Security in Automation –
possible threats and integrated measures in CODESYS

CODESYS Users Conference 2017

Manfred Werner

CODESYS® a trademark of 3S-Smart Software Solutions GmbH

Agenda

1. What is Security?
2. Situation in Industrial Security
3. Security Measures within CODESYS

© 3S-Smart Software Solutions GmbH

What is Security?

Safety

VS.

Security

Protect humans

„Keep crazy people from doing stupid things“

- Restricted complexity
- Failure prediction
- Availability is not central

Protect investments

„Keep smart people from doing clever things“

- Constantly growing complexity
- Prediction of threat situation is not possible
- Availability has top priority

© 3S-Smart Software Solutions GmbH

What is Security?

„Keep smart people from doing clever things!“

© Author unknown, Location: Konsequenz, Universität Bielefeld

© 3S-Smart Software Solutions GmbH

Situation in Industrial Security

Vulnerabilities incidents in industrial security:

- RISI 2010 (ICSJWG Spring Conference):
  - 162 incidents since 2000
  - 78% unintended (handling or device errors, viruses)
  - 22% intentional, 53% of which by insiders (employees) and 47% by externals (including suppliers)

Vulnerabilities in products (ICS):

- ICS-Cert Advisories
  - 44 vulnerabilities in different products from January until May 2013
  - Are systematically searched for by security consultants (service providers)

Remarkable:

The incidents have nothing to do with the vulnerabilities.

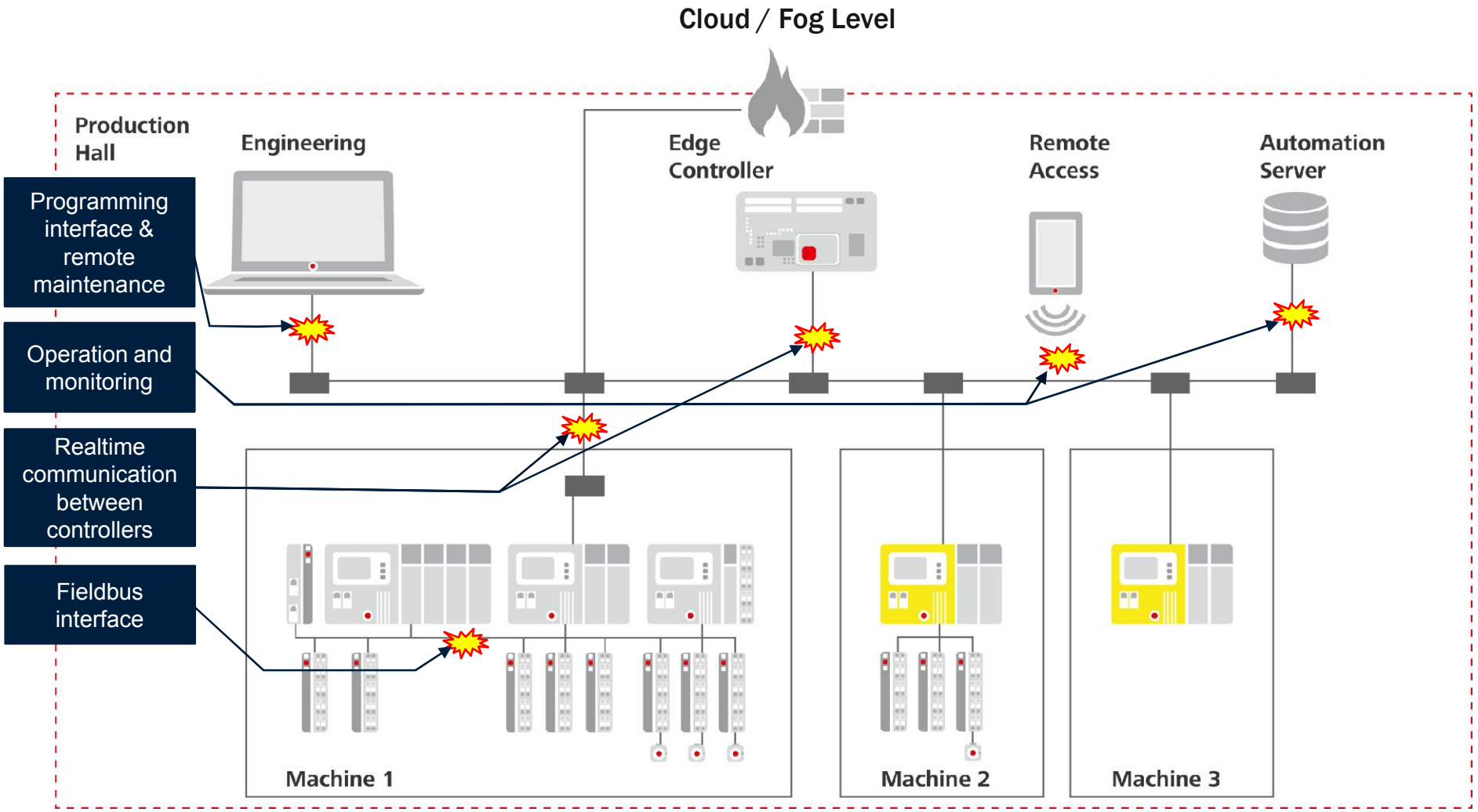
Known, targeted attack on an application

