HoliSec

Holistic Approach to Improve Data Security

AUTOSAR Secure Onboard Communication
Goals and Reasoning Behind the Freshness Design

Presenter: Christian Sandberg

March 26, 2019

Background material: Christian Sandberg (Volvo Trucks), Thomas Rosenstatter (Chalmers)

VINNOVA FFI VOLVO VOLVO ARC CORE CHALMERS ASSURED SECURITY CONSULTANTS RI.SE Research Institutes of Sweden

Outline

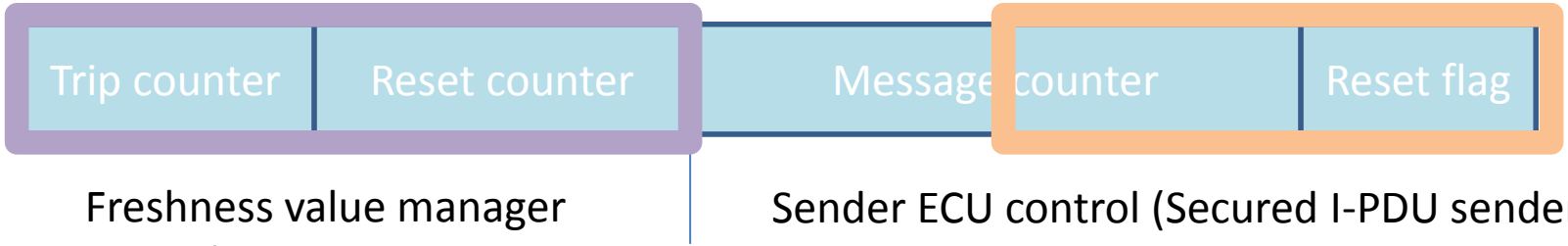
- **Industry requirements**
- **Overview of Security Profile 3**
- **Centralized vs decentralized freshness manager**
- **Periodic vs on-demand synchronization**
- **Data exchange**
- **Questions**

Industry Requirements (some of them)

- J1939 compliant (e.g. For CAN 8 byte frames, 29bit id...)
- Same algorithm for multi -protocol, e.g. CAN, Ethernet (aid gateway transparency)
- Avoid single-point-of-failure designs
- Consider resynch speed to quickly get communication running (e.g. following startup, sleep, or erroneous restart by a communicating party)
- ...

SecOC: Security Profile 3

- Introduces a Freshness Value Manager concept, FVM
  - Centralised as well as decentralized freshness manager (single/multi master)
- Provides frame definitions
  - CAN only
  - Missing Ethernet and dual CAN frame configuration



Sender ECU: Secured I-PDU (payload, both truncated freshness (Message Counter and Reset flag) & MAC)
FVM: TripResetSyncMessage (trip counter, reset counter) resets all Message Counters when transmitted (if centralized FVM is used)

