

Timing-Master-Fehler

Analyse und Korrektur von Timing-Master-Fehlern

Dieser Artikel fokussiert ein Hauptanwendungsszenario im Automobilsektor, einen einzelnen Timing-Master (TM) innerhalb eines MOST-Netzwerks. Auf einem Netzwerk-Fehlermodell für eingebettete Systeme basierend wird abgewogen, welche mit einem TM verbundenen Fehlereffekte zu einem nicht verfügbaren Netzwerk oder zu einer fehlerhaften Kommunikation führen können. Zudem wird geprüft, ob die durch das Protokoll zur Verfügung gestellten Fehlertoleranz-Mechanismen helfen, die offensichtlichsten Fehler zu erkennen.

Von Bernhard Fechner

Jeder Master (Network, Connection, Power und Timing) innerhalb eines MOST-Netzwerks birgt einen potentiellen „single point of failure“. Der Ausfall eines Masters kann somit den Ausfall des gesamten Netzwerks nach sich ziehen. Der Timing-Master (TM) sitzt in der Regel in der Haupteinheit des Infotainment-Systems. Er stellt einen wesentlichen Bestandteil eines solchen Netzwerks dar, da er für den Netzwerkstart, die Erzeugung von MOST-Frames und

den Systemtakt verantwortlich ist. In diesem Beitrag werden mehrere Fehlerquellen im Kontext des TM identifiziert, die ein unerwartetes Fehlverhalten verursachen können. Der TM ist eine Grundvoraussetzung für eine gültige Ringbruchdiagnose [1].

Fehlerursachen können datenabhängiger Jitter, falsche Werte des synchronen Bandbreiten-Kontroll-Registers (SBC), des Boundary Descriptors oder fehlerhafte S/PDIF-Eingänge sein. Da MOST mittlerwei-

le auch für sicherheitsrelevante Systeme wie Einparkhilfen verwendet wird, ist die Wahrnehmung potentieller Fehlerquellen für eine korrekte Funktion essentiell. Basierend auf einem Fehlermodell werden Fehlerursachen identifiziert und diskutiert sowie aufgezeigt, wie sich Fehler tolerieren lassen.

Der Ausfall eines Masters in einem MOST-Netzwerk kann das Versagen des gesamten Systems bedeuten. Gewöhnlich sitzen der Netzwerk- und der Timing-Master in einem Knoten, wobei der TM den Systemtakt liefert. Jeder Knoten innerhalb eines MOST-Systems synchronisiert sich mit diesem Signal. Ein MOST-Netzwerk ist daher synchron und der TM immer Knoten Null (InstID 0x00, Adresse 0x400, logisch 0x100). Die Netzwerktopologie ist ein Ring, die aber beispielsweise durch den Einsatz eines Hub zu einer Ring-Stern-Topologie erweitert werden kann, wobei Knoten gelöscht und eingefügt werden können, ohne die Funktion des Netzwerks zu stören. Dieser Artikel betrachtet Fehler innerhalb eines Systems, das aus einem TM besteht, da dieser Systemaufbau (z.B. in der Automobilindustrie) weit verbreitet ist. Hinzu kommt die Annahme, dass es sich um nicht-systematische Fehler handelt. Ein Fehlermodell für vernetzte eingebettete Systeme [7] wird verwendet. Hier können fünf verschiedene Fehlereffekte festgehalten werden: LOST (LO, verlorenes Paket), CORRUPT (CO, Bit-Flip innerhalb des übertragenen Pakets), CUT (CU, Bit des übertragenen Pakets verloren), DUPLICATE (DU, Paket mehrfach gesendet) und CARRIER (CA, keine Netzwerkfunktion).

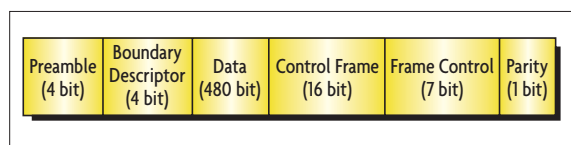
Timing-Master-Fehler

Der TM sitzt meistens in der Head-Unit [2]. Er stellt eine systemrelevante Komponente dar, da er für den Netzwerkstart, die Erzeugung von Frames und den Systemtakt verantwortlich ist. Bild 1 zeigt exemplarisch den Aufbau

automat
300m/1000

eines MOST25-Frames (für MOST150 siehe [1]).