- StuxNet

© 3S-Smart Software Solutions GmbH

Situation in Industrial Security

Vulnerabilities



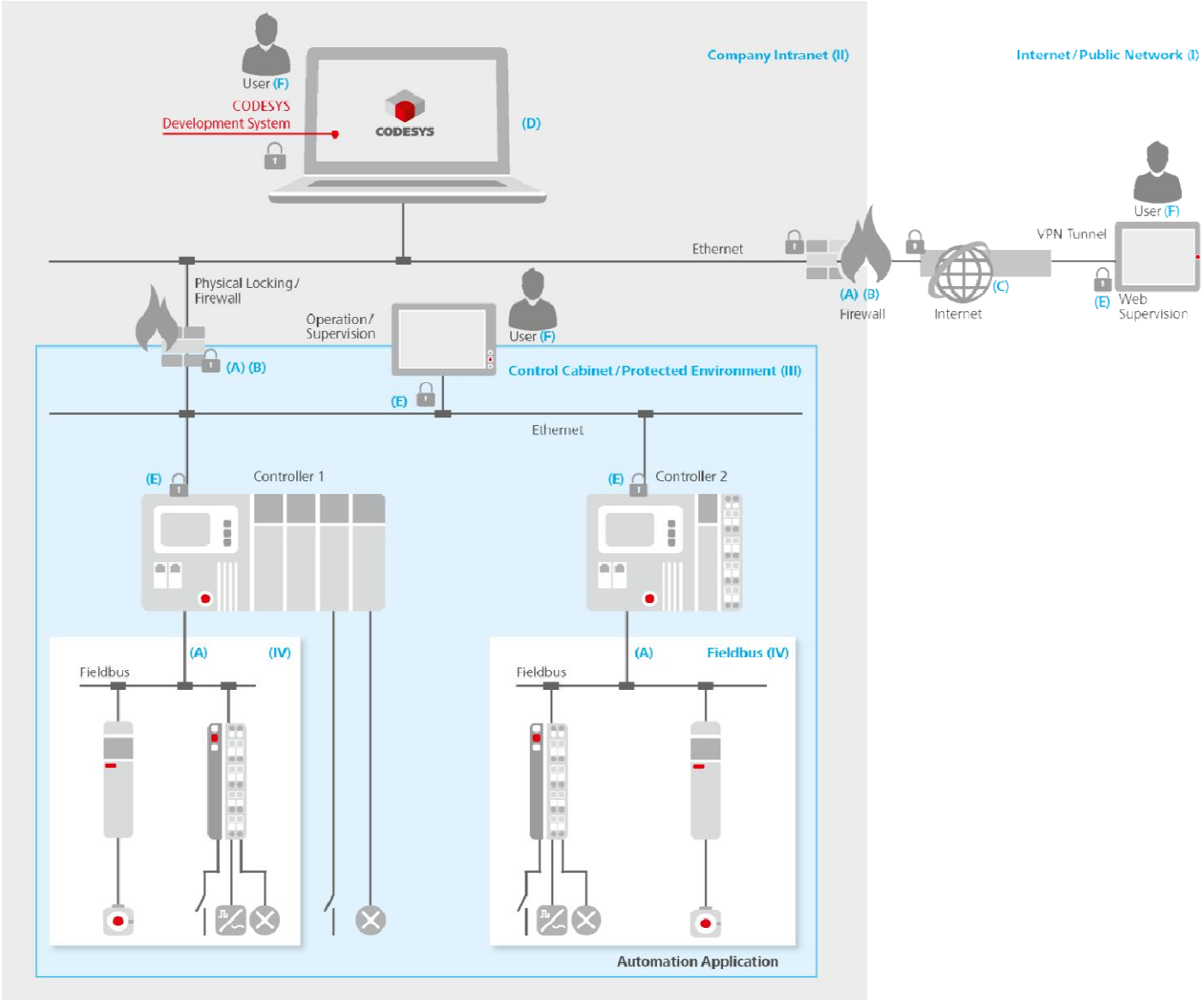
© 3S-Smart Software Solutions GmbH

IEC 62443 protection level

- **Level 1:** Occasional and accidental threat
  - Example: Hard disk failure
  - Example: Operating error
- **Level 2:** Intentional threat by simple means
  - Example: Password guessed correctly
- **Level 3:** Intentional threat by highly-developed means
  - Example: Hacker tools
- **Level 4:** Intentional threat by highly-developed means and extended resources
  - Example: Specific development
  - Example: Knowledge of the application
  - Example: Corruption of insiders

