

# UNTERSUCHUNGSBERICHT

## RESEARCH REPORT

Nr./No.: 2021 22410/6130

- 1 Initiative/**  
*Initiative*
- DGUV TEST Prüf- und Zertifizierungsstelle  
Fachbereich Bauwesen  
c/o BG BAU - Berufsgenossenschaft der Bauwirtschaft  
Prävention  
Am Knie 6  
81241 München
- 2 Untersuchungsobjekt/**  
*Research specimen*
- 2.1 Hersteller/  
*Manufacturer*
- Liebherr-France SAS,  
2 avenue Joseph Rey - B.P. 90287  
FR – 68005 Colmar
- Liebherr-Hydraulikbagger GmbH  
Liebherrstraße 12  
DE – 88457 Kirchdorf/Iller
- Volvo Construction Equipment Germany GmbH  
Max-Planck-Strasse 1  
DE – 54329 Konz
- Wacker Neuson Linz GmbH  
Flughafenstraße 7  
A – 4063 Hörsching
- als Mitglieder der Arbeitsgemeinschaft  
Machines in Construction MiC 4.0  
powered by VDMA und HDB
- 2.2 Bezeichnung/  
*Designation*
- Anbaugeräteschnittstelle MiC 4.0 Attachment Protocol
- 2.3 Kennzeichnung/  
*Marking*
- MiC 4.0 Attachment Protocol
- 2.4 Weitere Angaben/  
*Further details*
- 
- 3 Kurzbeschreibung des**  
**Untersuchungsobjekts/**  
*Description of the*  
*research specimen*
- Spezifikation des Kommunikationsprotokolls einer standardi-  
sierten Datenschnittstelle auf Basis des CAN-Bus und des  
SAE J1939-Protokolls für Anbaugeräte an Baumaschinen  
(Anbaugeräteschnittstelle).

Die standardisierte Datenschnittstelle dient zur Kommunikation von Steuergeräten an Baumaschinen mit Schnellwechseleinrichtungen und den daran angebrachten Anbaugeräten

#### **4 Untersuchung/ Research**

##### **4.1 Ziel der Untersuchung/ Objective of research**

Untersuchung, ob das vorgestellte Untersuchungsobjekt

- ausreichende Maßnahmen zur Erkennung der anzunehmenden Übertragungsfehler und
- eine ausreichend niedrige Restfehlerrate

für Sicherheitsfunktionen mit einem Performance Level d vorsieht.

##### **4.2 Untersuchungsgrundlagen/ Research requirements**

- [1] DIN EN ISO 13849-1:2023-12, Sicherheit von Maschinen – sicherheitsbezogene Teile von Steuerungen Teil 1: Allgemeine Gestaltungsleitsätze
- [2] DIN EN ISO 19014-4:2021-01, Erdbaumaschinen - Funktionale Sicherheit - Teil 4: Gestaltung und Beurteilung von Software und Datenübertragung für sicherheitsrelevante Steuerungssysteme
- [3] GS-ET-26:2014-03, Grundsätze für die Prüfung und Zertifizierung von „Bussystemen für die Übertragung sicherheitsbezogener Nachrichten“

##### **4.3 Umfang der Untersuchung/ Extant of research**

Konzeptbeurteilung

#### **5 Untersuchungsergebnis/ Research result**

Das vorgestellte Untersuchungsobjekt mit den beiden Datentypen I und II ist geeignet für eine logische Verbindung zur Realisierung von Sicherheitsfunktionen mit einem Performance Level d verwendet werden zu können.

##### **Besondere Hinweise/ Special remarks**

Die Hinweise Nr. 1 bis 5 in Abschnitt 7 des Untersuchungsberichts sind zu berücksichtigen.

#### **6 Anlagen/ Enclosures**

-

Im Auftrag

Sachbearbeiter



Dipl.-Ing. Thomas Bömer



Dipl.-Ing. Karl-Heinz Büllesbach



Dr. Andreas Schmid

## 7 Untersuchungen und Ergebnisse

### 7.1 Aufgabenstellung

Aufgabe des IFA war die Beurteilung des vorgestellten Kommunikationsprotokolls bezüglich des erreichbaren Performance Levels nach DIN EN ISO 13849-1. Die Untersuchung fand im Zeitraum von Oktober 2021 bis Juli 2024 auf Basis der bereitgestellten Herstellerdokumentation im IFA statt.

