Neue Ansätze und Methoden für die Fehlermodellierung und -behandlung bei automobilen Videodatenübertragungsstrecken

Jan Bauer
Daimler AG
Stuttgart, Germany
jan.j.bauer@daimler.com

Karlheinz Blankenbach
Hochschule Pforzheim
Pforzheim, Germany
karlheinz.blankenbach@hs-pforzheim.de

Mirko Conrad
samoconsult GmbH
Berlin, Germany
mirko.conrad@samoconsult.de
https://orcid.org/0000-0003-3221-6503

Andreas Hudak
STZ Electronic Systems GmbH
Mühlacker, Germany
andreas.hudak@stz-es.com

Frank Langner
Daimler AG
Stuttgart, Germany
jan.j.bauer@daimler.com

Matthäus Vogelmann
Hochschule Pforzheim
Pforzheim, Germany
matthaeus.vogelmann@hs-pforzheim.de

Chihao Xu
Universität des Saarlandes
Saarbrücken, Germany
chihao.xu@lme.uni-saarland.de

***Zusammenfassung* — Kamera-Monitor-Systeme und die damit einhergehende digitale Übertragung von Videodaten kommen zunehmend in sicherheitsrelevanten Systemen im Kraftfahrzeug zum Einsatz. Um sicherheitsrelevantes Fehlverhalten zu vermeiden, müssen diese Systeme gegen Fehler und Ausfälle abgesichert werden. Der Beitrag schlägt ein Fehlermodell für die Videodatenübertragung vor und skizziert mögliche Sicherheitsmechanismen zur Fehlererkennung und -behandlung.**

***Abstract* — Camera monitor systems and the associated digital transmission of video data are increasingly being used in safety-relevant automotive systems. To avoid safety-related malfunctioning behavior, these systems must be protected against faults and failures. This paper proposes a fault model for video data transmission and outlines possible safety mechanisms to detect and handle faults in video links**

Keywords — Camera Monitor Systems (CMS), Video Data Transmission, Fault Model, Functional Safety, ISO 26262

I. EINLEITUNG

In modernen Fahrzeugen werden Videodaten oft zwischen mehreren Kameras, Bildprozessoren und Displays übertragen. Die gesteigerte Anzahl der Komponenten mit einer notwendigen Partizipation an der Videodatenübertragung ist auf der Kameraseite durch die Verbreitung von videobasierten Assistenzsystemen und auf der Displayseite durch den gesteigerten Bedarf, diese Informationen adäquat dem Fahrer und Passagieren darzustellen, begründet. Wird ein Kamerabild auf einem Display dargestellt, kann es durch die Darstellung von fahrrelevanten Informationen zu Anforderungen bezüglich der funktionalen Sicherheit kommen.

Teil-, hoch- oder vollautomatisierte Fahrzeuge beziehen einen nicht unerheblichen Teil der Information über ihre Umgebung von bildgebenden Aufnahmeverfahren. Werden die dort anfallenden Videodaten im Fahrzeug übertragen, müssen zur Gewährleistung der Funktionssicherheit ebenfalls Maßnahmen ergriffen werden.

Darüber hinaus werden Videodaten zu Empfängern außerhalb des Fahrzeugs übertragen, wie z.B. für automatisierte Parkvorgänge. Auch hier kann bspw. die Verknüpfung der Bildinformation mit einer eventuellen Entscheidung für die Fahrzeugbewegung sicherheitsrelevant sein.

Im Rahmen einer Bestandsaufnahme wurden von den Autoren mehr als 20 Use-Cases mit Videoübertragung (Video Use-Cases) identifiziert, die potentiell funktional abgesichert werden müssen.

Die Videoübertragung ist ein Spezialfall der Datenübertragung. Die Videoübertragung unterscheidet sich dabei, in der hohen Bandbreite in eine Übertragungsrichtung und die in den meisten Fällen verbindungslose Übermittlung (d.h. es findet kein expliziter Aufbau einer Kommunikationsbeziehung vor dem Datenaustausch statt) in einem sogenannten Pixel-Stream.

Die übertragenen Videodaten werden dann entweder (R_D) über eine Anzeige in ortsaufgelöste Lichtinformation umgesetzt und als Bild von einem Betrachter wahrgenommen, oder (R_P) von einem Videoprozessor mit einem Algorithmus weiterverarbeitet, um entsprechende Merkmale der Umgebung wie z.B. Verkehrszeichen zu erkennen. Der Fall (R_P) geht dabei über die Funktionalität herkömmlicher Kamera-Monitor-Systeme (Camera Monitor Systems, CMS [13]) hinaus.

Im Fall (R_D) kann zur Verbesserung der Benutzererfahrung (User-Experience) eine Bildverbesserung beispielsweise unter Nutzung von Farbraumkonvertierungen oder durch eine Überlagerung mit zusätzlichen Inhalten erfolgen. Weiter werden die Eigenschaften der visuellen Wahrnehmung genutzt, um z.B. durch Kompression der Videodaten die Effizienz der Übertragung zu optimieren. Verfahren für die Absicherung müssen in diesem Fall entsprechend robust gegenüber den (validen) Änderungen der Bildverbesserung, Überlagerung und Kompression sein. Gleichzeitig müssen ungültige Änderungen wie z.B. einfrieren des Bilds erkannt werden. Sowohl bei (R_D) als

auch bei (R_P) muss die Integrität der Daten und die verzögerungsfreie Übertragung sichergestellt werden.