Design decisions

On-demand resync

Periodic sync

Decentralized FVM

Centralized FVM

Information exchange

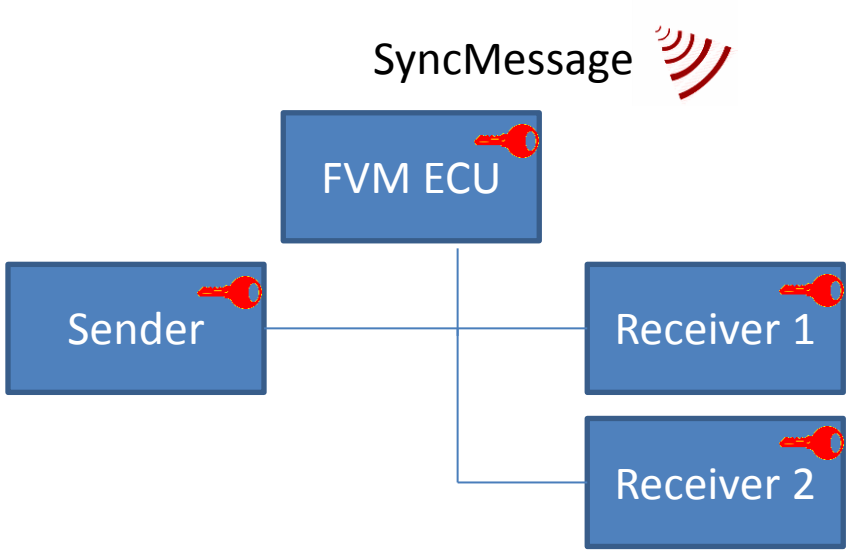
Centralized Freshness Value Manager

Pros

- Low bandwidth utilization from sync message
- Less strain on CAN ID pool utilization
- Lower footprint in RAM and NVM since the upper bits of 64 bits FV are managed centrally

Cons

- Single point of failure
  - Backup FVM + protocol needs to be arranged
- Same symmetric key in FVM ECU and all ECUs. Aids extraction by hacker to emulate FVM
- Needs to be located in an ECU that is always on



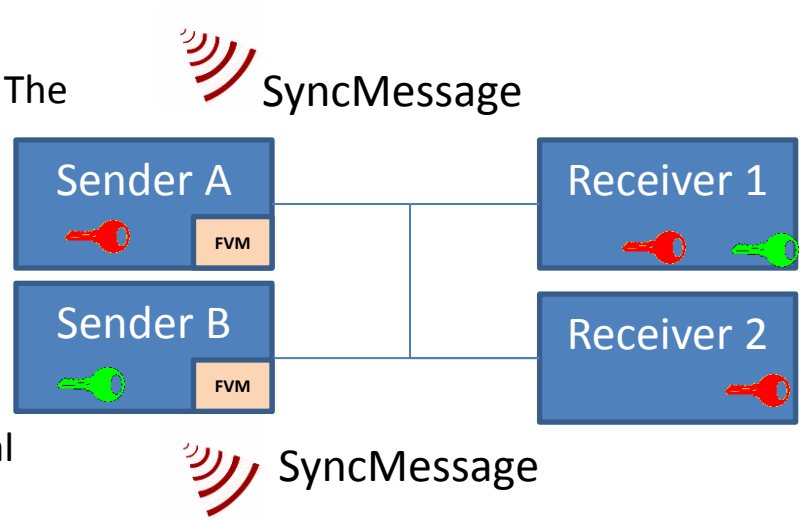
Decentralized Freshness Value Manager

Pros

- Less of a single point of failure for the entire vehicle. The problem remains on node level.
- Unique key per sender FVM + set of receivers
- Less need to locate an ”always on” -ECU

Cons

- More utilization of CAN id’s
- Higher resource (RAM, NVM) need to store individual freshness counters in Sender and Receiver

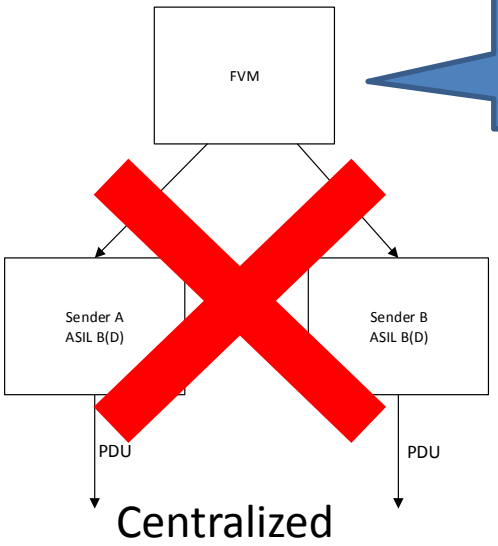


Example. *Receiver 1 is consumer of data from both Sender A and B, Receiver 2 only of Sender A*

