



(Foto: Bosch)

Mit Sicherheit

Heutzutage wird MOST hauptsächlich für Multimedia-Anwendungen im Automobil eingesetzt. Eventuell ist es auch möglich, MOST für sicherheitskritische Anwendungen zu verwenden. In diesem Einsatzgebiet werden Kommunikationsfehler zu einem ernstem Problem, da durch sie Gegenstände oder sogar Personen schwer gefährdet werden können. Im Auftrag der MOST Cooperation hat der TÜV Nord/IFM untersucht, welche Maßnahmen ergriffen werden müssen, um die Anforderungen des kommenden Sicherheitsstandards für die Automobilindustrie ISO 26262 zu erfüllen, die auch bestehende Normen, z.B. IEC 61508 und ähnliche berücksichtigt [5, 6, 7].

Als Lösung wurde eine Architektur mit einer zusätzlichen Sicherheitsschicht als Basis für sicherheitskritische Anwendungen vorgeschlagen [3, 4]. Die Sicherheitsschicht stellt einen zuverlässigen Dienst für die Übertragung sicherheitskritischer Anwendungsdaten über das MOST-Netzwerk zur Verfügung.

▣ Beispielanwendung Parksystem

Ein kamerabasiertes Parksystem (camera-based parking; CBP), das bereits

MOST150 für sicherheitskritische Anwendungen

Dieser Artikel analysiert die Möglichkeit, sicherheitskritische Anwendungen mit Hilfe des MOST150-Protokolls zu implementieren, wobei gängige und künftige Sicherheitsnormen berücksichtigt werden. Dies betrifft im Besonderen den aktuellen Entwurf der Norm ISO 26262 für Sicherheit im automobilen Einsatz. Eine zusätzliche Sicherheitsschicht stellt die sichere Kommunikation über ein MOST-Netzwerk unter Verwendung von Sicherheits-Codes bereit.

Von Dr. Jens Lisner und Johannes Specht

in modernen Automobilen zu finden ist, kann als sicherheitskritische Anwendung betrachtet werden. Eine Kamera sendet ein digitales Live-Bild der Rückwärtssicht des Fahrers an eine Anzeige im Armaturenbrett. Als Format wäre z.B. ein Motion-JPEG-Video-Stream möglich, wie es von preisgünstigen Kameras geliefert wird. Fehler wie fehlende, verzögerte oder eingefrorene Bilder können Gefährdungen verursachen. Im Falle von eingefrorenen Bildern beispielsweise könnte der Fahrer eine freie Fläche hinter dem Fahrzeug vermuten und trotz eines hinter dem Fahrzeug befindlichen Hindernisses rückwärts fahren. Sachbeschädigungen oder sogar

verletzte Personen können die Folge sein. Daher ist es notwendig, solche Fehler zuverlässig zu erkennen, um den Fahrer zu warnen, dass die angezeigten Daten nicht mehr zuverlässig sind.

In dieser Beispielapplikation kann das zugrunde liegende MOST-Netzwerk wie in Bild 1 unterteilt werden. **► Sender:** Der Sender ist ein einzelner Knoten im Netzwerk. Er ist mit der Kamera verbunden und führt den für die Kamera zuständigen Teil der Host-Anwendung aus. Die Host-Anwendung sendet die Kameradaten über den lokalen MOST-INIC (Intelligent Network Interface Controller) in das Netzwerk.

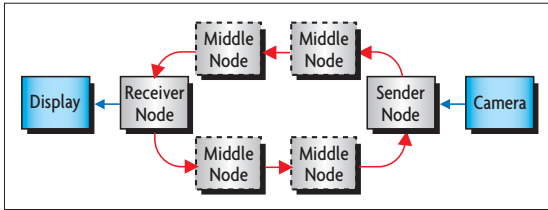


Bild 1. MOST-Netzwerk mit Sender, Empfänger und mittleren Knoten.

