Safe and secure communication

Agile Safety Workshop
Trondheim, May 30, 2016

Presented by Stig Petersen, SINTEF ICT
stig.petersen@sintef.no

Evolution of industrial communication

Phase 1: Dedicated wires

One dedicated wire from control system to each individual field instrument.

Phase 2: Fieldbuses

Multiple instruments connected to a single wire using fieldbus technologies.

Phase 3: Open and shared infrastructures

Transmission over open and/or shared systems, e.g. Ethernet.

This also includes transmission over wireless networks.

Standards for safe communication

EN 50159: Railway applications

Safety-related communication in transmission systems.

IEC 61784-3: Industrial communication networks

Functional safety fieldbuses.

EN 50159 – Railway applications (2010 ed.)

EN 50159 classifies communication systems into three categories:

Category 1 – Closed systems

Systems under the control of the designer, and fixed during their lifetime.

Category 2 – Open systems

Systems partially unknown or not fixed, but unauthorized access can be excluded.

Category 3 – Open systems

Systems which are not under the control of the designer, and unauthorized access has to be considered.

EN 50159 – Railway applications (2010 ed.)

A transmission system has the following fundamental safety services:

- Message authenticity
- Message integrity
- Message timeliness
- Message sequence

These services must be considered and provided to the extent needed for the application, for both open and closed systems.

EN 50159 – Railway applications (2010 ed.)

A transmission system can be subjected to the following **threats**:

- Repetition
- Deletion
- Insertion
- Re-sequence
- Corruption
- Delay
- Masquerade

The **threats** have the following **defenses**:

- Sequence number
- Time stamp
- Time-out
- Source and destination identifiers
- Feedback message
- Identification procedure
- Safety code
- Cryptographic techniques

EN 50159 – Railway applications (2010 ed.)

EN 50159 categories and security requirements:

Category 1 – Closed systems — **Need not consider security**

Systems under the control of the designer, and fixed during their lifetime.

Category 2 – Open systems

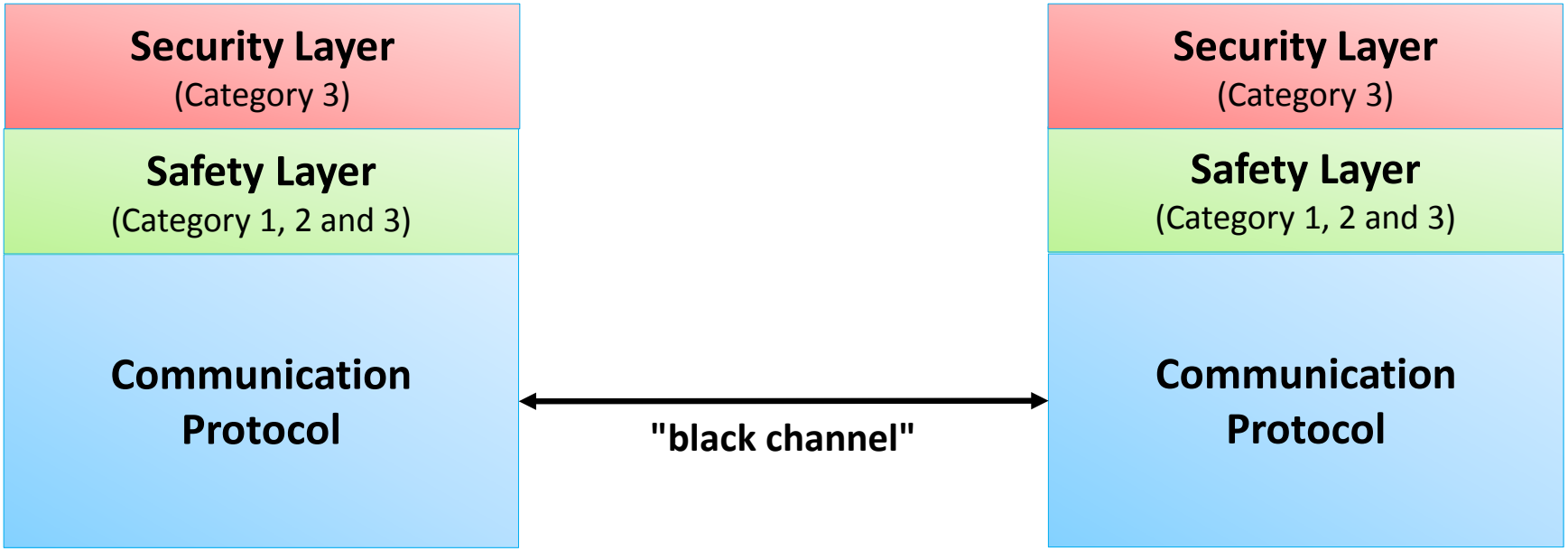
Systems partially unknown or not fixed, but unauthorized access can be excluded.