Viele der derzeit bekannten bzw. verwendeten Mechanismen zur Absicherung der Datenübertragung bei Fehlern und Ausfällen sind für die allgemeine Datenübertragung ausgelegt und betrachten den Sonderfall der Videoübertragung nicht im benötigten Umfang. Hieraus ergeben sich potentielle Lücken bei der Gewährleistung der Funktionssicherheit [12] bei vielen state-of-the-art als auch bei zukünftigen Video Use-Cases. Beispielsweise gibt es nur beschränkte Mechanismen, um festzustellen ob Videodaten korrekt übertragen und durch das Display in die entsprechende Lichtinformation umgesetzt wurden.

Im vorliegenden Paper wird ein Konzept vorgestellt, dass eine funktionale Absicherung von Videoübertragungen von der Quelle (nach Erzeugung der Pixel) bis zur Umwandlung der Pixel in optische Information (R_D) bzw. zum Empfänger (R_P) ermöglicht. Dabei werden bekannte Verfahren zur Absicherung der Qualität bei Videoübertragungen für die Nutzung innerhalb der funktionalen Sicherheit betrachtet und mit neuen Verfahren kombiniert, um eine möglichst holistische Absicherung der Videoübertragungskette zu erreichen.

II. ABLEITUNG EINES FEHLERMODELLS FÜR DIE ÜBERTRAGUNG VON VIDEODATEN

Voraussetzung für die systematische Absicherung eines technischen Systems, bspw. eines Systems zur Videodatenübertragung, ist die Kenntnis der möglichen *Ausfallarten* (failure modes), die in diesem System auftreten können, also die Definition eines geeigneten *Fehlermodells* (fault model).

Für die klassische Datenübertragung kann ein solches Fehlermodell aus der Funktionssicherheitsnorm *ISO 26262* [12] abgeleitet werden.

Um eine hohe Fehleraufdeckung zu gewährleisten, müssen die folgenden Ausfallarten berücksichtigt werden:

- Informationsverfälschung (corruption of information)
- Informationsverlust (loss of information)
- fehlerhafte Informationsabfolge (incorrect sequence of information)
- Informationswiederholung (repetition of information)
- Hinzufügen von Information (insertion of information)
- Informationsverzögerung (delay of information)
- Maskeradefehler oder fehlerhafte Adressierung (masquerade or incorrect addressing of information)
- Nichtempfang oder nichtintendierter Empfang von Informationen (asymmetric information sent from a sender to multiple receivers, information from a sender received by only a subset of the receivers)
- Verhinderung des Zugriffs auf einen Kommunikationskanal (blocking access to a communication channel)

Anhand eines derartigen Fehlermodells kann die Wirksamkeit von Sicherheitsmechanismen zur Fehlererkennung bzw. -vermeidung systematisch analysiert werden. Da den Autoren ein angepasstes Fehlermodell für den Spezialfall der Übertragung von Videodaten nicht bekannt ist soll ein solches nachfolgend erarbeitet werden.

Hierfür wird das in Fig. 1 illustrierte generische Modell einer Videodatenübertragungsstrecke zugrunde gelegt. Eine Videoübertragungsstrecke besteht aus einem Sender *(Sender, S)*, einem Übertragungskanal *(Transmission, T)* und einem Empfänger *(Receiver, R)*. Dabei können S, T und R aus mehreren Teilen bestehen.

Im Falle eines Rückfahrkamera- (Rear View Camera) Systems werden die aus den eigentlichen Pixeldaten und zugehörigen Metadaten bestehenden Videodaten (I) bspw. durch eine Rückfahrkamera erzeugt und von dieser über einen ungesicherten (sog. grauen) Kanal digital an den Empfänger (I") bspw. ein Monitor in der Mittelkonsole übertragen (Fig. 1). Die Übertragung T: I→I" kann dabei drahtgebunden als auch drahtlos erfolgen.

Eine zusätzliche Herausforderung ergibt sich dadurch, dass sich optional innerhalb des ungesicherten Übertragungskanals weitere Elektronikkomponenten, genannt *Modifier (M)* befinden können, die die zu übertragenden Videodaten auf bestimmte Art und Weise verändern können (I*).

In dem in Fig. 1 dargestellten Rear View Camera System könnte eine zwischengeschaltete Head Unit bspw. die Bildhelligkeit oder den Kontrast optimieren, ein Kamerabild skalieren, es in ein größeres Gesamtbild einbetten oder augmentieren.

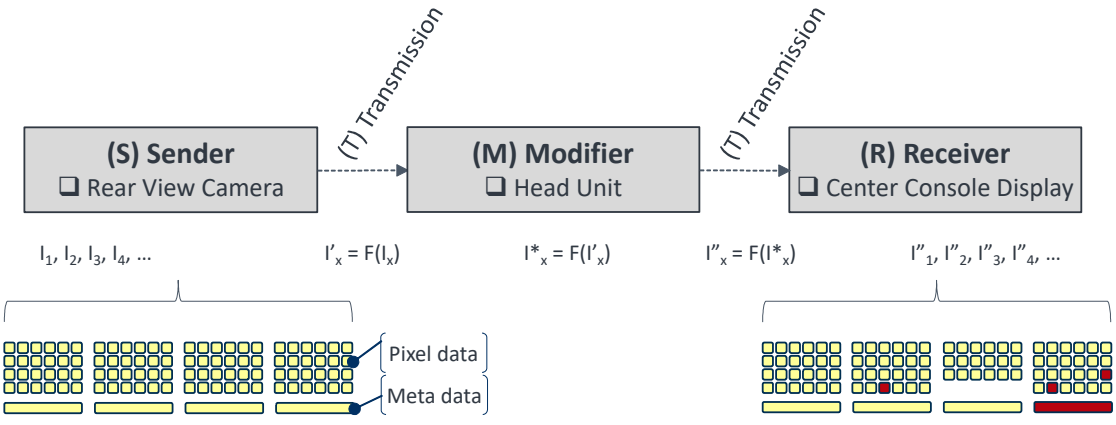

Fig. 1. Modell der Videodatenübertragungsstrecke

Zulässige Bildtransformationen sollen dabei durch die Sicherheitsmechanismen toleriert werden. *Unzulässige Bildtransformationen*, die bspw. dazu führen, dass der Nutzer die relevanten Bildinformationen nicht mehr erkennen kann, sollen dagegen erkannt werden.

