its business. Instead of simply providing a limited solution for specific cybersecurity tasks, Kaspersky Lab works closely with the leading ICS companies to establish a whole new level of security maturity for every aspect of industrial control systems, including SCADA, PLCs, IIoT, as well as for secure ICS communications, incident processing and much more.

Last year Kaspersky Lab, in collaboration with BE.services, presented Embedded Security Shield technology to harden CODESYS runtime – the functional engine widely used in programmable logic controllers.

By using Kaspersky Security System for Linux, the solution hardens CODESYS runtime and provides additional guarantees in case CODESYS components responsible for communications with the rest of the ICS infrastructure are exploited. It operates on top of Linux and uses Linux containers to sandbox potentially dangerous software components. Kaspersky Security System uses a pre-defined set of security policies to ensure the system persists in a secure state.

KSS helps Embedded Security Shield eliminate the majority of attack vectors that are often encountered in any ICS infrastructure. However, Embedded Security Shield is not a 100% secure solution due to the Linux platforms that operate inside embedded operating systems. It's a well-known fact that exploiting a Linux kernel vulnerability can bypass even the most powerful protection.

The present-day reality requires new approaches that offer no opportunities to attackers and, at the same time, don't impact on other ICS characteristics like performance, real-time properties and just as importantly – costs.

The Kaspersky Lab solution

Kaspersky Lab is constantly working on its core technologies and among them is its very own operating system – KasperskyOS – capable of implementing a new level of cybersecurity for ICS.

Successful progress in hard real-time support makes KasperskyOS an ideal platform for PLCs.

In 2018, BE.services, in cooperation with Kaspersky Lab, successfully adapted CODESYS runtime to run on KasperskyOS.

CODESYS runtime, like Embedded Security Shield, was divided into two isolated parts – the Communication component and Core component – during development.

The Communication component handles requests from the ICS network and it is the primary target for cyberattacks. KasperskyOS guarantees reliable isolation of the software components running under its control. This means any problem that occurs in the Communication component is restricted to its sandbox and does not affect the rest of the solution. KasperskyOS, in combination with Kaspersky Security System (KSS), controls all the communications between the CODESYS Communication component and the CODESYS Core component. KSS performs an analysis of all the inter-component interactions in the system and decides if the operation is possible or not – then KasperskyOS enforces this verdict. Therefore, the Communication component can only interact

"The Embedded Security Shield under KasperskyOS is a high-end cybersecurity solution for IoT devices and edge controllers. We have ported the CODESYS logic engine under KasperskyOS in order to allow and simplify secure-by-design control system design. BE.services' expertise in industrial automation, combined with Kaspersky Lab's expertise in cybersecurity allow us to provide dedicated solutions to automation vendors."

Dimitri Philippe,
CEO, BE.services GmbH

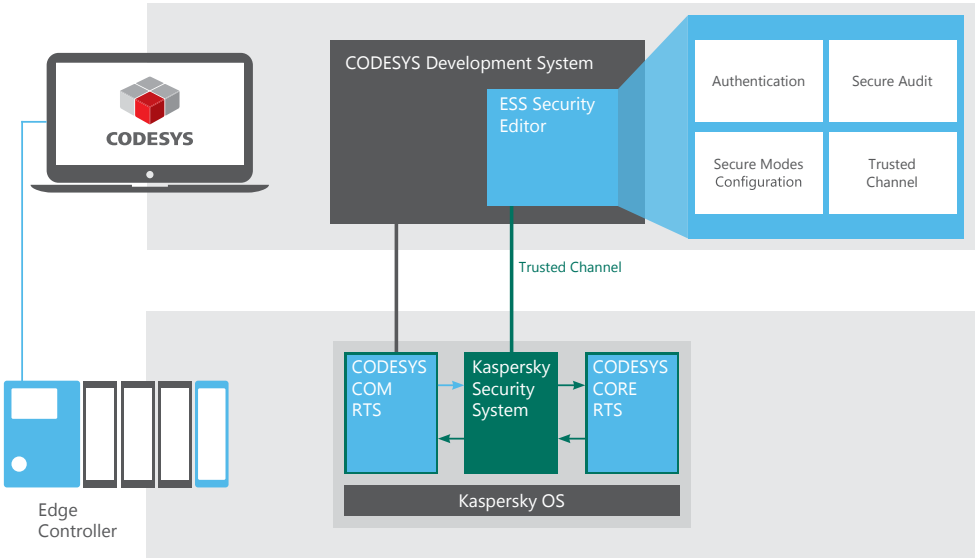
with the Core component – responsible for running the PLC program and communicating with equipment over the field bus – in a safe and secure manner in accordance with the specified security policies.

KasperskyOS was designed to be secure. It has microkernel architecture and the microkernel has a tiny attack surface – it provides only three system calls. It also implements best practices and state-of-the-art approaches to operating system security to ensure it works properly in a wide range of conditions. It works in close conjunction with Kaspersky Security System – an integral part of KasperskyOS that supports a variety of formal security models capable of describing almost any aspect of secure system behavior. KSS introduces an independent layer of security at the lowest level of the system and secure behavior is described separately from the solution business logic.

As a result, the system becomes extremely reliable from a cybersecurity point of view. Even when a software component running on KasperskyOS is attacked, it won't impact normal system behavior. More than that, the Kaspersky Security System engine detects all security policy violations and makes it possible to undertake appropriate recovery actions.

To summarize, running CODESYS runtime natively on KasperskyOS makes it possible to achieve PLC functional goals, while proper software architecture and the security properties of KasperskyOS/KSS guarantee the most reliable operational security.

It's worth mentioning that KasperskyOS implements an extended set of security patterns out of the box (Trusted Channel (TLS-based framework), Secure Audit, Secure Update and many others). They provide a way of securely controlling and configuring the solution as well as ensuring it is kept in a constant state of security.



About Kaspersky Lab

Kaspersky Lab is a global cyber-security company celebrating its 20th anniversary in 2017. The company'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. Kaspersky Lab's comprehensive security portfolio includes leading endpoint protection and a number ofspecialized 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. Learn more at www.kaspersky.com.

About BE.services

BE.services GmbH is an embedded software technology and service provider for industrial automation, with offerings ranging from consulting on the firmware to specific development tasks or turn-key projects. BE.services is also a distributor and system integrator of KasperskyOS, a dedicated secure OS for connected devices and KSS for non-CODESYS-based ICS.

Result

- **Functionality**
  The solution provides full-bodied CODESYS runtime functionality; the guarantees of high-level security do not conflict with the functional requirements.

- **Performance**
  According to Kaspersky Lab internal tests that covered a huge range of use case scenarios, the performance impact of Kaspersky Security System checks varies from 0.5% to 5%, compared to a solution without KSS. Thanks to the simplicity of the KasperskyOS microkernel and provision of highly optimized drivers, the performance of a KasperskyOS-based solution can be made even higher than similar Linux-based solutions. When it comes to hard real-time requirements KSS test results show that, due to its architecture, security policy calculations only cause minimal delays that do not affect the real-time characteristics of the overall solution.

- **Integration**
  KasperskyOS-based CODESYS runtime implementation is fully compatible with CODESYS IDE, which saves on development time and implementation costs.

- **Security**
  Embedded Security Shield's security properties meet the most stringent, up-to-date security requirements for modern ICSs without any of the conflicts pertinent to other ICS characteristics.

KasperskyOS®

Find out more at
os.kaspersky.com

www.kaspersky.com