A close-up photograph of a printed circuit board (PCB) with various electronic components, including gold-plated connectors, capacitors, and integrated circuits. The image is partially obscured by a white semi-circular shape that contains the text.

Streaming Data for a Safety Related Application in MOST150

Dr. Jens Chr. Lisner (TÜV NORD/IFM)

Dipl. Inf. (FH) Johannes Specht (TÜV NORD/IFM)

Frankfurt, March 23rd, 2010

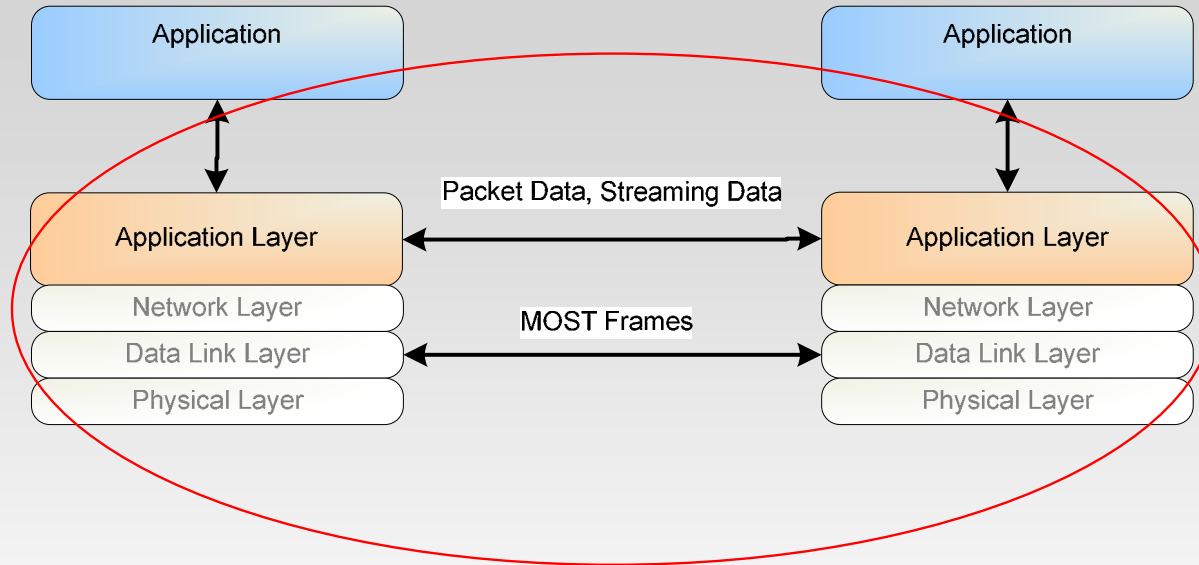
- Communication Engineering
 - FlexRay Conformance Test
 - FlexRay Interoperability Test
 - Automotive Network Tests for Validation and Optimization (VNVS)
 - Paper Studies (Parameterization, X-by-Wire Systems, Safety)
 - SW-Tools (e.g. FIBEX-Checker for ASAM and OEMs)
 - Physical Layer Modeling
 - ...
- Functional Safety
 - Hazard- and Risk Analysis
 - Safety Requirements Specification
 - Probabilistic SIL Verification
 - Safety Analysis (FMEDA, FTA, ...)
 - Seminars, Trainings, Workshops
 - Consortia Work:
 - VDA FAKRA FuSi (ISO 26262)
 - DKE 954 (IEC 61508 Rev2)
 - FlexRay, AUTOSAR, TTA Steer-by-Wire WG
 - ...

I	Goals
II	Fault-Model
III	Requirements for Concept
IV	Concept for a Safety Layer
V	Conclusions and Further Work

December 2008: Request by MOST Coop. for ...

- Analysis:
 - Can MOST150 be used for Safety-Critical Applications?
- Concepts:
 - Generic “Safety layer” for the MOST150 protocol
 - Including Control, Packet and Streaming Data Channel
 - Considering relevant Safety Standards

System to be regarded



Communication System:

- Electrical/Optical Physical Layer (Channel)
- INIC
- Higher layers of the protocol (SW)

not Part of this study: Applications (assumed to be fault-free)

Studies by TÜV NORD/IFM on behalf of the MOST Coop.