- ▶ Empfänger: Der Empfänger ist ein zweiter, einzelner Knoten des Netzes, z.B. die HMI (Human-Machine Interface), der die Kameradaten für das lokal angeschlossene Display empfängt.
- ▶ Mittlere Knoten: Da MOST eine Ringtopologie verwendet, können zusätzliche Knoten zwischen Sender und Empfänger existieren. Die Kommunikation zwischen Sender und Empfänger wird durch diese Knoten weitergeleitet.
- ▶ Kanal: Der Kanal verbindet die oben beschriebenen Knoten. Es kann eine elektrische oder optische physikalische Schicht eingesetzt werden.

Innerhalb des Netzes gibt es viele potentielle Fehlerquellen. Auf dem Kanal kann es zu Bit-Fehlern kommen, z.B. durch elektromagnetische Interferenz (EMI). Außerdem sind alle Knoten, einschließlich der mittleren Knoten, potentielle Fehlerquellen, die nicht unterschätzt werden dürfen. Ein INIC kann zum Beispiel Nachrichten bei der Weiterleitung in den Ring stören, Nachrichten zwischen lokaler Host-Anwendung und dem Netzwerk unterschlagen oder fehlerhafte Nachrichten auf den Kanal senden. Obwohl MOST Fehlererkennungsmechanismen hat, werden diese Mechanismen im INIC selbst realisiert. Im Falle eines INIC-Fehlers ist das Protokoll deshalb nicht in der Lage, Übertragungs-

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.

Bild 1. Beispiele aus der ISO 26262 für Fehlverhalten

fehler zuverlässig zu entdecken.

Über die ISO DIS 26262

Für die Analyse hat TÜV Nord/IFM die Anforderungen des kommenden Standards ISO 26262 zugrunde gelegt [3, 4]. Der Standard definiert Methoden, Vorgehensweisen, Maßnahmen und eventuell notwendige Einschränkungen während des Entwurfs, der Entwicklung und des Betriebs sicherheitskritischer elektrischer und elektronischer Systeme. Der Standard benennt verschiedene abstrakte Fehler-szenarien in Nachrichtensystemen, die für sicherheitskritische Systeme betrachtet werden müssen. Diese beziehen sich auf keine spezifische Schicht

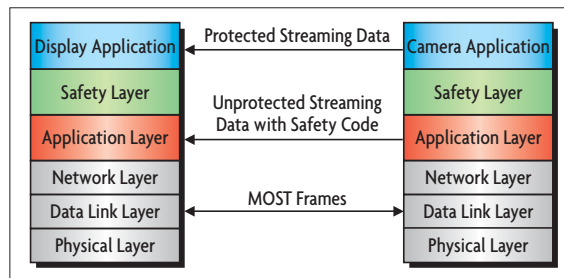


Bild 2. Der MOST-Protokoll-Stack mit Sicherheitsschicht im CBP-System.

im ISO/OSI-Modell. Stattdessen beschreiben sie die Fehler auf logischer Ebene zwischen verschiedenen Kommunikationsteilnehmern. Der Einfachheit halber kann ein einzelnes Motion-JPEG-Bild des CBP-Systems als eine Nachricht betrachtet werden, wobei eine Folge von Nachrichten ein Video-Stream ist. Die Tabelle zeigt eine Teilmenge der Fehler-szenarien und führt

Beispiele für Fehler im Video-Stream an.

Von besonderem Interesse für sicherheitskritische Anwendungen ist die Restfehlerrate, da diese eine bestimmte Schwelle nicht überschreiten darf, um den erforderlichen ASIL (Automotive Safety Integrity Level) zu erreichen.

Konzept einer Sicherheitsschicht mit MOST

Eine zusätzliche Sicherheitsschicht zwischen der Anwendung und dem INIC kann den notwendigen Schutz liefern. Bild 2 zeigt den MOST-Protokoll-Stack einschließlich einer Sicherheitsschicht und der darauf befindlichen CBP-System-Host-Anwendungen. Die Sicherheitsschicht stellt sichere virtuelle Nachrichtendienste auf der MOST-Applikationsschicht zur Verfügung [1].