Voraussetzung für die Entwicklung und vor allem die Bewertung von Mechanismen für die Absicherung der Videodatenübertragung ist die Aufstellung eines geeigneten *Fehlermodells für eine Videodatenübertragung*.

Prinzipiell können zunächst einmal die gleichen Ausfallarten wie bei der klassischen Datenübertragung auftreten, d.h. das Fehlermodell für die Videodatenübertragung muss daher mindestens die o.g. Ausfallarten berücksichtigen:

- FM_{01}: Bildverfälschung
- FM_{02}: Bildverlust
- FM_{03}: fehlerhafte Bildabfolge
- FM_{04}: Bildwiederholung
- FM_{05}: Hinzufügen von Bildern
- FM_{06}: Bildverzögerung
- FM_{07}: Maskeradefehler oder fehlerhafte Adressierung
- FM_{08}: Nichtempfang oder nichtintendierter Empfang von Bilden
- FM_{09}: Verhinderung des Zugriffs auf eine Bildübertragungsstrecke

Darüber hinaus wurden weitere videospezifische Ausfallarten identifiziert, die ebenfalls berücksichtigt werden müssen. Hierzu gehören z.B.:

- FM_{10}: eingefrorenes Bild (frozen image)
- FM_{11}: fehlerhafter Bildausschnitt / Vergrößerungsfaktor (erroneous field of view / zoom factor)
- FM_{12}: fehlerhafte Bildgröße (erroneous image size)
- FM_{13}: fehlerhafte Metadaten (erroneous meta data)
- FM_{14}: fehlerhafte Bilddarstellung (erroneous image display)
- FM_{15}: Verlust notwendiger Bildinformation (loss of essential image information)
- FM_{16}: fehlerhafte Bildtransformation (unintended image transformation)

III. SICHERHEITSMECHANISMEN

Um die o.g. Fehlermöglichkeiten zu erkennen bzw. zu behandeln, wurden von den Autoren bekannte Sicherheitsmechanismen für die einzelnen Bestandteile der Videodatenübertragung zusammengetragen und potentielle Lücken identifiziert.

Diese Vorgehensweise wird in den folgenden Unterabschnitten anhand der Beispiele Absicherung des Übertragungskanals T auf physikalischer Ebene (Unterabschnitt A) und Absicherung des Empfängers R in Form eines Displays (Unterabschnitt B) beschrieben. Darüber hinaus werden komponentenübergreifende (systemweite) Absicherungsverfahren mittels Hashing und Watermarking beschrieben (Unterabschnitte C, D).

A. Absicherung des Übertragungskanals (T)

Für Videoübertragungen können prinzipiell verschiedene physikalische Übertragungsverfahren und Übertragungsmedien verwendet werden. Heutige Verfahren für die Videoübertragung im Fahrzeug verwenden vornehmlich elektrische drahtgebundene Verfahren, daher soll sich an dieser Stelle auf die elektrischen drahtgebundenen Verfahren fokussiert werden. Heutige Mechanismen zur Absicherung der physikalischen Übertragungsschicht haben das Ziel, die Qualität der Videoübertagung sicherzustellen, d.h. Ausfälle und Störungen zu erkennen und / oder zu vermeiden.

Dazu zählt die *Erkennung von Fehlern der physikalischen Verbindung* (Line Fault Detection) mit den Möglichkeiten:

- Verbindungsunterbrechung
- Kurzschluss nach Masse
- Kurzschluss zur Versorgungsspannung (oder anderen Spannungen)
- Kurzschluss zwischen den Übertragungsleitungen
- erhöhter Leitungswiderstand zwischen Sender und Empfänger
- fehlerhafter Leitungsabschluss

Besteht eine physikalische Verbindung, kann bspw. über die *Aussendung eines Testsignals* vom Sender zum Empfänger, den dortigen Empfang und die Rückmeldung an den Sender die logische Verbindung beidseitig überprüft werden. Der Zustand der logischen Verbindung wird in vielen automotive Übertragungssystemen mit einem Link-Lock signalisiert.

Die Übertragung der Videodaten über einen Übertragungskanal kann durch *Error-Detection Codes (EDC)*, bspw. die Verwendung eines *Cyclic Redundancy Checks (CRC)*, abgesichert werden. Auf diese Weise können eventuelle elektro-magnetische Störungen auf der Videoübertragungsstrecke erkannt werden. Die Verwendung von *Error-Correction Codes (ECC)* erlaubt eine *Forward Error Correction (FEC)*, also eine automatische Korrektur bestimmter Übertragungsfehler.

Neben der Möglichkeit, Fehler zu erkennen bzw. zu korrigieren, können aus den genannten Verfahren die aktuelle Anzahl der Übertragungsfehler aus der CRC-Auswertung (F_{CRC}) bzw. Anzahl der Fehlerkorrekturen (C_{FEC}) abgeleitet werden und als Messgröße für die *Qualität der physikalischen Verbindung* Q_{TP} verwendet werden. Diese Qualitätsbewertung der physikalischen Verbindung Q_{TP} kann durch *Messung der physikalischen Empfangseigenschaften* wie bspw. der vertikalen, horizontalen Augenöffnung (A, B) erweitert werden.

Darüber hinaus verwenden heutige Videoübertragungsstrecken *Ausgleichsfilter* auf Frequenzbasis (Equalizer) *zum Ausgleich der frequenzabhängigen Dämpfung auf der Übertragungsstrecke*. Der Abstand der aktuellen zur maximal möglichen Aussteuerung dieser Filter über die Frequenz $\Delta D(f)$ kann als weiterer Parameter für die Qualitätsbewertung der Übertragungsstrecke genutzt werden.