Category 3 – Open systems — **Must implement security mechanisms**

Systems which are not under the control of the designer, and unauthorized access has to be considered.

EN 50159 – Railway applications (2010 ed.)

EN 50159 introduces application level end-to-end safety and security:



IEC 61784-3: Functional safety fieldbuses (2016 ed.)

Security is not covered by IEC 61784-3, but the standard refers to:

- IEC 61784-4 for profile specific security mechanisms
- IEC 62443 for common security mechanisms

IEC 61784-3 defines the term "closed communication system", but not "open communication system".

The "security layer" is not covered by IEC 61784-3.

Traditional fieldbuses for safety can be considered closed systems, or open systems without unauthorized access.

Evolution of industrial communication

Phase 1: Dedicated wires — **Category 1**

One dedicated wire from control system to each individual field instrument.

Phase 2: Fieldbuses — **Category 1 or 2**

Multiple instruments connected to a single wire using fieldbus technologies.

Phase 3: Open and shared infrastructures — **Category 3**

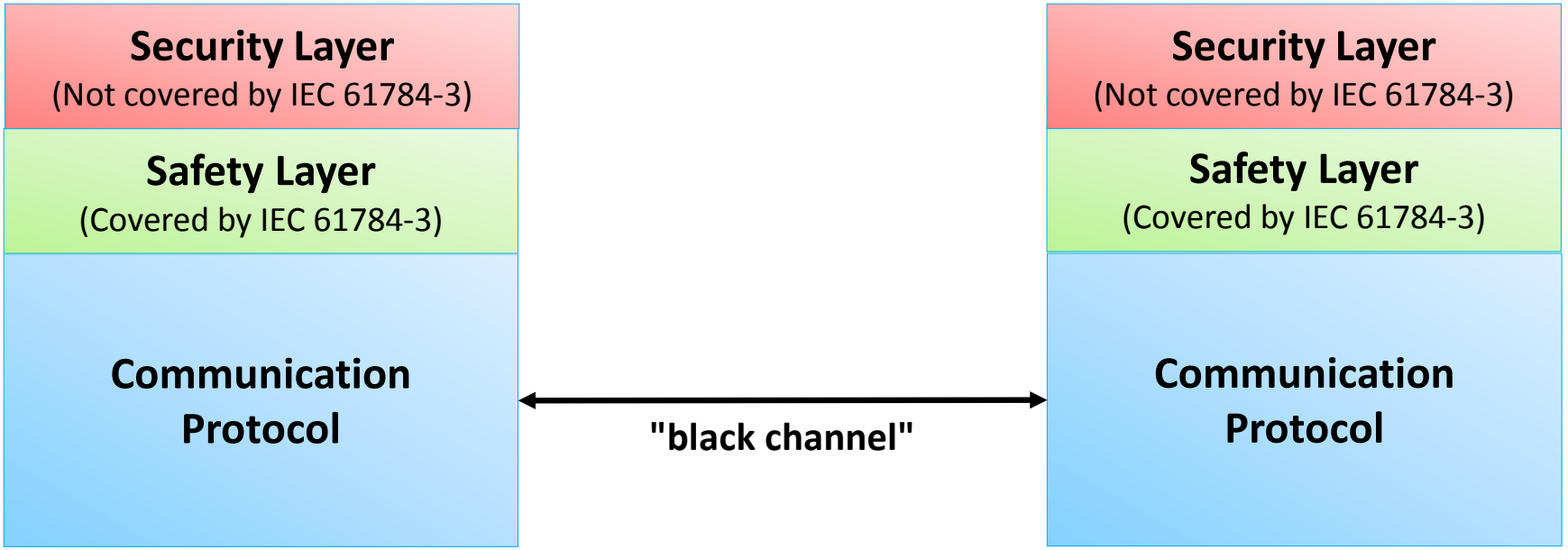
Transmission over open and/or shared systems, e.g. Ethernet.

This also includes transmission over wireless networks.

Category 3 transmission systems must implement security mechanisms.

IEC 61784-3: Functional safety fieldbuses (2016 ed.)

The move from closed, to open and shared transmission systems requires security mechanisms to be implemented.



Technology for a better society