### 7.2 Umfang der Untersuchung

Untersuchungsobjekt ist die in [DOK01] bereitgestellte Spezifikation des Kommunikationsprotokolls MiC 4.0 Attachment Protocol zur sicherheitsgerichteten Kommunikation von Steuergeräten an Baumaschinen mit:

- den angebrachten Schnellwechseleinrichtungen,
- den angebrachten Adapter- und End-Werkzeugen,
- einer externen Anbaugeräte-Erkennungshardware und
- optional einem zusätzlichen Display, z. B. zur Parametrisierung oder zur Ansteuerung von Sonderfunktionen.

*Hinweis 1: Das Untersuchungsergebnis gilt nur für die spezifizierte direkte Kommunikation zwischen einer Datenquelle und einer Datensenke im Netzwerk (peer-to-peer).*

Zum Umfang der Untersuchung gehören nicht:

- Beurteilung der Kommunikation mit anderen Kommunikationspartnern als den oben genannten Geräten, z. B. Kommunikationspartner in einer Cloud zur Realisierung einer höheren Kommunikationsebene,
- Beurteilung der Funktionalen Sicherheit der steuerungstechnischen Implementierung in Hard- und Software aller an der Ausführung des Kommunikationsprotokoll notwendigen Befehlsgeräten (Sensoren), Steuergeräten, Aktoren etc.,
- Beurteilung der Definition des sicheren Zustands einer Baumaschine mit Schnellwechseleinrichtung, Anbaugeräte bzw. Anbauwerkzeug,
- Beurteilung der sicherheitsgerichteten Parametrierung (z. B. Verfahren und Werkzeug zur Festlegung der Source Adresse eines CAN-Bus-Knotens),
- Beurteilung von Konformitätsbewertungskriterien und -tests für die Realisierung von MiC 4.0 Komponenten,
- Beurteilung der Anforderungen durch Produktnormen an bestimmte Maschinentypen, z. B. wenn die Baumaschine durch Anbringen eines bestimmten Anbaugeräts zu einer anderen Maschine wird, z. B.: Anbaugerät Palettengabel, sofern relevant.

*Hinweis 2: Das Untersuchungsergebnis gilt nicht für eine eventuelle Nutzung des proprietären Datenbereichs im MiC 4.0 Attachment Protocol.*

*Hinweis 3: Es empfiehlt sich, für die Realisierung von MiC 4.0 Komponenten Konformitätsbewertungskriterien und -tests zu spezifizieren.*

## 7.3 Beschreibung des Untersuchungsobjekts

### 7.3.1 Allgemeines

Baumaschinen werden mit Schnellwechseleinrichtungen ausgestattet, um einen schnellen Austausch der Anbaugeräte bzw. der Anbauwerkzeuge (z. B. Löffel, Greifer, Hydraulikhammer etc.) von unterschiedlichen Herstellern zu ermöglichen.

Die oben genannten Hersteller haben ein herstellerübergreifendes und maschinenunabhängiges Protokoll zur Kommunikation von Steuergeräten der Baumaschinen mit den Schnellwechseleinrichtungen (en: quick coupler) und den daran angebrachten Anbaugeräten spezifiziert. Abbildung 1 zeigt den vorgesehenen Bereich der Kommunikation vom Steuergerät der Baumaschine bis hin zum Anbaugerät.

Untersuchungsobjekt ist die Spezifikation dieses Kommunikationsprotokolls der Datenschnittstelle bzw. Anbaugeräteschnittstelle auf Basis des CAN-Bus und des SAE J1939-Protokolls.