Ein MOST-Netzwerk besteht aus bis zu 64 PnP-Knoten. Jeder Knoten hat eine RX- (receive) und TX-Schnittstelle (transmit). Ein Block besteht aus 16 Frames (pro Frame 512 Bits bei MOST25, 1024 Bits bei MOST50, 3072 Bits bei MOST150). Die ersten acht Bits jedes Frames sind die Präambel und der Boundary Descriptor (BD). Die Präambel indiziert den Frame-Anfang und ermöglicht die Synchronisation zum eingehenden Datenstrom. Hierfür wird der Anfang eines Blocks mit einer davon verschiedenen Präambel gekennzeichnet. Der BD separiert die Daten in einen synchronen (Vielfaches von 4, mindestens 24 byte) und asynchronen (maximal 36 byte)



I Bild 1. Ein MOST25-Frame.

Teil. Bild 2 illustriert den Fluss von Frames innerhalb eines MOST-Netzwerkes mit mehreren Knoten. Die Daten und der Frame-Kontroll-Teil werden durch einen zyklischen Blocksicherungs-Code (CRC) gesichert. Leider gibt [1] keine Hinweise darauf, welche Polynome zum Einsatz kommen, noch welche Bits eines Frames in die Paritätsberechnung eingehen. Daher wird angenommen, dass Präambel, BD und Frame-Kontrolle in die Berechnung eingehen. Abschließend werden einige Schlussfolgerungen gezogen.

■ Initialisierung/System-Lock

Im Zustand „NetInterfaceInit“ löscht der TM das System-Lock-Flag (SLF) auf der Sicherungsschicht. Dieser Wert wird an alle Netzwerk-Interface-Controller (NIC) übertragen. Sobald der TM ein stabiles Lock erkennt, wird das SLF gesetzt. Dieser Zustand wird bei einem der Ereignisse InitReady oder InitErrorShutdown (CA) verlassen. InitReady wird eingenommen, wenn ein stabiles Lock durch den TM erkannt wurde. Wenn das SLF zufällig gesetzt oder zurückgesetzt wird, wird

dieser Fehler durch das Paritäts-Bit erkannt, wenn kein anderes Bit fehlerhaft gesetzt ist.

■ SBC (synchronous bandwidth control)/BD

Mit Hilfe des BD lässt sich ein synchroner und asynchroner Bandbreitenbereich in Vielfachen von vier (Bytes) angeben, wodurch sich die Bandbreite an die tatsächlichen Anforderungen anpassen lässt. Der Wert des BD liegt normalerweise zwischen sechs und 15. Das Register (SBC) wird durch den NIC des TM verwaltet. Während des ersten Teils der Initialisierungsphase können Störungen auftreten. Aus diesem Grund setzt der Master den SBC auf einen Wert kleiner als sechs (gewöhnlich vier) – einen Wert, der während des normalen Betriebs ungültig ist. Der Wert des SBC wird an alle Knoten verteilt und dann auf einen Wert gesetzt,

der den normalen Betrieb anzeigt. Dies wird durch die Knoten im System entdeckt und über das Ereignis Net_On der Anwendung angezeigt. Eine Änderung des SBC durch den TM führt zur Wiederherstellung der synchronen Kommunikation.

Ein (fehlerhaftes) Umschalten des SBC führt aus diesem Grund zu einem Zusammenbruch der (synchronen) Kommunikation (CA). Folglich sollten das SBC-Register sowie das SLF durch ein Paritäts-Bit geschützt werden. Zusätzliche Logikeinschränkungen sollten das unerwünschte Umschalten des SBC verhindern.

