

Timing master faults

Every master (network, connection, power, and timing) in a MOST network can be a potential single point of failure. The Timing Master (TM) mostly is suited inside the Head-Unit. It is a crucial component in such a network, since it is responsible for the network start, generation of MOST frames and system clock. In this work, we identify several faults within a TM which can cause unexpected and unwanted system behavior, e.g. the TM being a prerequisite of a valid ring break diagnosis [1], data-dependent jitters, wrong Synchronous Bandwidth Control (SBC) register or boundary values and faulty S/PDIF inputs. This is important, since MOST is also used for safety-relevant systems such as a park assist. Based on a fault model for networked embedded systems, the article identifies potential faults and shows how these can be tolerated.

A master in a MOST network can be a potential single point of failure. Usually the Network and Timing Master (TM) reside in one node. The TM provides the system clock. Every node within a MOST system is synchronizing to this signal. A MOST network therefore is a synchronous network. The TM is always node zero (InstID 0x00, address 0x400, logical 0x100) in the ring. The MOST network topology is logically a ring, but can be extended by using a hub to e.g. a ring-star topology, where nodes can be deleted and inserted without disturbing the operation of the ring. As it is widely used in the automotive industry, we consider faults within a system consisting of a single TM. Here, five different non-systematic. As network fault model, the basic fault model from [7] for basic networked embedded systems is used. Here, five different effects can be listed: LOST (LO, packet lost), CORRUPT (CO, bits of the transmitted packet flipped), CUT (CU, bits of the transmitted packet lost), DUPLICATE (DU, packet was sent twice) and CARRIER (CA, no network function). The remaining of

Analysis and cure of timing master faults

This article regards the main application scenario for the automotive sector, a single timing master within a MOST network. Based on a five-effect network fault model for embedded systems and non-systematic faults, the article clarifies which fault effects related to the TM will lead to an unavailable network or faulty communication. Furthermore the article verifies how fault-tolerance mechanisms provided by the protocol can help to detect the most obvious faults.

From Bernhard Fechner

this article is organized as follows: firstly, the issues with single timing masters are discussed followed by a conclusion.

■ Timing master faults

The TM mostly resides in the head-unit [2]. It is a crucial component, because it is responsible for the network start, the generation of MOST frames and for the system clock. **Figure 1** shows the setup for a MOST25 frame (for MOST150 see [1]) exemplarily.

A MOST network consists of up to 64 PnP-nodes. Each node has a RX- and TX-port. One block has 16 data frames (512 bit MOST25, 1024 bit MOST50, 3072 bit MOST150). The first eight bits of each frame are the preamble and the boundary descriptor (BD). The preamble indicates the start of a frame and enables re-synchronization to the incoming data stream. The start of a block is marked with a different preamble. The boundary descriptor divides the data into a synchronous (multiple of four, minimum 24 bytes) and asynchronous (maxi-

mum 36 bytes) part. **Figure 2** illustrates the flow of frames within a multiple-node MOST network. The data and the control frame are secured by a CRC, whereas [1] does not give a hint, which polynomials are used, nor which areas of a frame are included in the parity calculation. In that case, preamble, BD and frame control are assumed. Within the following sections some of the most important TM functions and failures are discussed.

Initialization / system lock

When entering state NetInterface-Init, the TM clears the System Lock Flag (SLF) on the data link layer. This value is transferred to all MOST Net-

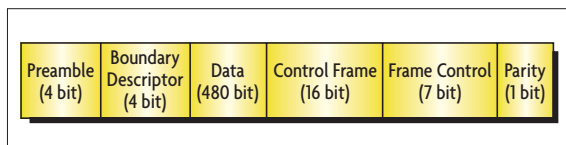


Figure 1. A MOST25 frame.

work Interface Controllers (NICs). As soon as the TM recognizes a stable lock, it sets the SLF. The state is left on one of the events InitReady or InitErrorShutdown (CA). InitReady is issued, if a stable lock was recognized by the TM. If the SLF is accidentally set or reset, it will be recognized by the parity bit, if no other bit is faulty.

SBC / BD

With the help of the BD, a synchronous and asynchronous bandwidth range can be specified in multiples of four (in bytes). The bandwidth can therefore be adjusted to actual demands. The value of the BD is between six and 15. The register (SBC) is administrated by the NIC of the TM. During the first part of the initialization phase, disturbances can occur. The master will set the SBC to a value less than six (usually four), which is invalid during normal operation. The value of the SBC is distributed to all nodes and then set to a value indicating normal operation.

The change is detected by other nodes in the system and signaled over the event Net_On to the application. A change of the SBC by the TM will lead

to a re-establishing of synchronous communication. A (faulty) toggling of the SBC will therefore lead to a breakdown of synchronous communication (CA). The SBC register as well as the SLF should be protected by a parity bit. Additionally, logic constraints should be introduced to omit the unwanted toggling of the SBC.

Preamble / oscillator

The preamble is generated based on the oscillator input or by the S/PDIF input signal of the TM. All Timing Slaves (TS) synchronize with a PLL on the system clock. The TM receives the frame again after passing the last TS. Since the phase is shifted due to

the signal runtimes of each MOST node, it restores the original frame with its PLL and creates the next frame. There can be three potential fault sources –

the oscillator, a faulty S/PDIF signal and bit-flips in the preamble.

A faulty oscillator or S/PDIF can lead to a false lock/unlock and therefore to the fault effects CU, CO and LO (as well as preamble bit-flips). From the specification [1] it is unclear how the preamble should look like. A single fault can be detected by parity.

