



Definitely safe

MOST150 for safety related applications

This paper presents an analysis which discusses the possibility to implement safety related applications using the MOST150 protocol respecting current and forthcoming safety standards, especially the current draft of the ISO 26262 standard for safety in the automotive field. A safety layer provides safe communication over a MOST network using safety codes.

By Dr. Jens Lisner and Johannes Specht

Today, MOST is widely used for multimedia applications in the automotive field. It might be possible to use MOST for safety critical applications. In this application domain, communication faults become a serious issue since they can severely damage objects or even injure persons.

On behalf of the MOST Cooperation TÜV Nord/IFM has investigated which measures have to be taken in order to fulfill the requirements of the forthcoming safety standard for the automotive industry ISO 26262, which also respects necessary requirements of current standards, e.g. IEC 61508 [5, 6, 7].

As a solution, an architecture with a safety layer as basis for safety related applications has been proposed [3, 4]. The safety layer provides a dependable service for the transmission of safety related application data over a MOST network.

■ Example parking system

A camera-based parking system (CBP), as already found in modern automobiles, can be considered as a safety related application. A live picture of the rear view of the car is captured by a camera, digitized and transmitted to a display in the dashboard.

The transmission could be a Motion JPEG video stream as delivered by several low-cost cameras.

From a safety point of view, several failures like missing, delayed or frozen pictures could cause hazards. In case of frozen pictures, for example, the driver could assume a free range behind the vehicle and reverses despite of an obstacle or even person. Relying on this information could lead to damaged objects or injured persons. It is essential to detect such failures reliably in order to warn the driver that the displayed data is no longer valid.

Considering MOST in this example application, the underlying network can be subdivided as shown in **figure 1**:

► Sender: The sender is a single node of the network. It is connected to the camera and executes a host application. The host application sends the camera data via the local MOST INIC (Intelligent Network Interface Controller) to the remaining network.

► Receiver: The receiver is a second single node of the network, e.g. the HMI (Human Machine Interface), which receives the camera data for the local connected display.

▶ **Middle nodes:** Since MOST uses a ring topology, additional nodes between the sender and the receiver may exist. The communication between sender and receiver is forwarded by these nodes.

▶ **Channel:** The channel connects the previously described nodes. An electrical or optical physical layer can be used.

Within the network, multiple potential sources of errors exist. The most obvious source is the channel, which can introduce bit errors e.g. caused by EMI, especially when an electrical physical layer is used.

Moreover, all nodes, including the middle nodes, are a potential source of errors that must not be underestimated. Each INIC for example, has the potential to harm the network traffic during forwarding, drop data between the local host application and the remaining network or to introduce malicious transmissions on the chan-

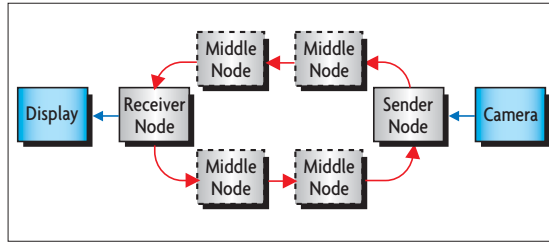


Figure 1. MOST network with sender, receiver and middle nodes.

nel. Although MOST includes error detection mechanisms, these mechanisms are in general realized in the INIC itself. Thus, the protocol is not able to reliably detect several communication failures.

■ About the ISO DIS 26262

TÜV Nord/IFM considered the requirements of the forthcoming ISO 26262 standard [3] [4]. It defines methods, proceedings, activities and constraints during design, development and operation of safety critical electrical and electronics systems.

As part of this, various abstract failures of communication systems are introduced that must be taken into account for safety related systems. These failures do not address a specific ISO / OSI layer. In-

stead, they rather describe failures during logical message transmission between different communication peers. For simplicity, a single Motion JPEG picture of the CBP system can be considered as one message, where a sequence of messages assembles a video. The **table** shows a subset of the failures and gives examples with respect to this message representation.

Of special interest for safety critical applications is the residual error rate, since this error rate must not exceed a certain threshold to reach the required Automotive Safety Integrity Level (ASIL).