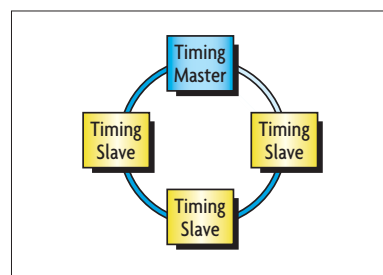
■ Präambel/Oszillator

Die Präambel wird aus dem Signal des Oszillators oder mit dem S/PDIF-Eingangssignal des TMs erzeugt. Alle Timing-Slaves (TS) synchronisieren sich mit einer PLL auf den Systemtakt. Der TM empfängt jeden Frame noch einmal vom letzten TS. Da die Phase wegen der Signaldurchlaufzeiten jedes Knotens verschoben wird, stellt er den ursprünglichen Frame mit seiner PLL wieder her und erzeugt den nächsten Frame. Dabei können drei potentielle

Fehlerursachen (neben einem fehlerhaften PLL-Regelkreis) vorkommen – der Oszillator, ein fehlerhaftes S/PDIF-Signal und Bit-Flips in der Präambel. Ein fehlerhafter Oszillator oder S/PDIF kann zu einem unerwünschten Lock/Unlock und daher zu den Fehlereffekten CU, CO und LO (sowie Präambel-Bit-Flips) führen, die im Folgenden besprochen werden. Der exakte Präambel-Aufbau geht leider ebenfalls nicht aus der Spezifikation hervor. Wieder lässt sich ein einzelner Fehler durch die Paritätsberechnung ausfindig machen.

■ Lock/Unlock, Shutdown-Flag

Ein TS ist im Zustand Lock, wenn er ein Signal an seinem Eingang erhält, auf das sich seine PLL synchronisieren kann. Ansonsten geht er in den Zustand Unlock über [1]. Wenn sich der Knoten auf das Signal für mindestens 100 ms synchronisieren kann, wird ein stabiles Lock angenommen (unter der Voraussetzung, dass in der Zeit t_{Lock} keine Unlock-Ereignisse vorkommen), ansonsten ein Short Lock. Wenn der TM ein stabiles Lock entdeckt, wird angenommen, dass sich das gesamte Netzwerk stabilisiert hat.



I Bild 2. Timing-Master und Slaves.

Der TM ist im Zustand Lock, wenn er den gesendeten aus dem erhaltenen Frame wieder herstellen kann (natürlich sollten alle TS in diesem Fall im Zustand Lock sein). Zudem kann ein fehlerhafter TM einen Unlock eines Knotens (LO) verursachen. Dies veranlasst den erfassenden Knoten, einen Frame mit gesetztem Shutdown-Flag zu senden, was eine (unbeabsichtigte) Stilllegung des Netzwerkes (CA) verursacht. Dies ist ebenfalls zutreffend, wenn das Shutdown-Flag zufällig gesetzt wird, wobei sich dieser Fehler durch die Paritätsberechnung auf-

decken lässt. Der Zustand Lock in MOST25 oder MOST150 nimmt an, dass das Licht eingeschaltet (Light on) ist. Natürlich kann das Netzwerk nicht starten, wenn das Licht nicht eingeschaltet ist (CA, siehe Systemausfälle).

▣ Zufällige Frames

Eine nichtkonforme Oszillatorfrequenz oder eine fehlerhafte Logik zur Generierung von Frames können zur Erzeugung von gekürzten oder fehlerhaften Frames (LO, CO, CU) führen. Daneben lassen sich Frames auch zufällig oder fehlerhaft erzeugen (DU, CO, CU, babbling idiot). DU ist schwierig zu erfassen, da das MOST-Protokoll Sequenznummern nicht direkt unterstützt. CO und CU lassen sich durch den CRC innerhalb des Datenbereiches erfassen. Alle CO- und CU-Frames, bei denen der CRC nicht beeinflusst wird, können durch die Paritätsberechnung erkannt werden, wenn keine Doppelfehler vorliegen.

▣ Systemausfälle

Bei einem einfachen Ring kann eine Unterbrechung des Rings den Ausfall (LO, CA) des gesamten Netzwerks bedingen. Ein Ringbruch kann z.B. durch eine defekte Kontrolleinheit oder einen Bruch der optischen Faser verursacht werden. Für hohe Verfügbarkeit kann der Ring mit einfachen Mitteln (mehrere RX, TX, Verdrahtung) zu einem n-modular redundanten Ring erweitert werden, wobei eine doppelte Ringstruktur häufig gegen Ringunterbrechungen [3] eingesetzt wird [4, 5].