Wird ein zu definierender Schwellwert für die Qualität der Übertragungsstrecke Q_{TP} unterschritten, können dann entsprechende Fehlerbehandlungsmechanismen aktiviert

werden. Mögliche Fehlerbehandlungsmechanismen sind bspw. die *präventive Abschaltung von betroffenen Funktionen (P_D)* oder eine *abgestufte Funktionsreduktion (Graceful Degradation, G_D)*. Eine Graceful Degradation kann bspw. durch eine auf der Qualitätsbewertung Q_{TP} basierende Anpassung des Bandbreitenbedarfs per Reduktion der Auflösung oder Bildwiederholrate erfolgen.

Ziele der weiteren Arbeiten zur Absicherung der physikalischen Übertragung sind zum einen die Definition geeigneter Funktionen zur Qualitätsbewertung auf Basis der einzelnen Qualitätsparameter

$$Q_{TP} = f\,(\Delta D,\, C_{FEC},\, F_{CRC},\, A,\, B,\, \ldots\,)$$

und zum anderen die Entwicklung entsprechender Methoden zur abgestuften Funktionsreduktion P_D, G_D auf Basis dieser Qualitätsbewertung Q_{TP}

$$P_D = f\,(\,Q_{TP}\,)$$

$$G_D = f\,(\,Q_{TP}\,)$$

B. Absicherung des Empfängers (R)

Um im Falle einer Videoübertragung eine Ende-zu-Ende Absicherung zu erreichen, muss auch die Umwandlung der digitalen Pixelinformationen in sichtbares Licht durch das Display überprüft werden.

Sollen aufgetretene Bildfehler oder -degradationen nicht nur erkannt, sondern auch in deren Ursache bestimmt werden können, ist neben der optischen Ausgabe auch die Signalverarbeitungskette innerhalb des Display-Moduls zu überwachen. Somit kann die Absicherung des Displays anhand zweier, sich ergänzender Ansätze angestrebt werden:

- Optoelektronischer Ansatz: *optoelektronische Erfassung der Emission des Displays*
- Elektrischer Ansatz: *Messung von elektrischen Größen* (bspw. Stromverbrauch) *und Überwachung der Daten-Signale im Display-Modul*

Optoelektronische Methoden basieren auf der Erfassung des dargestellten Bildes mittels eines optischen Systems und dessen Vergleich mit den empfangenen Bilddaten oder Metadaten der Bildgenerierung in der Kamera. Ultimativ sollte die Lichtinformation der einzelnen Pixel erfasst werden. Hierfür ist es erforderlich, die zeitliche Intensität sowie die Ortskoordinaten der von den Pixeln ausgesendeten Lichtstrahlen und somit ein zweidimensionales Lichtfeld *I(x,y,t)* zu erfassen. Ziel ist es hierbei, die Bildintegrität und die Erkennbarkeit des Bildinhaltes zu ermitteln.

Naheliegend ist die *Erfassung der optischen Ausgabe mittels* einer vor dem Display angebrachten *Kamera*, wodurch ein hoher Grad der Fehlererkennung erreicht wird. Diese kann jedoch aus bautechnischen Gründen nicht in allen Fällen eingesetzt werden und der erforderliche Auswerte- und Analyseaufwand ist hoch.

Eine abgewandelte Methode ist die *Erfassung der optischen Ausgabe mittels* eines auf das Displayglas aufgebrachten *Wedge-Lightguide* [7]. Dieser Lichtleiter kann in Form einer dünnen, semitransparenten Folie einen Teil der Intensität der Lichtstrahlen zu einem optoelektrischen Sensor weiterleiten, ohne dass deren Ortsinformation verloren geht. Anstatt einer Kamera können dort auch niedrigauflösende Sensoren als Kompromiss zwischen Signalverarbeitungsleistung und Informationsgehalt eingesetzt werden. Bei der Verwendung eines (semi-)transparenten OLED kann ein Wedge-Lightguide oder eine Kamera auch hinter dem Panel verbaut werden (Fig. 2).

Diese beiden Methoden können prinzipiell einem Displaymodul hinzugefügt werden, während eine *Erfassung der optischen Ausgabe mittels Fotosensoren in jedem Pixel des Displays* [8] bereits bei der Herstellung des elektro-optischen Wandler (z.B. LCD) integriert werden muss. Dieser Ansatz rechnet sich nur bei höchsten Stückzahlen.

Ein modernes, hochauflösendes Aktiv-Matrix-Display besteht neben dem eigentlichen elektro-optischen Wandler (Display Glass) aus einer Vielzahl von Mikroprozessoren und Halbleitern (Panel Electronics). Natürlich setzt eine fehlerfreie optische Ausgabe eine ebenso funktionierende Elektronik voraus; im Umkehrschluss können auftretende Fehlfunktionen der Elektronik anhand einer fehlerhaften optischen Ausgabe erkannt werden. Ziel der in der Panelelektronik umzusetzenden Sicherheitsmechanismen ist die Erkennung von Fehlerfällen wie z.B. ein nicht kompatibles Eingangssignal oder ein gestörter Bildaufbau.