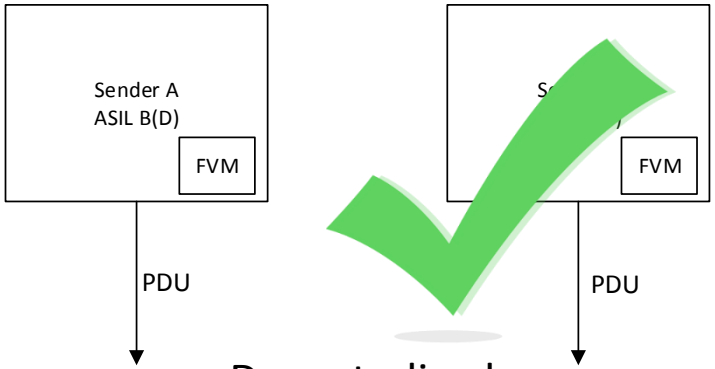
What about a functional safety viewpoint?

Assume ASIL D Item that needs redundancy

Would need multiple centralized FVM, who need to be synchronized and also send freshness data on different physical networks.



Centralized



Decentralized

Periodic SyncMessage or On-Request

Periodic

Pros

- Less CAN id utilization
- Less logic in the Sender/Receiver nodes

On request

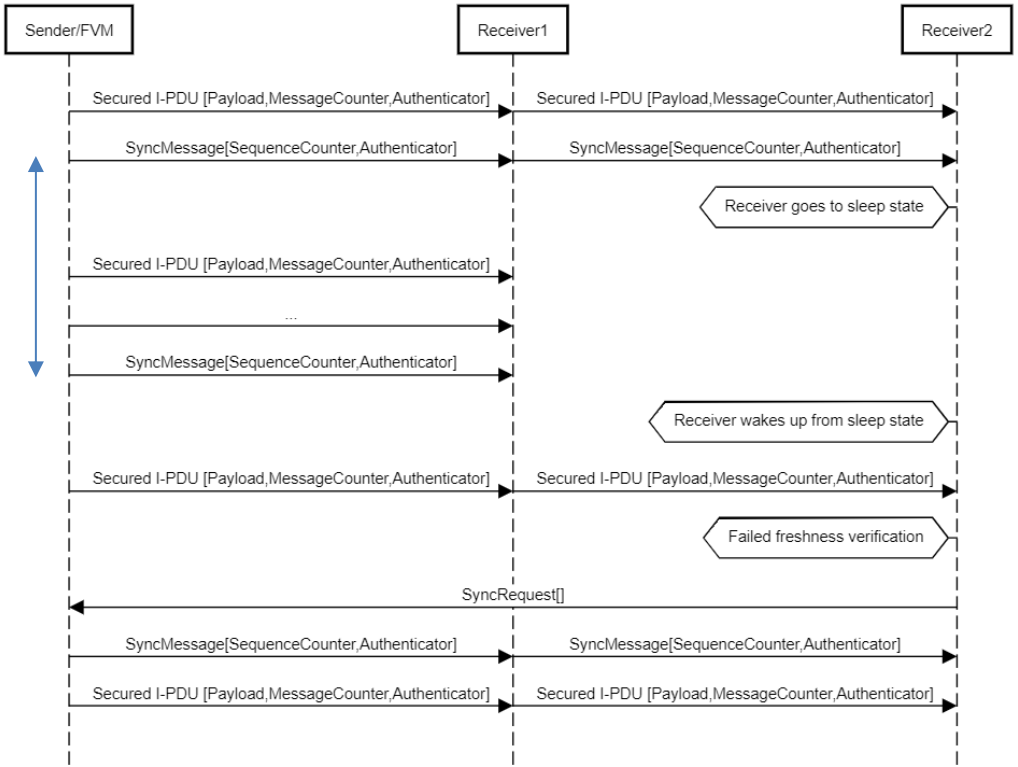
Pros

- Fast resync, order of tens of milliseconds

Sender ECU: Sends SynchMessage periodically and also when a Receiver requests it by using a SynchRequest message.

Receiver: Decides whether to wait for periodic resynch, or ask for resynch immediately

Data exchange



- Sender ECU is the freshness value manager
- Combination of periodic and on-demand resynch mechanism

HoliSec

Holistic Approach to Improve Data Security

Thank you for your attention!