- **Pre-Study:**
 - Safety-related application possible with MOST150?
 - Yes: Safety Layer Concept
- **Streaming Data Study:**
 - Safety-related application using streaming data?
 - Safety Layer for streaming data
- **Control Channel and Connection Management:**
 - Safety-related application using the control channel?
 - (in progress)

Example application

“Camera-based parking” scenario

- Driver starts parking
- Camera streams live picture to the drivers’ dashboard
- E.g. Motion JPEG Video Stream

Safety relevance

- Missing, delayed or frozen pictures
 - Driver assumes free range behind car
 - Damaged objects and/or injured persons

Relevant Documents

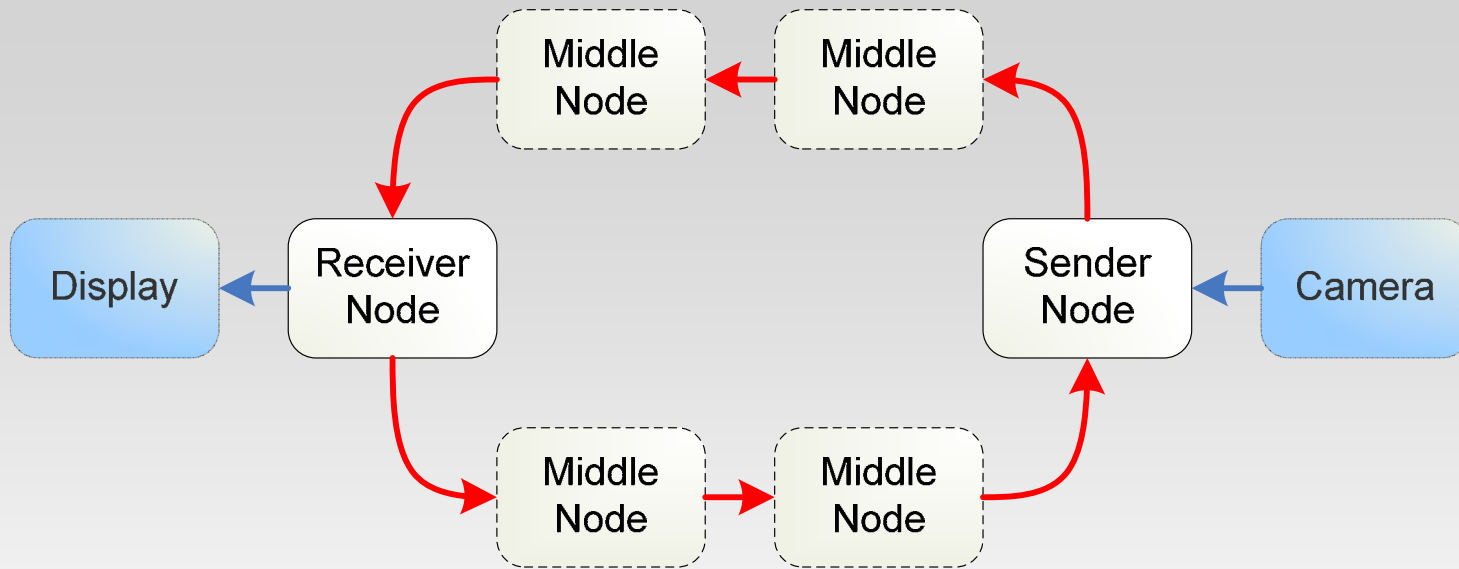
MOST

- MOST 3.0 Protocol Specification
- MOST 3.0 Stream Transmission Specification

Relevant Safety Standards

- ISO/IEC DIS 26262, refers to ...
 - IEC 61508
 - IEC 61784-3
 - IEC 62280-1

I	Goals
II	Fault-Model
III	Requirements for Concept
IV	Concept for a Safety Layer
V	Conclusions and Further Work



- Source (sender): Camera (FBlock) fault-free
- Sink (receiver): Display (FBlock) fault-free
- MOST150 nodes: MOST AL & INIC possibly faulty
- Channel: EPL/OPL possibly faulty

Fault-Model: Data Streams

- Application (multimedia) Stream
 - e.g. MPEG-Frames, JPEG-Pictures
 - Size depends on data format
 - Source: Camera
 - Sink: Display

- “Block Stream”
 - Encoded in MOST150 frame
 - Specific number of bytes reserved for block
 - “Messages”

