



Network Communications

Henry Robertson

12GeV PSS Final Design Review

September 16/17, 2009

PROFIsafe

- First communications protocol to meet IEC 61508 that permits both standard and safety-related communications on one bus line
- Defined in IEC 61784-3-3 as an international standard
- PROFIsafe profile allows safe communications for the open standard buses PROFIBUS and PROFINET on the basis of standard network components
- In connection with PROFINET, PROFIsafe also supports fail-safe wireless communications via IWLAN

PROFIsafe - Safety Message Frame

- In safety mode, data are transmitted consistently between the F-CPU and F-I/O in a safety message frame. The safety message frame in accordance with PROFIsafe consists of the following:
 - Process data (user data)
 - Status byte/control byte (coordination data for safety mode)
 - Sequence number
 - CRC (Cyclic Redundancy Check) signature

PROFIsafe - Monitoring Time and Sequence Number

- The F-CPU assigns a sequence number to the F-I/O for time monitoring of the message frame update in the PROFIsafe protocol
- A valid, current safety message frame with a valid sequence number must be received by the F-CPU and the F-I/O within an assignable monitoring time.
- If a valid sequence number is not detected within the monitoring time, the F-I/O is “passivated”.

PROFIsafe - CRC Signature

- A CRC signature contained in the safety message frame protects the validity of the process data in the safety message frame, the accuracy of the assigned address references, and the safety-relevant parameters.
- If a CRC signature error occurs during communication between the F-CPU and F-I/O, e.g. due to intermittent electromagnetic interference, the F-I/O is “passivated”.

Network Security

- The security module (S612) protects individual components and entire networks against data theft and manipulation by implementing a firewall and a virtual private network (VPN).

Network Security - Firewall

- Protection of the internal network:
 - Only communication channels between devices from the external network and the internal network that are defined in advance are allowed
 - This is carried out by a packet filter working on layer 2 and 3 on the security module. The packet filter controls the communication between the internal network and the external network (see Figure 1).
- The firewall offers packet filtering:
 - Filter adapted from OpenBSD for IP-packets with stateful packet inspection
 - Filter for Non-IP-packets (Ethernet packets or Layer-2-packets) was developed by Siemens for the security module
- There is also a bandwidth limitation in order to avoid denial of service (DoS) attacks and cache flooding