© 3S-Smart Software Solutions GmbH

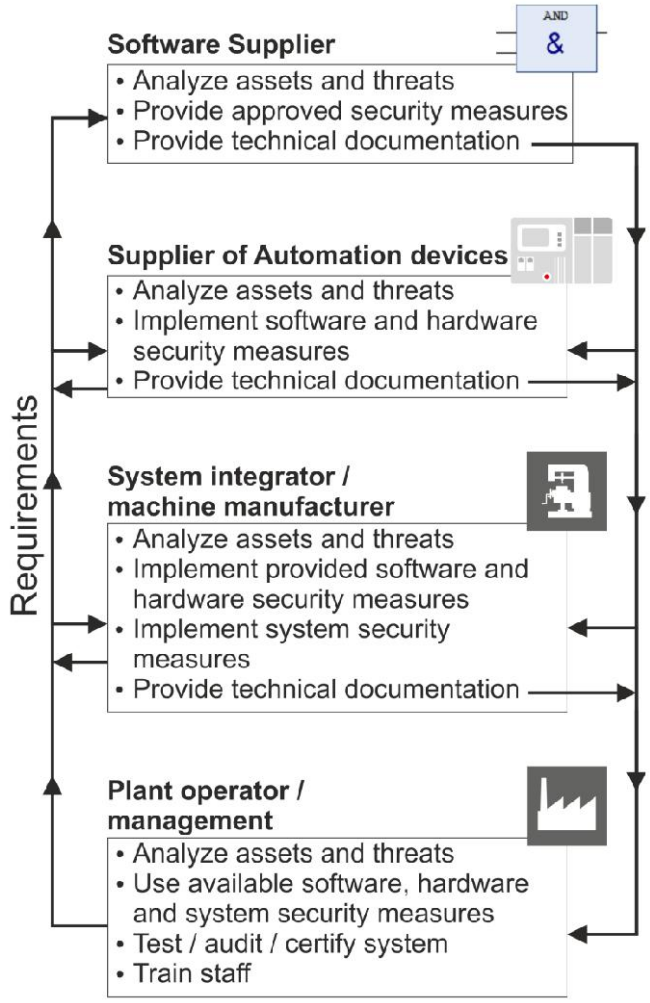
Situation in Industrial Security



© 3S-Smart Software Solutions GmbH

Situation in Industrial Security

Security responsibilities in industrial control applications



© 3S-Smart Software Solutions GmbH

Security measures within CODESYS

Security Whitepaper

- Guidline for OEMs, System Integrators and Operators
- Introduction in security subjects in industrial automation
  - Involved parties
  - Definition of the security level
  - Available tools in CODESYS to achieve the desired security level
  - Dealing with detected security vulnerability

© 3S-Smart Software Solutions GmbH

Security measures within CODESYS

CODESYS Development System

Measure	Whitepaper Section	Measure relevant for			Suitable measure against
		Suppliers of automation components	System integrators / machine builders	Operator	
Encryption of the source code of the application	5.1.1 (10)		X		Occasional / unintentional threats and attacks
User administration on project level	5.1.2 (11)		X		Occasional / unintentional threats and attacks

© 3S-Smart Software Solutions GmbH

Security measures within CODESYS

CODESYS Runtime System

Measure	Whitepaper Section	Measure relevant for			Suitable measure against
		Suppliers of automation components	System integrators / machine builders	Operator	
Access to the runtime system with authentication / permission management	5.2.1 (11)	X	X	X	Occasional / unintentional threats and attacks
Encryption and signing of the executable application code	5.2.2 (11)	X	X		Attacks
Controller operation mode	5.2.3 (12)		X		Occasional / unintentional threats and attacks
Interactive login	5.2.4 (12)	X	X		Occasional / unintentional threats
Disaster recovery	5.2.5 (12)	X	X	X	Occasional / unintentional threats
Communication encryption between the IDE and the controller	5.2.6 (12)	X	X	X	Attacks

© 3S-Smart Software Solutions GmbH

Security measures within CODESYS

IEC 61131-3 Application code

Measure	Whitepaper Section	Measure relevant for			Suitable measure against
		Suppliers of automation components	System integrators / machine builders	Operator	
Access restrictions out of the application / library	5.3.1 (13)	X	X		Occasional / unintentional threats and attacks
Unlocking additional functions	5.3.2 (13)	X	X		Occasional / unintentional threats and attacks