Fig. 2. Transparentes OLED mit der Möglichkeit zur optischen Überwachung des Displayinhaltes von der Panel-Rückseite

Die elektrischen Ansätze zur Überwachung des Displays werden anhand des Blockschaltbildes in Fig. 3 diskutiert. Im Wesentlichen sind in der Panelelektronik folgende Komponenten enthalten:

- Das Display Interface (De-Serializer) empfängt die darzustellenden Daten über eine serielle Schnittstelle (ähnlich HDMI) und wandelt diese typischerweise auf LVDS Signale für den Timing Controller um.
- Der Timing Controller (TCON, z.B. [1]) formatiert den Input-Bilddatenstrom in Signale (z.B. [4]) für Zeilen- (row driver) und Spaltentreiber (column driver) um.
- Die Zeilentreiber steuern eine Zeile nach der anderen an, während die Spaltentreiber (z.B. [5]) die zugehörigen Graustufen-Daten einspielen.
- Der Gamma- und VCOM-Buffer stellt LCD-spezifische Spannungen zur Verfügung.
- Das LCD-Backlight stellt die Lichtquelle des LCDs dar.

Naheliegende Ansätze zur Fehlererkennung und -analyse sind die Spannungs-, Strom-, Leistungs- und Signal-Überwachungen aller oben aufgeführten Panelelektronik-Komponenten.

Bei einem OLED-Display ist der Stromverbrauch maßgeblich durch die Graustufen der Pixel bestimmt. Somit stellt der *Abgleich zwischen Stromverbrauch und Graustufen-Histogramm* eine erste und einfache Überwachung bei OLEDs dar. Mit erweiterten Methoden im Zeitbereich und

Referenzmessungen ist dies auch bei LCDs möglich. Es ist offensichtlich, dass in beiden Fällen bei keiner oder nur sehr geringer Leistungsaufnahme kein Bild dargestellt wird.

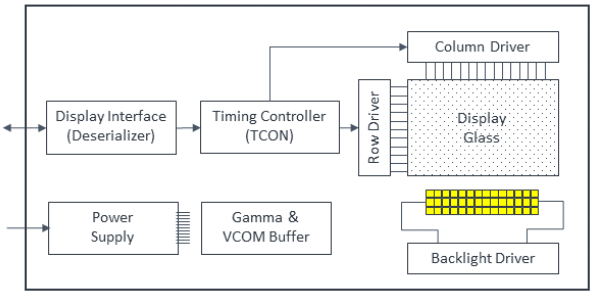

Fig. 3. Typisches Blockschaltbild eines LCD-Displaymoduls

Die digitalen Signale am Eingang und im Panel können bezüglich ihrer Frequenz, Dauer, Austastlücken etc., d.h. des korrekten Timings, überwacht werden *(Timing-Überwachung der digitalen Signale)*. Bei Abwesenheit oder falschem Timing wird typischerweise kein oder nur ein gestörtes Bild visualisiert. Eine weitere, klassische Methode ist die Nutzung von *Error-Detection Codes*, bspw. die Kontrolle des CRC über die Bilddaten.

Aufwändigere Überwachungsmethoden basieren auf der *Analyse darzustellender Bildinhalte* (geliefert über die Metadaten) *und* deren *Vergleich mit den Daten im Bilddatenstrom*. Ein *Telltale-Monitoring* durch z.B. Abgleich einer Höchstgeschwindigkeitsinformation (darzustellender Bildinhalt) mit dem dargestellten Verkehrszeichens (Daten im Bilddatenstrom) ist Stand der Technik [6].

In Summe existiert displayseitig eine Vielzahl von Mechanismen zur Fehlererkennung mit unterschiedlicher Effektivität und sehr unterschiedlichen Kostenindikationen.

Viele fehlerhafte Darstellungen auf einem Display sind vom Betrachter problemlos als solche zu identifizieren (perceived faults), z.B. der Nichtempfang von Bildern (FM_{08}) oder bestimmte Bildstörungen. Kritischer sind kaum zu erkennende Fehler wie falsche Graustufen-Spannungen, die wichtige Bildinhalte quasi „unsichtbar“ werden lassen oder eine Bildverzögerung (FM_{06}). Die einzusetzenden Fehlererkennungsmechanismen sollten daher auf diese Fehlerarten fokussieren.

Als möglicher Fehlerbehandlungsmechanismus, bspw. bei fortwährenden CRC-Fehlern, kommt die *präventive Abschaltung des LCD-Backlights* P_D (sicherer Zustand ‚keine Bilddarstellung‘ bzw. ‚Anzeige eines (dunklen) Ersatzbildes‘) in Frage.

Anwendungsabhängig kann jedoch auch hier die Anzeige eines degradierten Bildes *(Graceful Degradation)* G_D bei erkannten Störungen (z.B. digitale Blockartefakte) oder Degradationen (z.B. Rauschen) gefordert sein (sicherer Zustand ‚Anzeige eines degradierten Bildes‘) ggf. in Kombination mit einer geeigneten Indikation für den Betrachter, dass der Bildinhalt fehlerbehaftet ist. Als Beispiel kann der Video Use-Case ‚Überwachung des Fahrzeugs durch einen Remote-Operator‘ dienen; hierbei erscheint ein degradiertes Bild nützlicher als das vollständige Unterbinden des Informationsflusses.

C. Komponentenübergreifende Absicherung: Hashing

Moderne Autos zeigen dem Fahrer hochqualitative Videodaten an. Anpassungen an die Umgebung und Augmentieren mit Hilfslinien und Symbolen unterstützen den Fahrer zusätzlich in der Durchführung seiner Fahraufgaben. Dafür kann das originale Kamerabild verschiedene Verarbeitungsschritte durchlaufen. Diese Bearbeitungsschritte sind i.d.R. nicht gemäß eines definierten Automotive Safety Integrity Level (ASIL) gemäß ISO 26262 abgesichert, sondern zumindest in Teilen auf QM-Level realisiert.

Ein videoübertragendes System muss in einem solchen Fall gewährleisten, dass das originale und bearbeitete Bild von Betrachter gleich bzw. ähnlich wahrgenommen werden und für die Durchführung der Fahraufgabe notwendige Bildinformationen nicht verloren gehen.