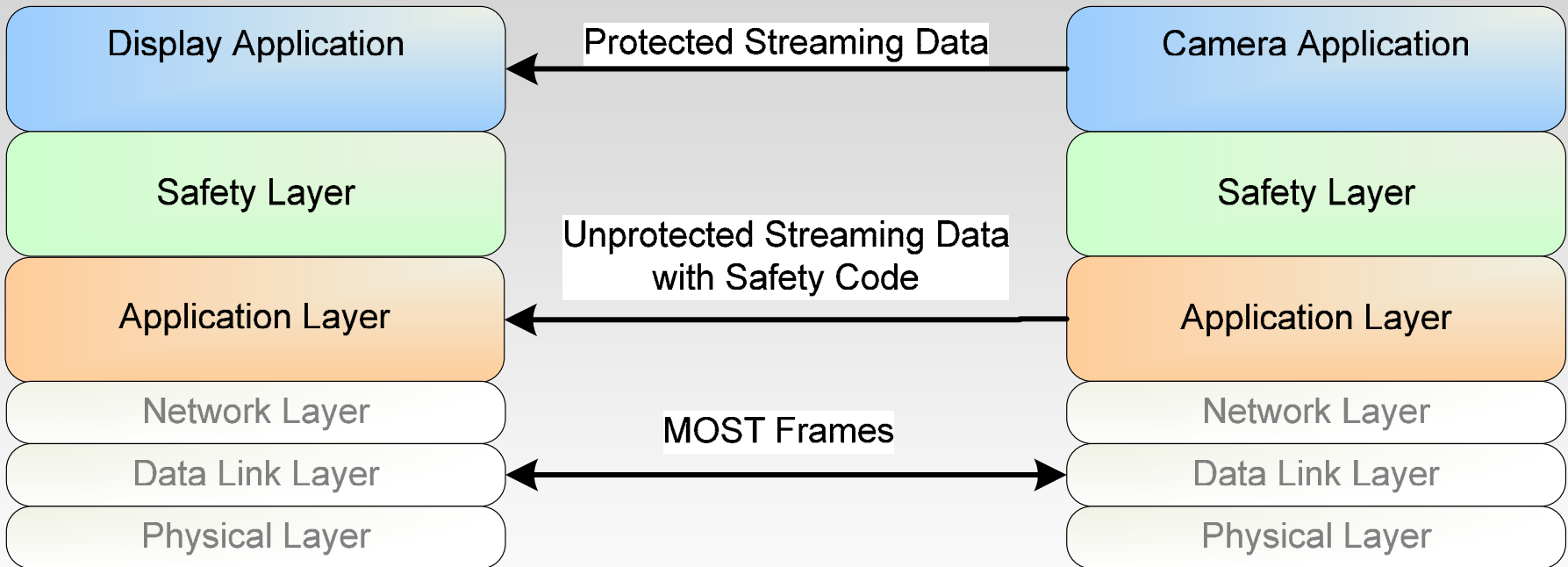
Fault-Model: Failures to be Regarded (Examples)

Failure	Example for Motion JPEG
Failure of Communication Peer	A power failure of a node.
Unintended Message Repetition	The camera node sends multiple copies of one picture.
Message Loss	A picture is lost during transmission.
Re-sequencing	The camera node sends multiple pictures in unintended order.
Message Corruption	A picture is changed by a middle node.
Message Delay	The INIC of the receiver node delivers a picture too late to the local host application.

I	Goals
II	Fault-Model
III	Requirements for Concept
IV	Concept for a Safety Layer
V	Conclusions and Further Work

- In case of an error:
 - System should go into a “safe” state:
 - Driver cannot rely on Camera-based Parking Assistant
 - Driver must be informed (Warning Signal)
 - Monitor should be switched off
 - Fail-Silent behavior
- ⇒ Error must be detected by Safety Layer
- Safety Layer assumed to be fault-free (not part of the protocol stack)