Lock / unlock, shutdown flag

A TS is in the state lock, if it receives a signal at its input that its PLL can synchronize on. Otherwise, it will go to the state unlock [1]. If a MOST node can synchronize on the signal to minimum 100 ms, we have a stable lock (assuming that in time t_{lock} no unlock events occurred), otherwise a short lock. If the TM detects a stable lock, it is assumed that the whole network is stable. The TM is in the state lock if it can recreate the sent frame from the received one (naturally, all TS are locked in this case).

A failing TM will probably cause an unlock of a succeeding node (LO). This causes the detecting node to send a frame with a shutdown flag set, causing an (unintended) network shutdown (CA). This is also true if the

shutdown flag is set accidentally (CA). However, this fault can be detected through parity. The lock state on MOST25 or MOST150 assumes that the light is switched on. Naturally, the network cannot start, if the light is not switched on (CA, see total system failures).

Random frames

A non-conformant oscillator frequency could lead to the generation of cut or corrupt frames (LO, CO, CU), as well as a faulty frame generation logic. Additionally, there can be the case of a babbling idiot, frames generated randomly or corrupt (DU, CO, CU). DU is difficult to detect since the MOST protocol does not directly support sequence numbers. CO and CU frames can be detected through the CRC within the data section. All CO and CU frames where the CRC is not influenced can be detected by the parity, in case that there are no double faults.

Total system failures

With a ring-like topology a single break will cause a total system failure (LO, CA). A ring break can e.g. be caused through a defect control unit or a break within the optical fiber. For high availability, the ring can be extended with simple means (multiple RXs, TXs, wiring) to an n-modular redundant ring, whereas a double-ring structure is the most common means against ring breaks [3] certified with [4, 5]. In case of a ring-break diagnosis all devices must issue light on. Afterwards every device is asked if it received light on. This can be accomplished since MOST control units have a single-wire interface [6] besides the optical interface. Therefore, a

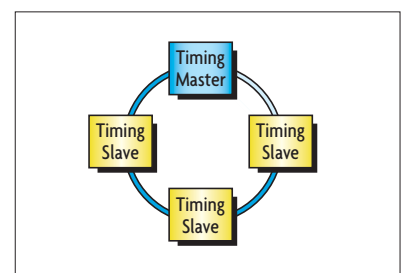


Figure 2. Timing master and slaves.

defective ring segment can be localized.

A MOST node has a bypass (in the NIC between fiber-optic receiver and transmitter), which can be used if the node is in low-power mode. In case of a node failure, the transceiver will switch to low-power mode without influencing the network function. On a short lock or an InitErrorShutdown, the bypass will be deactivated. The most obvious case of a complete failure is the failing of the light source (CA) or a permanent failure of the TM. On a sudden signal off (SSO), the Shutdown-flag is set and the detecting device as well as the designated TM store the cause of the fault (MOST150, SSO or CU – critical unlock, see [1]) and an emergency shutdown will be conducted. Here, the only means to tolerate the fault is redundancy.

In case of a non-designated TM, an AllSlaveNetwork will be initiated to enable a (valid) ring break diagnosis. However, if the number of designated TMs is not equal to one (All Slave, MultiMaster see [1]) or a valid relative node position is not available, a diagnosis error will be signaled and a shutdown initiated.

■ Jitter

The jitter-amounts data dependent-jitter (DDJ) and uncorrelated jitter [2] can accumulate so that the TM is not able to reconstruct the signal and cannot synchronize if the signal is outside the master-jitter tolerance, resulting in lock-errors (LO). High-frequent DDJ will be limited by PLL; low-frequent DDJ will be forwarded. To measure DDJ, a pattern is used which changes between the lowest (0x00) and highest (0xff) value. For efficient analysis and fault simulation, timing faults such as DDJ can be injected by the use of FPGAs [8].

■ Conclusion

There are several protocol and implementation enhancements possible. Some points are unclear, because the author did not have access to a TM/MOST implementation. That's why neither the polynomials used for CRC nor which sections are secured

by parity are specified, furthermore, if and which internal registers are secured by parity. Therefore it is assumed that every bit outside the data and control blocks is protected. *bg*

Literature

- [1] MOST Cooperation: MOST Specification Rev. 3.0, May 2008.
- [2] *Grzempa, A.*: MOST – Das Multimedia-Bussystem für den Einsatz im Automobil, based on MOST spec. 2.4, Franzis, ISBN-13: 978-3-7723-4149-6, 2007.
- [3] http://bosch-sicherheitsprodukte.de/content/language1/html/1611_DEU_XHTML.asp, checked 12/01/09
- [4] DIN EN 60849: VDE 0828-1. Elektroakustische Notfallwarnsysteme (IEC 60849:1998); Deutsche Fassung EN 60849:1998, 1998.
- [5] BS 5839-8:2008: Fire detection and fire alarm systems for buildings. Code of practice for the design, installation, commissioning and maintenance of voice alarm systems, 2008.
- [6] *Zimmermann, W.; Schmidgall, R.*: Bussysteme in der Fahrzeugtechnik – Protokolle und Standards. Vieweg+Teubner, 3rd edition, ISBN 978-3-8348-0447-1, 2008.
- [7] *Fummi, F.; Quaglia D.; Stefanni, F.*: Network Fault Model for Dependability Assessment of Networked Embedded Systems, pp. 54 – 62, 2008. IEEE International Symposium on Defect and Fault Tolerance of VLSI Systems, 2008.
- [8] *Fechner, B.*: Dynamic delay-fault injection for reconfigurable hardware. In Proc. 10th IEEE Workshop on Dependable Parallel, Distributed and Network-Centric Systems, 2005.



Bernhard Fechner

has an accident insurance education and received a Master and PhD in computer science, both from the University of Hagen. He worked several years as a consultant. His research interests include hard- and software design and analysis of (fault-tolerant) architectures and protocols.