Eine weit verbreitete Methode für einen solchen Bildvergleich ist die *Scale-Invariant Feature Transform (SIFT)* [2]. Dieses und ähnliche Bildabsicherungsverfahren basieren auf Features wie z.B. den sogenannten Harris Corners. Ein direkter Einsatz für die Absicherung eines Modifiers ist jedoch nicht zielführend, da diese speziellen Verfahren mit dem Hintergrund der Objekterkennung entwickelt wurden und nicht die ‚Identität‘ eines Bildes berücksichtigen. Dennoch können manche Aspekte dieser Algorithmen für unsere Anwendung herangezogen werden [1].

Eine probate Methode, die Datenintegrität einer Bildübertragung mit Bildverarbeitung (vgl. Fig. 1) zu gewährleisten, ist es, mit einer *Hash-Funktion h* ein beschreibendes Label des Bildes I, das am Anfang der Übertragungsstrecke steht, zu erzeugen.

$$h : I \rightarrow E$$

Der Output der Hash-Funktion E enthält die beschreibenden Eigenschaften des Bildes. E benötigt nur einen Bruchteil der Datenmenge von I und kann entweder in den Austastlücken der Pixeldaten oder als Bestandteil der Metadaten geleitet werden. Am Ende der Übertragungsstrecke ist das Bild I'', das aufgrund der möglichen Bildbearbeitung pixelweise stark vom Originalbild I abweichen kann. Das bearbeitete Bild I" hat dann den Hash-Wert von E''.

$$h : I'' \rightarrow E''$$

Die Herausforderung ist es nun, ein Verfahren zu entwickeln, das die Unterscheidung zwischen gewünschten und fehlerhaft veränderten Bildern (inhaltlich anders) ermöglicht. Der Kern der Technologie liegt im Entwurf einer speziellen Hashfunktion und einer Matching-Funktion, die eine hohe und robuste Diskriminanz aufweisen.

Wichtig ist es zudem, dass E ohne nennenswerte Latenz erzeugt wird, damit das Verfahren für sicherheitsrelevante Anwendungen eingesetzt werden kann. Das gleiche gilt auch für E'': Dieses muss unmittelbar nach dem Empfang des Bildes I'' erzeugt werden. Auch die Matching-Funktion von E und E'' soll schnell ein Ergebnis liefern, ob die Videodaten ungewünscht verändert oder fehlerhaft übertragen worden sind. Die Algorithmen sollen nach Möglichkeit am Anfang und am Ende der Übertragungsstrecke eingesetzt werden, so dass eine hohe Integrität der Videodaten erreicht werden kann.

D. Komponentenübergreifende Absicherung: Watermarking

Neben den bereits betrachteten, primär einer Komponente des Übertragungsmodells für Videodaten zuordenbaren Fehlererkennungs- und Fehlerbehandlungsmechanismen können weitere, systemübergreifende Mechanismen erforderlich sein. Als Vertreter dieser Kategorie sollen hier die *Absicherung sicherheitsrelevanter Inhalte mittels Wasserzeichen* und die *Absicherung der zeitlichen Synchronität* betrachtet werden.

Je nach Video Use-Case kann ein erzeugter Videoinhalt sicherheitsrelevant sein. Derartige Inhalte werden im Rahmen des sicherheitsgerichteten Entwicklungsprozesses gemäß ISO 26262 definiert. Je nach Anwendungsfall gelten für diesen Inhalt besondere Anforderungen bezüglich der Anzeige, bspw. kann es vorkommen, dass ein eingefrorener sicherheitsrelevanter Inhalt I_S nicht angezeigt werden darf. Wird im Fahrzeug ein solcher sicherheitsrelevanter Videoinhalt I_S erzeugt, kann dieser Videoinhalt zur Absicherung mit einer entsprechenden Markierung *(Wasserzeichen, W)* versehen werden. Jedes Display das potentiell den Videoinhalt I_S anzeigen könnte, muss eine Methode zur Detektion von des Videoinhalts I_S implementieren um eine fehlerhafte Anzeige zu verhindern.

Eine probate Methode dafür ist das Hinzufügen von Informationen zu den Bilddaten in Form eines sichtbaren / unsichtbaren, robusten / fragilen Wasserzeichens *W*. Ein Beispiel für eine robuste, unsichtbare Methode des Wasserzeichens ist in [14] zu finden. Zusätzlich kann optional ein zufälliger Wert *K* (z.B. geheimer oder öffentlicher Schlüssel) verwendet werden. Durch das Hinzufügen des Wasserzeichens *W* und dem Zufallswert *K* wird die ursprüngliche Bildinformation I_S verändert [11]:

$$I_S \times W \times K \rightarrow \tilde{I}$$

Der Erkennungsprozess kann dann über den folgenden Zusammenhang erfolgen [11]:

$$\tilde{I} \times W \times K \rightarrow \{0,1\}$$

Ziel ist es nun geeignete Methoden für das Hinzufügen der Markierung, mit entsprechender Robustheit gegenüber Veränderungen, sowie entsprechende Methoden zur Erkennung der Wasserzeichen zu finden. Darüber hinaus können fragile Wasserzeichen dazu verwendet werden, um festzustellen ob eine Änderung an den Videodaten vorgenommen wurde. Auch hier ist es wichtig das Hinzufügen, Erkennen (und Entfernen) der Markierung ohne nennenswerte Verzögerung durchzuführen.