Network Security - Firewall

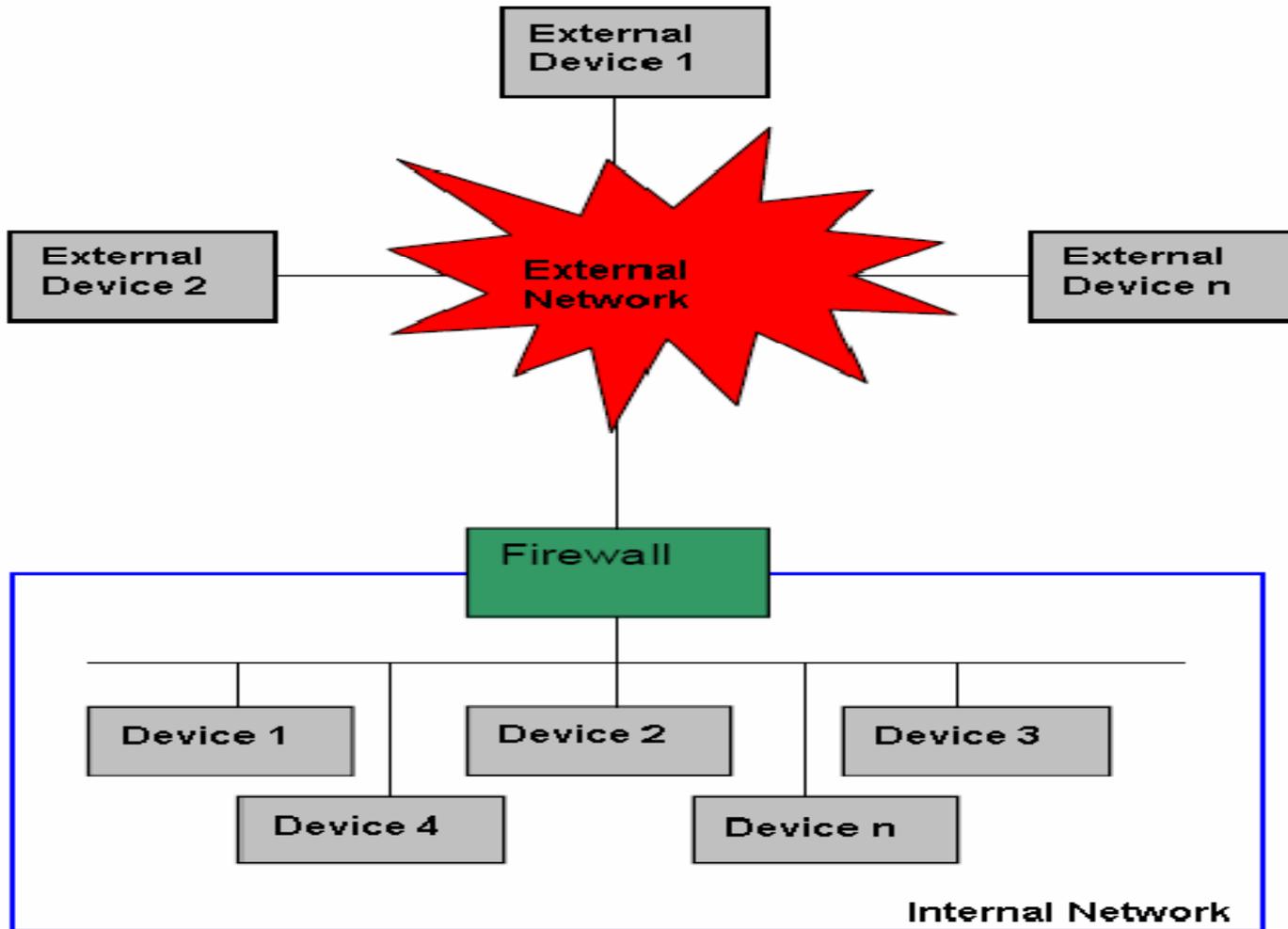


Figure 1: Firewall function of the security module

Network Security - VPN Tunneling

- The module also has the task to connect two or more networks to each other.
- This happens physically over the external network in such a way that messages from a protected device to another one are sent over the unprotected external network through a secure tunnel.
- In order to safeguard the confidentiality of the data, the security module can build up a VPN tunnel based on IPsec.
- When several bilateral tunnels are combined, the resulting network is called a VPN as represented in Figure 2.

Network Security - VPN Tunneling

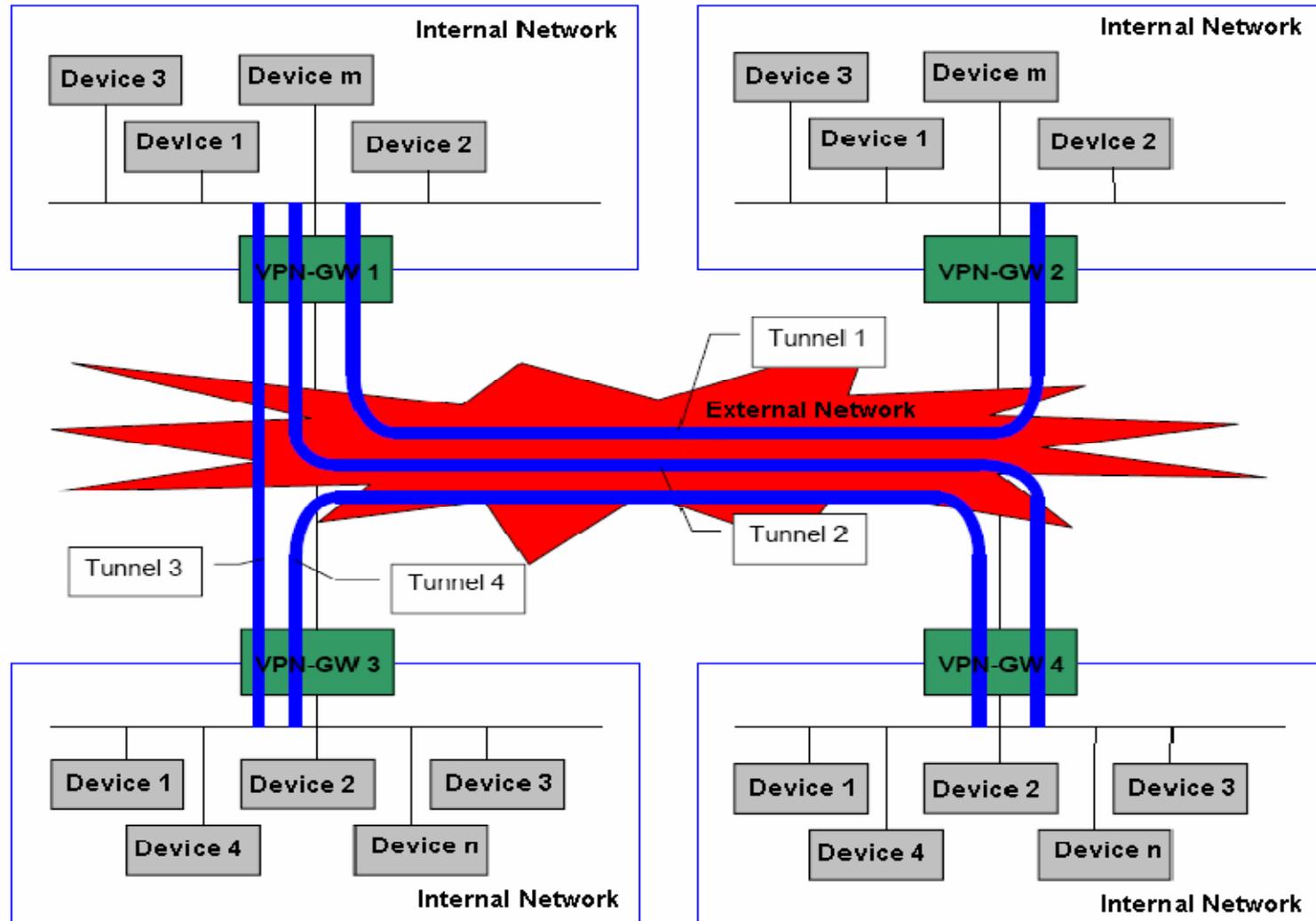


Figure x: VPN function of the security module

Network Security - VPN Tunneling

- For the communication over a VPN the security modules are collected in groups.
- For each VPN there is a so called network certificate with corresponding private key that identifies the VPN.
- Each security module that belongs to the VPN holds a certificate which is signed with the private key of the network certificate.
- The network certificate is issued by a certification authority (CA) or it is self issued.
- The VPNs are based on IPsec and use the IKE protocol for the key management. The implementation was adapted from OpenBSD.

Network Communications

Questions?