Um einen Ringbruch zu diagnostizieren, müssen alle Geräte das Signal Light on ausgeben. Anschließend wird jeder Knoten gefragt, ob er Light on empfangen hat. Dies lässt sich trotz eines Ringbruchs durchführen, da die MOST-Kontrolleinheiten eine weitere Schnittstelle [6] neben der optischen enthalten. Aus diesem Grund lässt sich ein fehlerhaftes Ringsegment sogar lokalisieren. Ein MOST-Knoten enthält einen Bypass (im NIC zwischen optischem RX und TX), der sich einsetzen lässt, falls der Knoten im Low-Power-Modus ist. Im Falle eines Knotenfehlers schaltet der Transceiver in den

Low-Power-Modus, ohne dabei die Funktion des Netzwerks zu beeinflussen.

Bei einem Short Lock oder einem InitErrorShutdown wird der Bypass abgeschaltet. Eine ganz offensichtliche Störung ist der Ausfall der Lichtquelle (CA) oder ein permanenter Fehler des TM. Bei einem plötzlichen Signalausfall (SSO) wird das Shutdown-Flag gesetzt, der empfangende Knoten sowie der TM speichern die Ursache des Ausfalls (MOST150, SSO, kritischer Unlock [1]) und eine Notabschaltung wird initiiert. Hier ist (strukturelle) Redundanz das einzige Mittel, diese Fehler zu tolerieren. Im Fall eines unbestimmten TM wird ein All-Slave-Network initiiert, um eine (gültige) Ringunterbrechungsdiagnose zu ermöglichen. Wenn die Zahl der TMs nicht gleich Eins (All-Slave, Multi-Master) oder eine gültige relative Knotenposition nicht verfügbar ist, wird ein Diagnosefehler signalisiert und das Netzwerk abgeschaltet.

▣ Jitter

Datenabhängiger (DDJ) und nicht korrelierter Jitter [2] können sich akkumulieren, so dass der TM das Signal eventuell nicht rekonstruieren kann. Dies ist dann der Fall, wenn das Signal außerhalb der Master-Jitter-Toleranz liegt. Hier werden Lock-Fehler (LO) verursacht, da der TM sich nicht synchronisieren kann. Hochfrequenter DDJ wird durch die PLL beschränkt, niedrigerfrequenter DDJ wird weitergeleitet.

Um den DDJ zu messen, wird ein Muster verwendet, welches zwischen dem niedrigsten (0x00) und höchsten (0xff) Wert changiert. Für die effiziente Analyse und Simulation von Timing-Fehlern lassen sich aktuelle FPGAs (Field Programmable Gate Arrays) einsetzen [8].

▣ Schlussfolgerung

Mehrere Protokoll- bzw. Implementierungsverbesserungen wurden aufgezeigt. Einige Punkte sind und bleiben wahrscheinlich unklar, da der Autor keinen Zugang zu einer TM/MOST-Implementierung hatte: Es sind weder die für den CRC verwendeten Polyno-

me spezifiziert noch welche Abschnitte durch Parität gesichert werden, weiterhin ob und welche internen Register durch Parität geschützt sind. Daher die Annahme, dass jedes Bit außerhalb der Daten und Kontrollblöcke in die Paritätsberechnung einfließt. *bg*

Literatur

- [1] MOST Cooperation: MOST Specification Rev. 3.0, May 2008.
- [2] Grzemba, 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, 3. Auflage, 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.



Dr. Bernhard Fechner

hat nach einer Ausbildung bei einer Unfallversicherung das Diplom in Informatik und den Doktor der Naturwissenschaften von der Universität Hagen verliehen bekommen. Er arbeitete mehrere Jahre als Berater. Seine Forschungsinteressen gelten dem Hardware- und Software-Design sowie der Analyse (fehlertoleranter) Architekturen und Protokolle.