Ein weiteres Kriterium für die Absicherung der Videodaten ist die *Bewertung des zeitlichen Versatzes* Δt_I *zwischen dem Originalbild I und dem empfangenen Bild I''* (vgl. Fig. 1).

$$\Delta t_I = |t(I) - t(I'')|$$

Eine Realisierungsmöglichkeit dafür besteht in der Kombination einer gemeinsamen Zeitbasis zwischen Sender S und Empfänger R und einem im Bild oder den Metadaten enthaltenen Zeitstempel. Die zeitliche Synchronisierung könnte bspw. über einen zusätzlichen bidirektionalen Kommunikationskanal, unter Verwendung von Laufzeitunterschieden, erreicht werden. Der Zeitstempel könnte im Sender als Teil der Markierung, z.B. als Modulation des Zufallswertes *K*, erfolgen.

Ziel ist es hier entsprechende Synchronisierungsmechanismen für die automobile Videoübertragung zu definieren und entsprechend robuste Lösungen für Einbringung in die Markierung und die entsprechende Erkennung zu finden.

IV. SICHERHEITSKONZEPT AUF SYSTEMEBENE

Systemabhängig muss die Umsetzung der einzelnen komponentenbezogenen und übergreifenden Absicherungsmechanismen auf Systemebene geeignet kombiniert und orchestriert werden.

Die pauschale Übertragung bekannter Maßnahmenkombinationen aus der herkömmlichen Datenübertragung wie bspw. der *Ende-zu-Ende-Absicherung* (End-to-end Protection, E2E), welche die Mechanismen Checksumme auf Applikationsebene, Botschaftszähler, Timeoutüberwachung und Senderkennung miteinander kombiniert, auf die hier betrachtete Videodatenübertragung ist jedoch nicht zielführend, da diese z.B. nicht tolerant in Bezug auf die zulässigen Bildtransformationen sind.

Eine systemabhängige Auswahl der Mechanismen muss dabei abhängig vom Automotive Safety Integrity Level (ASIL) des betrachteten *Sicherheitsziels* sowie der Definition des *sicheren Zustands* erfolgen.

Anwendungsabhängig können dabei typischerweise folgende sicheren Zustände unterschieden werden:

- SZ_{01}: keine Bilddarstellung
- SZ_{02}: Anzeige eines Ersatzbildes (z.B. schwarzer Bildschirm oder Fehlermeldung)
- SZ_{03}: Anzeige eines Bildes, das vom Betrachter als eindeutig fehlerhaft erkannt wird
- SZ_{04}: Anzeige eines degradierten Bildes (z.B. Bild mit geringerer Auflösung oder Frequenz)

Kann im Fehlerfall auf die Videodatenübertragung verzichtet werden (*Fail Silent* oder *Fail Safe*), bspw. bei einem elektronischen Seitenspiegel, kann über Fehlererkennungsmechanismen eine Fehlfunktion detektiert und das Display oder die Funktion deaktiviert werden (SZ_{01}) bzw. ein Ersatzbild angezeigt werden (SZ_{02}).

Besteht eine Verfügbarkeitsanforderung an die Videodatenübertragung *(Fail Operational)*, muss dagegen auch im Fehlerfall ein hinreichend geignetes Bild angezeigt werden. Dies kann über eine Degradierung der Videoübertragung (SZ_{04}) oder durch den Wechsel auf eine redundante Komponente erfolgen.

Viele der in III. definierten Fehlererkennungsmechanismen können so implementiert werden, dass sie Kenngrößen für einen systeminternen Test *(Built-In-Self-Test, BIST)* liefern. Unterschreitet eine Kenngröße oder eine Kenngrößenkombination einen Schwellwert, kann eine Fehlerbehandlung bzw. der Übergang in einen sicheren Zustand (ggf. auch vor Fahrtantritt) getriggert werden.

Zur systemweiten Orchestrierung der Sicherheitsmechanismen wird vorgeschlagen, die Kenngrößen der verschiedenen Fehlererkennungsmechanismen in einer dezidierten *Safety Unit (SAF)* zusammenzufassen. Damit ergibt sich das in Fig. 4 veranschaulichte generische *Modell einer Sicherheitsarchitektur zur Absicherung der Videodatenübertragung*.

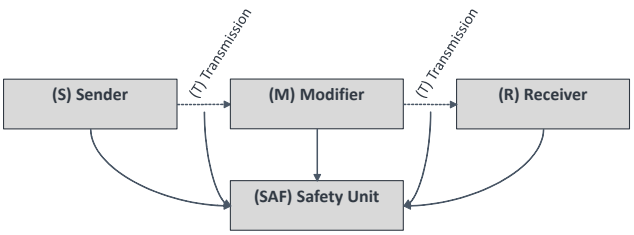

Fig. 4. Modell der Sicherheitsarchitektur

Die SAF muss dabei nicht als einzelne, separate Komponente ausgeführt sein, sondern kann bspw. in einer der anderen Systemkomponenten verortet sein oder über mehre Systemkomponenten (bspw. S und R) verteilt sein. Ebenso kann ein lokaler Datenaustausch zwischen S, T, M und R erforderlich sein, um übergreifende Sicherheitsmechanismen zu realisieren (bspw. ein Kommunikationskanal zwischen S und R zur zeitlichen Synchronisation).

V. ZUSAMMENFASSUNG UND AUSBLICK

Ausgehend vom Stand der Technik bei der Absicherung der allgemeinen Datenübertragung wurde von den Autoren ein generisches Modell der Videodatenübertragung und ein Fehlermodell für eine solche Übertragung vorgeschlagen. Die Modelle umfassen dabei die Veränderung von Bilddaten durch eine modifizierende Komponente innerhalb der Übertra-gungsstrecke.

Danach wurden vorhandene Sicherheitsmechanismen für einzelne Komponenten des Übertragungsmodells sowie komponentenübergreifende Sicherheitsmechanismen identifiziert und zusammengetragen. Dabei identifizierte Lücken wurden herausgearbeitet und es wurde damit begonnen, diese zu schließen.