■ MOST and the safety layer concept

An additional safety layer between the application and the INIC can provide the necessary protection. Figure 2 shows the MOST protocol stack including a safety layer and the CBP system host applications on top. The safety layer provides safe virtual communication services on top of the MOST application layer as defined in [1].

A standard technique in the safety domain to reach a high degree of fail-

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.

! Examples of communication failures, taken from the ISO 26262.

ure detection is the use of specific safety codes, which are embedded into the payload. Each safety code stores additional information, e.g. CRCs or sequence counters. The safety codes are introduced by the safety layer on the sender side and are analyzed on the receiver side. By this, the receiver's safety layer can reliably detect several failures in the incoming transmissions and execute a suitable reaction (e.g. indicate the error to the application).

The safety layer architecture in figure 2 uses the MOST application layer exclusively. Thus, safety codes must be transferred using existing interfaces of the protocol. For streaming data, a variety of possibilities can be considered, ranging from direct integration of safety codes into streams to transfer of the safety codes via the SAD channel (Stream Associated Data) which is otherwise used for content protection of multimedia streams [2].

■ Safety layer example for streams

For the given example, even simple measures on a safety layer allow detection of typical failures as described in the Table:

▶ **CRC (Cyclic Redundancy Check):** Both, the Motion JPEG picture as well as the safety code itself can be protected with additional CRCs. By this additional CRC, message corruptions caused by the channel or even by the INICs can be detected.

▶ **Sequence counter:** Sequence counters in the safety code are a typical measure to detect resequencing, message loss or unintended message repetition.

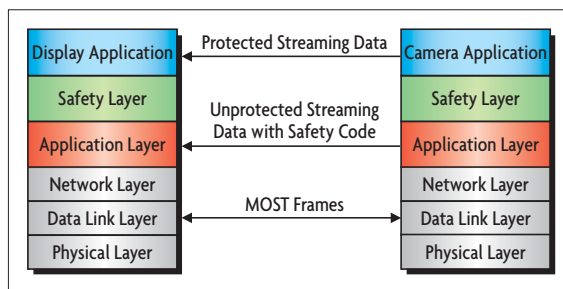
▶ **Message length:** Transferring the message length in a safety code gives the opportunity to check if a message is incomplete,

even without knowing details of the media format, i.e. Motion JPEG in this example.

▶ **Timeouts:** Besides safety codes, additional timeouts can be used to detect failures of a communication peer during streaming or delayed messages.

Going into more detail, additional MOST specific safety measures have been proposed in the study like stream start- and stream end-markers to detect more sophisticated failures than described herein [4]. The next goal is the reliable transmission of control protocol messages and the remaining core mechanisms of the protocol.

Quantitative analyses can be done to estimate the residual failure rates



! Figure 2. The safety layer architecture of the MOST protocol stack in the CBP system.

and to determine the required strength of safety codes, e.g. the strength of additional CRCs to reach a desired ASIL. The results of such an analysis can be proven by hardware testing results. sj

Literature

- [1] MOST Specification Rev. 3.0. MOST Cooperation. 2008.
- [2] MOST Specification for Stream Transmission Rev. 3.0 Draft. MOST Cooperation. 2008.
- [3] Report for the Pre-Study MOST Technology for Safety related Applications. TÜV Nord/IFM. 2009.
- [4] Streaming Data for a Safety-Related Application with MOST 3.0. TÜV Nord/IFM. 2009.
- [5] ISO DIS 26262, Road vehicles – Functional safety; Part 6: Product development: software level. International Organization for Standardization (ISO). 2009.
- [6] IEC 61508: Functional Safety of E/E/PE safety-related systems Part1-Part7. 1st Ed. 1998 – 2005.
- [7] IEC 61784-3: Industrial communication networks – Profiles Part 3: Functional safety fieldbuses. 2007.



Dr. Jens Lisner

is working in the area of Communication Engineering in the department Elektronik & IT of TÜV Nord/IFM.



Dipl.-Inf.(FH) Johannes Specht

is working in the area of Communication Engineering in the department Elektronik & IT of TÜV Nord/IFM.