

# Embedded Security Shield

Release 01.11.16



## Scope

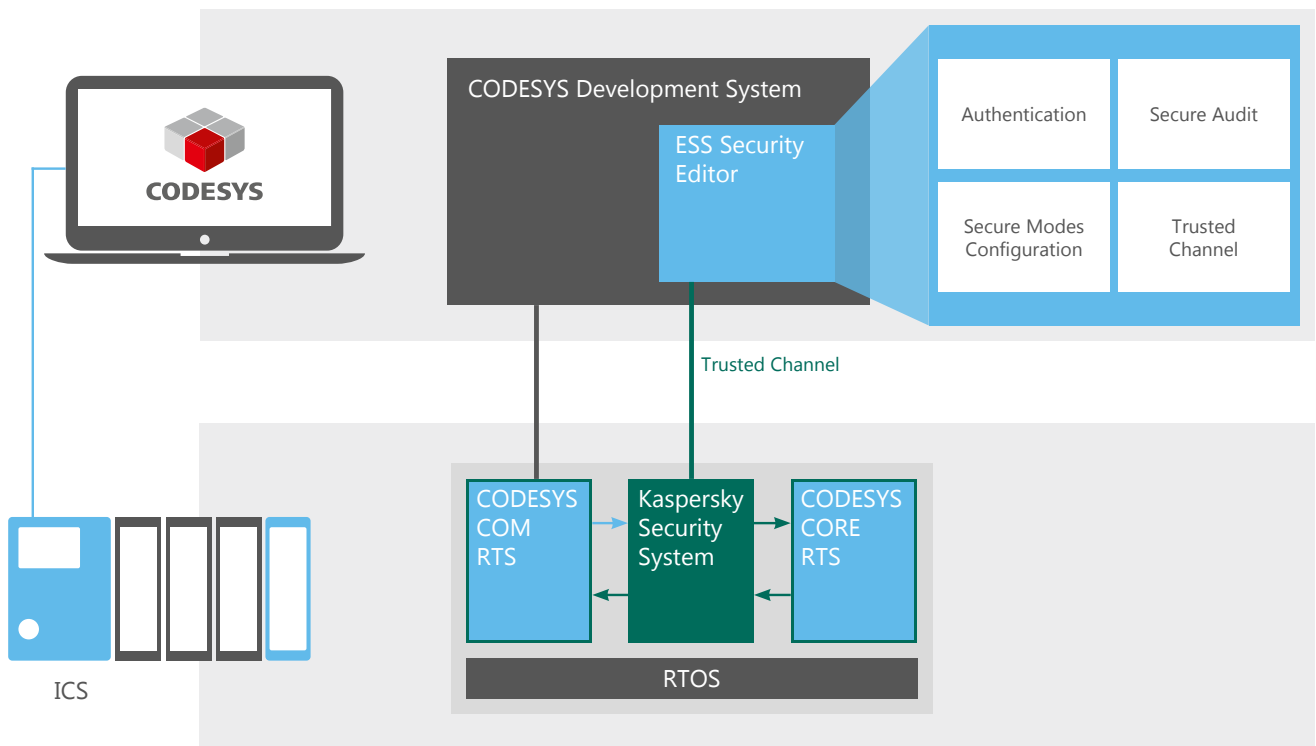
A new era of Industrial production has started with Industrie 4.0. The proliferation of connected devices multiplies the risk of attacks on Cyber Physical Systems. In industrial Automation, many Industrial Control Systems integrate the CODESYS technology from 3S-Smart Software Solutions. The Embedded Security Shield extends Kaspersky's Security System (KSS) for a complete integration into CODESYS and to secure the main communication channel, the CODESYS Gateway.

## Target Applications. Control systems in different vertical markets:

- Factory Automation – PLC, HMI, Motion Controller
- Process Automation – DCS, SCADA, Process controllers
- Energy production and distribution – RTU, Gateways, SCADA
- Building Automation – BAS, HMI
- Mobile Automation - ECU

## Functionality

- Cyber-security of the ICS
- Protection of the CODESYS Gateway communication channel
- Configuration of security policies directly in CODESYS
- Trusted communication channel with the CODESYS Development System
- Execution of the CODESYS Runtime in a secure environment
- Extendable framework to secure customer specific software tools and communication channels



Integration of the Embedded Security Shield in CODESYS

## Features and benefits

### Made by experts

ESS is based on Kaspersky Lab's KSS ⇒ trusted and recognized specialist for cyber security