Safety layer is built on top of ALS



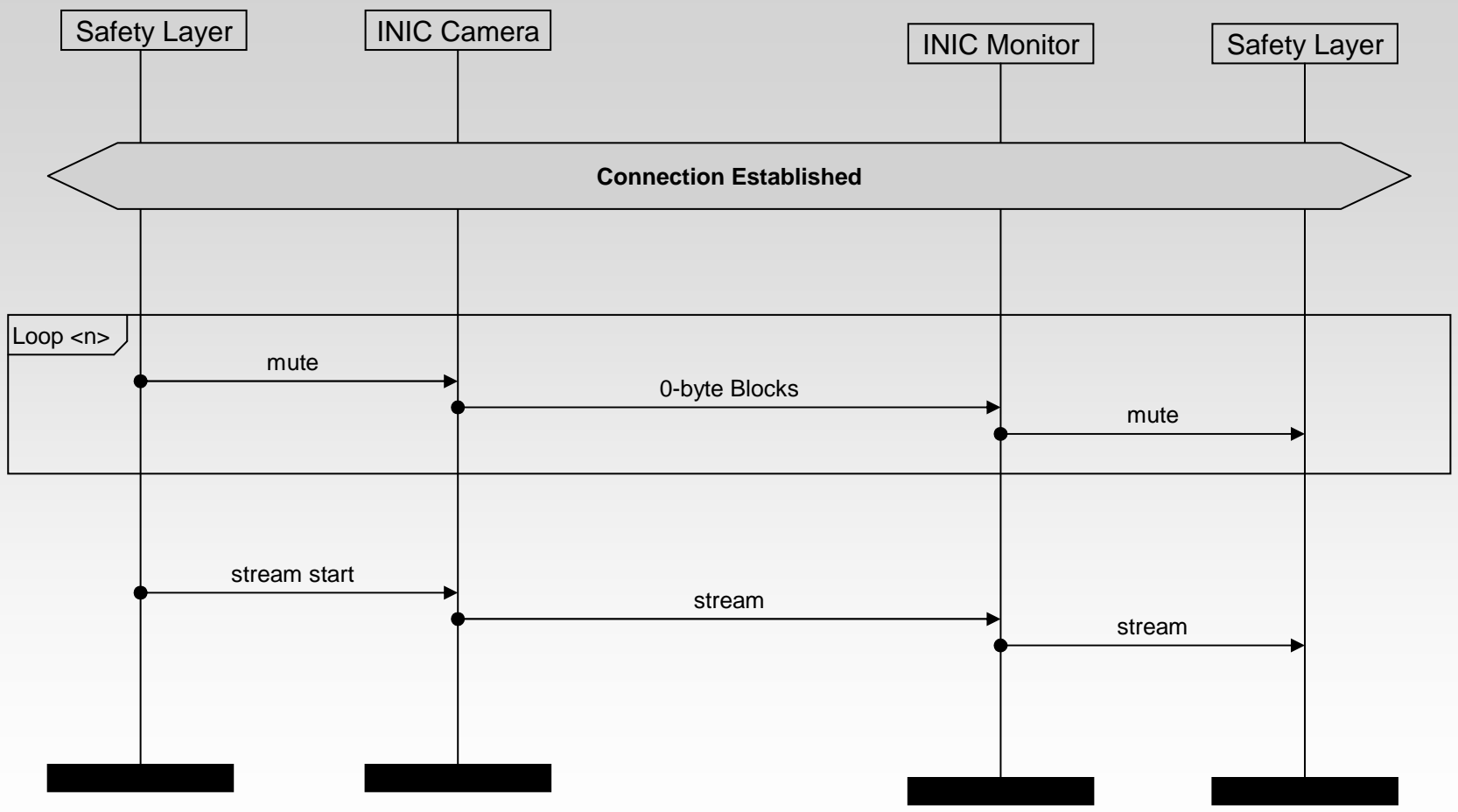
Requirements for Safety Concept: Requirements on Safety Codes

- Detection of ...
 - Bit Errors
 - Checksums (CRC, Cryptographic Signatures, ...)
 - Re-ordering/Insertion
 - Sequence counters

- Further measures ...
 - Timeouts
 - Length field or fixed image size (if possible)

I	Goals
II	Application Scenario
III	Fault-Model
IV	Requirements for Concept
V	Concept for a Safety Layer
VI	Conclusions and Further Work

Concept for a Safety Layer: Runtime Conventions



Concept for a Safety Layer: Integration of Safety Code in Streaming Data

- CRC
 - Requirements on CRC according to IEC 62280-1
 - Ethernet polynomial could be used (proven in use)
 - Cryptographic signatures should be considered
- Sequence Counter
 - Size depends on image rate
- Add safety code to blocks of fixed size
 - Fixed number of blocks per image (no length field)
 - Synchronous stream (no gaps)