© 3S-Smart Software Solutions GmbH

Security measures within CODESYS

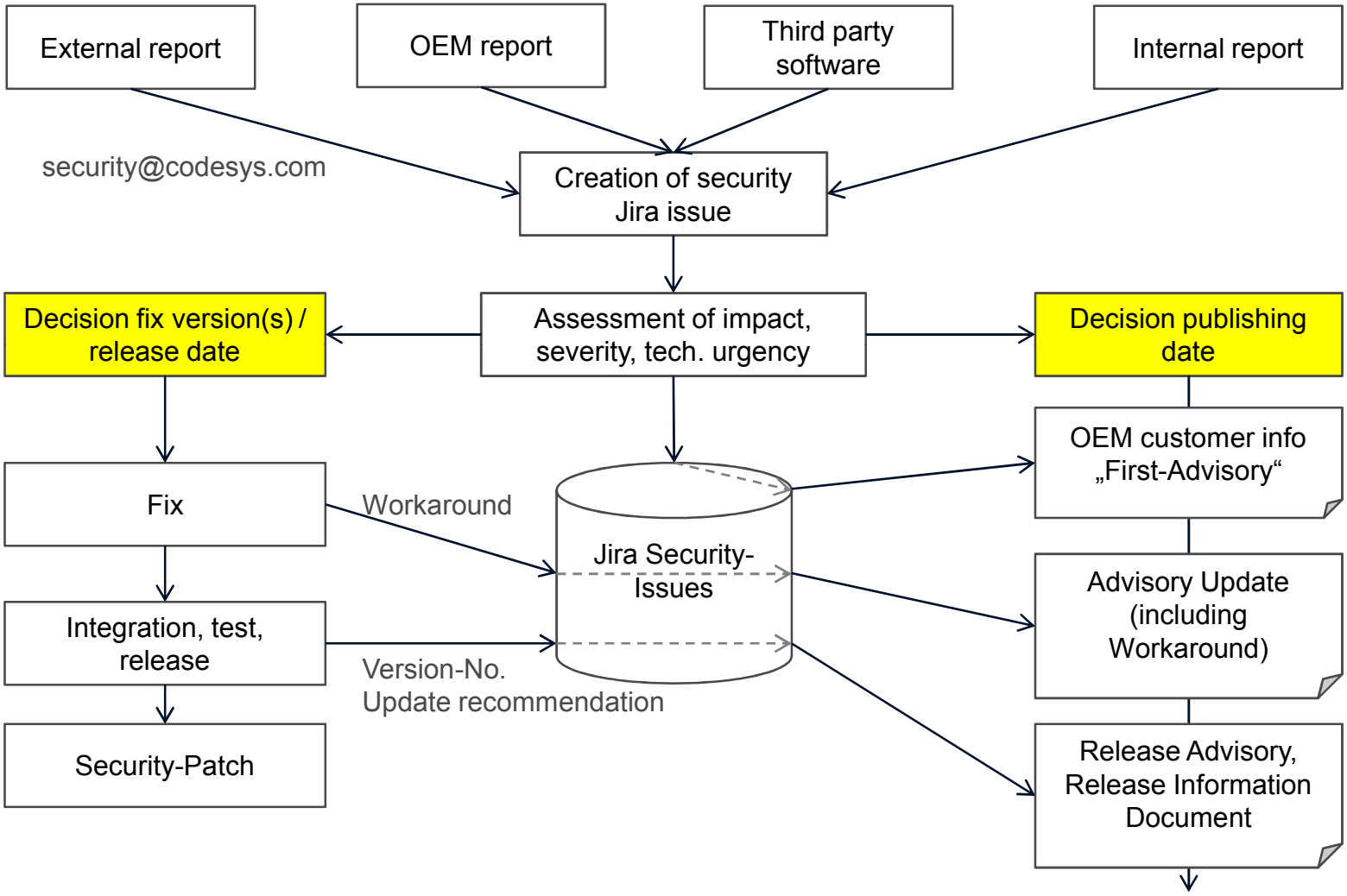
CODESYS Visualization

Measure	Whitepaper Section	Measure relevant for			Suitable measure against
		Suppliers of automation components	System integrators / machine builders	Operator	
Visualization User Management	5.4.1 (13)		X	X	Occasional / unintentional threats and attacks
Communication encryption for the CODESYS WebVisu	5.4.2 (13)	X	X	X	Attacks

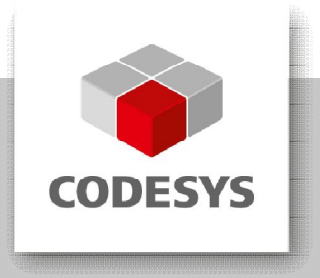
© 3S-Smart Software Solutions GmbH

Security measures within CODESYS

Handling of security vulnerabilities in CODESYS



© 3S-Smart Software Solutions GmbH



Inspiring Automation Solutions

Thank you for your attention.

CODESYS® is a registered trademark of 3S-Smart Software Solutions GmbH. Technical specifications are subject to change.
Errors and omissions excepted. No reproduction or distribution, in whole or in part, without prior permission.
Note: Not all CODESYS features are available in all territories. For more information on geographic restrictions, please contact support@codesys.com.

© 3S-Smart Software Solutions GmbH