### Complete integration

ESS provides the integration of KSS in CODESYS, both in the runtime and in the IDE ⇒ time and cost saving for the implementation

### Performance

Minimal delay caused by the security process ⇒ compatible with systems with hard real time behaviour

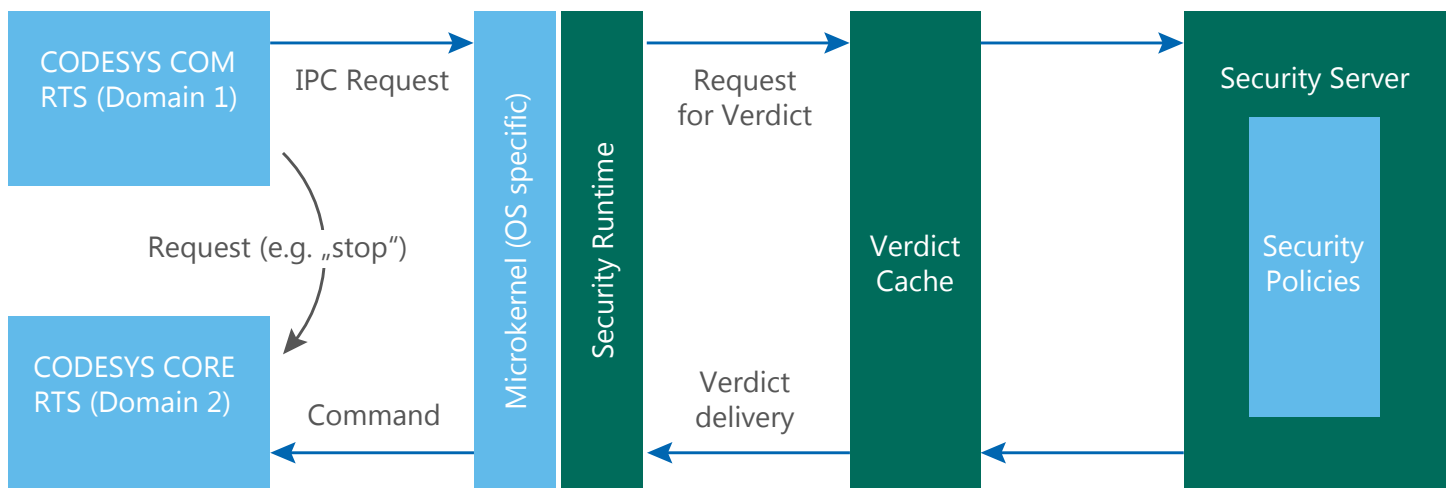
### Framework

The system is a technology, adaptable to the existing firmware. Different/additional communication channels can be secured by the same means ⇒ complete security with a single technology

### Expertise for support and development

BE.services can be contracted for development, extension or integration services ⇒ time and cost saving through 3rd party expertise

## Mechanism



The CODESYS Runtime System is divided into 2 domains:

- Communication
- Core

All communication to the ICS is handled through the Communication runtime. The Core runtime is isolated from any external communications happening through the CODESYS Gateway (communication with CODESYS, OPC, PLCHandler, data server, etc...).

All requests to the ICS come to the Communication Runtime. Their execution is checked by the Kaspersky Security System, a secure, mathematically proven, engine.

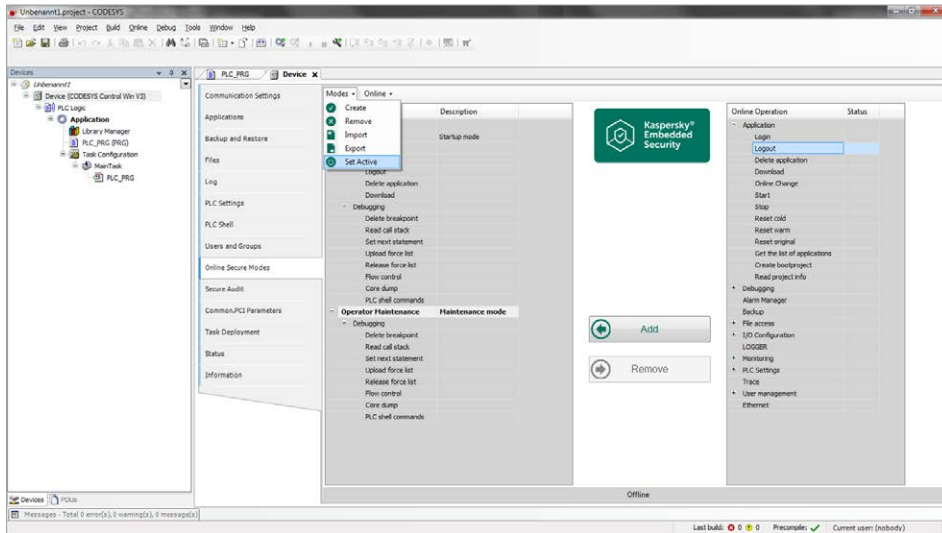
KSS checks the requests with the existing security policies and allows or denies them. The verdict cache retains previous requests to speed up execution of known past requests.