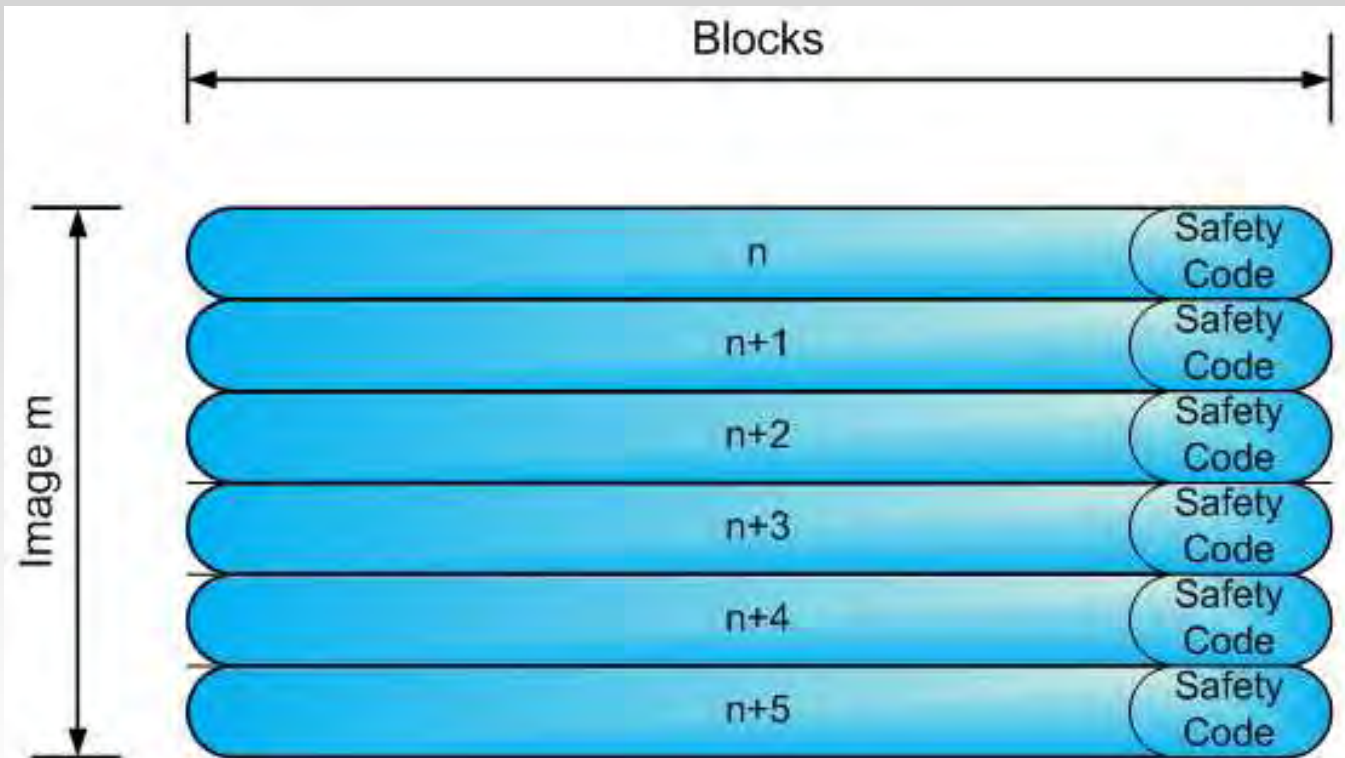
Concept for a Safety Layer: Integration of Safety Code in Streaming Data

Processing the safety code



Concept for a Safety Layer: Integration of Safety Code in Streaming Data

Embed safety code into separate blocks of data of fixed size



Concept for a Safety Layer: Integration of Safety Code in Streaming Data

Send safety code separately on the SAD channel



Concept for a Safety Layer: Monitoring of the Streaming Channel

- Stream start check
- Stream end check
 - Safety layer is able to detect repetitions or corrupted messages
- Timeout
- CRC
- Sequence counter

- INIC diagnostics?
 - If error reported “something is wrong” ...
 - Diagnostics not reliable (INIC may be faulty)

Concept for a Safety Layer: Measures in the Case of Errors

- Forward recovery into safe state
- Camera side
 - Safety layer signals an error
 - Camera should stop streaming
- Monitor side
 - Safety layer should report application
 - Application should display a warning

Summary:

- The CBP application is safety related
- It is possible to implement safety layer for CBP
- Assumptions
 - Simple data format
 - Synchronous stream
 - Connection management not part of safety related operation
- In case of errors
 - Safety related operation stops
 - Forward recovery
- Safety layer respects ISO CD 26262 requirements
- Safety integrity level up to SIL 3 may be possible

Future Projects:



- Prototypic Implementation of small subset
- Packet Channel Analysis
- MOST infrastructure
 - Network Management
 - Power Management
 - Influence of (one or more) Timing Masters
- Quantitative Analysis
- Empirical Analysis (e.g. fault injection)