Eine Standardtechnik im Bereich Sicherheitselektronik ist die Einbettung von Sicherheits-Codes in die Nutzdaten. Auf diese Weise lässt sich eine hohe Fehlererkennungsrate erreichen. Jeder Sicherheits-Code speichert Zusatzinformation, z.B. CRCs oder Sequenz-zähler. Die Sicherheits-Codes werden durch die Sicherheitsschicht senderseitig in die Nutzdaten eingebettet und auf der Empfängerseite ausgewertet. Dadurch kann die Sicherheitsschicht des Empfängers zuverlässig Fehler in den eingehenden Nachrichten entdecken und entsprechend reagieren (z.B. die

Anwendung über den Fehler informieren). Die Architektur mit der Sicherheitsschicht in Bild 2 verwendet ausschließlich die MOST-Applikationsschicht. So können für die Übertragung von Sicherheits-Codes die vorhandenen Schnittstellen des Protokolls verwendet werden. Um Sicherheits-Codes in Streaming-Daten einzubetten, sind verschiedene Möglichkeiten denkbar. Diese reichen von der direkten Integration von Sicherheits-Codes in Streams bis zur Übertragung der Sicherheits-Codes über den SAD-Channel (Stream Associated Data), der sonst für Content Protection verwendet wird [2].

Beispiel einer Sicherheitsschicht für Streams

In der gegebenen Beispielapplikation können Fehler, wie die in der Tabelle

beschriebenen, durch einfache Maßnahmen erkannt werden:

▶ **CRC (Cyclic Redundancy Check):** Sowohl das Kamerabild als auch der Sicherheits-Code selbst können mit einem zusätzlichen CRC geschützt werden. Durch diesen zusätzlichen CRC können Fehler erkannt werden, die durch den Kanal oder INICs verursacht werden, z.B. die Zerstörung von Nachrichten.

▶ **Sequenzzähler:** Sequenzzähler im Sicherheits-Code sind eine typische Maßnahme, um eine Umsortierung von Nachrichten, Nachrichtenverlust oder unbeabsichtigte Wiederholung von Nachrichten zu erkennen.

▶ **Nachrichtenlänge:** Durch Übertragen der Nachrichtenlänge in einem Si-

cherheits-Code ist es möglich, zu prüfen, ob eine Nachricht vollständig ist. Hierzu muss man keine Details über das Format kennen, wie beispielsweise Motion-JPEG.

▶ **Time-outs:** Neben Sicherheits-Codes können zusätzliche Time-outs verwendet werden, um Fehler während des Streamings oder verzögerte Nachrichten zu entdecken.

Die Studie zur Übertragung von sicherheitskritischen Streaming-Daten [4] enthält weiterführende, zusätzliche MOST-spezifische Sicherheitsmaßnahmen wie Stream-Start- und Stream-Ende-Markierungen, um die Fehlererkennung zu verbessern.

Das nächste Ziel ist die zuverlässige Übertragung von Nachrichten auf dem Control Channel und die Absicherungen der verbleibenden Kernmechanismen des Protokolls. Um die Fehlerraten und die erforderliche Stärke der Sicherheits-Codes abschätzen zu können, zum Beispiel die benötigte Länge von zusätzlichen CRCs, sollten quantitative Analysen durchgeführt werden. Auf diesem Wege lässt sich der gewünschte ASIL erreichen. Die Ergebnisse solch einer Analyse können durch Hardware-Tests verifiziert werden. *sj*

Literatur

- [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

ist Mitarbeiter der Communication Engineering im Bereich Elektronik & IT des TÜV Nord/IFM.



**Dipl.-Inf. (FH)
Johannes Specht**

ist Mitarbeiter der Communication Engineering im Bereich Elektronik & IT des TÜV Nord/IFM.