Failure Modes	Safety Mechanisms				# of applicable safety mechanisms
	SM_{01}	SM_{02}	...	SM_{xx}	
FM_{01}	✓	✓		○	> 0
FM_{02}	○	○		○	0
FM_{03}	○	○		✓	> 0
FM_{04}	○	✓		✓	> 0
FM_{05}	✓	✓		○	> 0
FM_{06}	✓	○		○	> 0
FM_{07}	✓	○		○	> 0
FM_{08}	✓	○		○	> 0
FM_{09}	○	✓		○	> 0
FM_{10}	○	○		✓	1
FM_{11}	○	○		○	0
FM_{12}	✓	✓		○	> 0
FM_{13}	✓	○		○	> 0
FM_{14}	✓	○		✓	> 0
FM_{15}	○	○		✓	> 0
FM_{16}	○	○		✓	> 0
...					

Fig. 5. Vorgehensweise zur Auswahl geeigneter Sicherheitsmechanismen

Die identifizierten Sicherheitsmechanismen SM sollen im weiteren Projektverlauf systematisch auf die identifizierten Ausfallarten FM abgebildet werden, um einen *Baukasten für die Absicherung der verschiedenen Videodatenübertragungen im Fahrzeug* bereit zu stellen (Fig. 5). Hierzu gehört auch eine *Abschätzung der Diagnosegüte* (Diagnostic Coverage, DC) der einzelnen Mechanismen. Für Ausfallarten, für die der Baukasten bisher nur wenige oder keine Sicherheitsmechanismen enthält, sollen gezielt *weitere Mechanismen entwickelt* werden.

Im Rahmen der Anwendung auf ein konkretes System werden dann zunächst a) die relevanten Fehlermodi identifiziert und b) für diese eine geeignete Kombination von Sicherheitsmechanismen aus dem Baukasten ausgewählt. Danach ist c) die generische Sicherheitsarchitektur geeignet zu instantiieren und d) die Sicherheitsmechanismen sind den einzelnen Komponenten der instantiierten Sicherheitsarchitektur zuzuordnen und dort zu implementieren.

REFERENCES

[1] E. Rublee, V. Rabaud, K. Konolige and G. Bradski, “ORB: and efficient alternative to SIFT or SURF”, IEEE Int. Conf. on Computer Vision, 2011.

[2] D. G. Lowe, “Distinctive Image Features from Scale-Invariant Keypoints”, Int. Journal of Computer Vision, Vol.50, No. 2, 2004, pp.91-110.

[3] T.-J. Kim, C. Baek, S. Chun, K.-H. Lee, J.-I. Hwang, K. Kwon, Y.-H. Kim, H.-S. Park, Y. Shin, S. Ryu, J.-Y. Lee, G. Hwang, G. Kim, “A timing controller embedded driver IC with 3.24-Gbps eDP interface for chip-on-glass TFT-LCD applications”, J SOC INF DISPLAY, Vol. 24, pp. 299-306, 2016, doi: 10.1002/jsid.446

[4] D. Lee, K. Lee, D. H. Baek, H. Pae, J. Lim, Y. M. Choi, Y. H. Lee, S.I. Lee, J. Lee, K. Nah and G. Hwang, “A 1.4-Gbps intra-panel interface with low-power and low-EMI schemes for Tablet PC applications”, J SOC INF DISPLAY, Vol. 20, pp. 661-668, 2012, doi:10.1002/jsid.134

[5] Ryu, S.-Y., Baek, D.-H., Lim, H.-W., Han, S.-K., Ryu, K.-H., Park, K.-H., Park, J.-Y., Lee, J.-M., Kim, T-J., Lee, J.-Y., and Kim, G.-N., “A 13-bit universal column driver for various displays of OLED and LCD”, J SOC INF DISPLAY, Vol. 24, pp. 277–285, 2016, doi: 10.1002/jsid.437

[6] M. Wittmeir, “Image Analysis to Support Functional Safety for Automotive Displays”, Proceedings of electronic displays Conference, WEKA, Munich, 2018, ISBN 978-3-645-50169-9

[7] Boual, S. , Large, T. , Buckingham, M. , Travis, A. and Munford, S., “Wedge Displays as Cameras”, SID Symposium Digest of Technical Papers, Vol. 37, pp. 1999-2002, 2006, doi:10.1889/1.2433445

[8] T. Nishibe and H. Nakamura, “Value-added integration of functions for silicon-on-glass (SOG) based on LTPS technologies”, J SOC INF DISPLAY, Vol. 15, pp. 151-156, 2007, doi:10.1889/1.2709736

[9] N. Boston, “A Mathematical Foundation for Watermarking”, Preprint (http://www.math.wisc.edu/~boston/bostonpreps.html).

[10] Galand, Fabien, and Gregory Kabatiansky. "Information hiding by coverings", *Information Theory Workshop, 2003.* IEEE, 2003.

[11] F. Petitcolas, R. Anderson and M. Kuhn, “Information Hiding - A Survey”, Proceedings of the IEEE, special issue on protection of multimedia content, 87(7):1062–1078, July 1999.

[12] ISO 26262:2011 / ISO/FDIS 26262:2018, Road Vehicles -- Functional Safety. International Standard 2011 / 2018.

[13] ISO 16505:2015, Road Vehicles – Ergonomic and performance aspects of Camera Monitor Systems – Requirements and test procedures. International Standard, 2015.

[14] K. Witt, J. Bauer, “A Robust Method for Frozen Frame Detection in Safety Relevant Video Streams Based on Digital Watermarking”, Electronic Display Conference, Nuremberg, 2017

[15] B. Kaiser, “Functional Safety of Camera Monitor Systems”, In: A. Terzis (Ed.), “Handbook of Camera Monitor Systems - The Automotive Mirror-Replacement Technology based on ISO 16505”, Springer 2016.