Security policies are defined and configured by the User's Security Administrator using the ESS Security Editor provided as an additional plug-in in CODESYS.

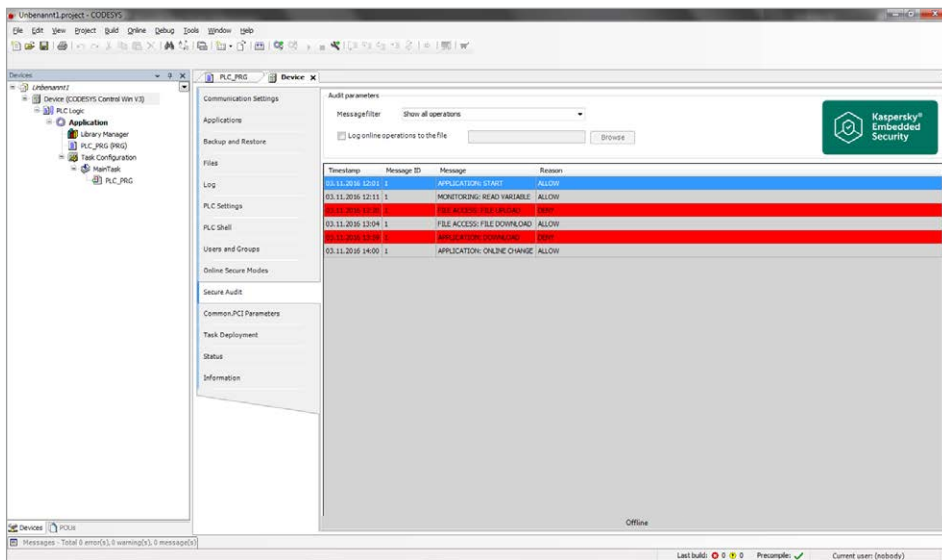
Secure communication for data exchange (security policies configuration, secure audit trail) between the ESS Security Editor and KSS is managed through specific trusted channel.

## Software Package includes

- Embedded Software:
  - Embedded Security Shield
  - Kaspersky Security System (KSS)
  - CODESYS Runtime extensions
- Development software:
  - ESS Security Editor plug-in for CODESYS



Configuration of the security modes



Secure Audit

## Engagement model

How to get?

Product	Manufacturer	Part Number	Sales Contact
Embedded Security Shield Toolkit	BE.services GmbH <a href="http://www.be-services.net">www.be-services.net</a>	0230113	info@be-services.net
Maintenance and Support package for ESS	BE.services GmbH <a href="http://www.be-services.net">www.be-services.net</a>	0230150	info@be-services.net



## Technical data

General system information		
Runtime size	Code	2.7 MB/ 3.3 MB (without/with ESS)
	Data	0.8 MB/1.0 MB (without/with ESS)
Communication		UDP / Serial / USB Trusted channel
Supported CPUs		X86, ARM, ARM Cortex, PowerPC Others on demand
Supported operating systems		Linux Others on demand

Performance data		
Command	Without ESS	With ESS
Application download (302 kB)	2.98 s	3.01 s
File transfer (1.5 MB)	28.80 s	28.87 s
OPC access (2000 variables of type byte)	4 ms	5 ms

Test hardware: Xilinx Zynq ZC702 (ARM Cortex A9)

### Evaluation Kit:

Evaluate the Embedded Security Shield on the Xilinx Zynq ZC702. More information under:  
[www.be-services.net/industrie-40/xilinx.html](http://www.be-services.net/industrie-40/xilinx.html)

## Support

Please contact [info@be-services.net](mailto:info@be-services.net)

[www.be-services.net](http://www.be-services.net)