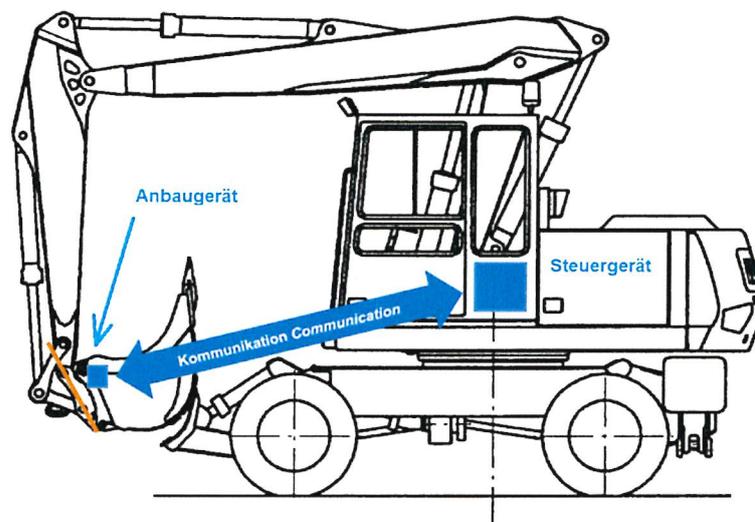


Abbildung 1: Definition des Kommunikationsbereichs des Untersuchungsobjekts  
(Quelle: [DOK09])

Es ist vorgesehen, dass mehrere Werkzeuge in Reihe aufgenommen werden können und das Steuergerät der Baumaschine mit diesen kommuniziert. Dabei wird zwischen Adapter-Werkzeugen (en: sandwich tool), die weitere Werkzeuge aufnehmen können und End-Werkzeugen (en: end tool) unterschieden. Im Rahmen des MiC 4.0 Attachment Protocols wird maximal eine Werkzeug-Kette von zwei Adapter-Werkzeugen und einem End-Werkzeug betrachtet.

Das MiC 4.0 Attachment Protocol ist geschlossenes proprietäres Kommunikationsprotokoll, d.h. auf einem MiC 4.0 Bus dürfen nur MiC 4.0 Teilnehmer miteinander kommunizieren.

Das Untersuchungsobjekt basiert auf dem SAE J1939-Protokoll. Das Untersuchungsobjekt nutzt die in SAE J1939DA:2019-02 (DA = digital annex) definierten Source Adressen (SA), Parameter Gruppen (PGN) und Suspect Parameter (SPN), als auch zusätzlich definierte SA, PGNs und SPNs. Diese werden im freien Bereich des SAE J1939 angelegt.

### 7.3.2 Grundlagen des SAE J1939-Kommunikationsprotokolls

Quelle: [DOK10] bis [DOK12]

Das Kommunikationsprotokoll SAE J1939 definiert die Kommunikation auf einem CAN-Bus (Controller Area Network, ISO 11898) in Nutzfahrzeugen zur Übermittlung von Steuerungsinformationen und Diagnosedaten. SAE J1939 verwendet den CAN-Bus als physikalische Schicht und definiert, welche Daten und wie diese Daten zwischen den elektronischen Steuergeräten (Electronic Control Unit, ECU) innerhalb eines Fahrzeugnetzwerks ausgetauscht werden. Typische zu steuernde Geräte sind der Motor, die Bremse, das Getriebe, usw.

Besondere Merkmale von SAE J1939 sind:

- Nutzung der erweiterten CAN-Identifizier (29 Bit),
- standardisierte CAN-Baudraten von 250 kBit/s und 500 kBit/s,
- Peer-to-Peer- und Broadcast-Kommunikation,
- Transportprotokolle für bis zu 1785 Datenbytes,
- Buszugriffskontrolle über eigenes Netzwerkmanagement,
- Definition von Parametergruppen für Nutzfahrzeuge und andere,
- Unterstützung herstellerspezifische Parametergruppen,
- Diagnosefunktionen.

SAE J1939-21 definiert ein Schema zur Interpretation des 29-Bit-CAN-Identifiziers. Mittels der sogenannten Parametergruppe wird der CAN-Identifizier in verschiedene Segmente unterteilt. Dabei stellt nur ein Teil des 29-Bit-CAN-Identifizier die eigentliche Parametergruppe dar, der Rest wird als Quelladresse, Zieladresse, Priorität und Data Pages (DP/EDP) interpretiert.

Jede Parametergruppe kann durch eine eindeutige Nummer, die Parameter-Gruppennummer (PGN), identifiziert werden. Bit 24 „Data Page“ (DP) und Bit 25 „Extended Data Page“ (EDP) sind ebenfalls Bestandteil der PGN und werden als die beiden höchstwertigen Bits der PGN mitgezählt. Der PGN-Zahlenbereich wird durch die beiden „Data Page“-Bits in vier PGN Seiten eingeteilt, wobei für SAE J1939 nur drei genutzt werden.

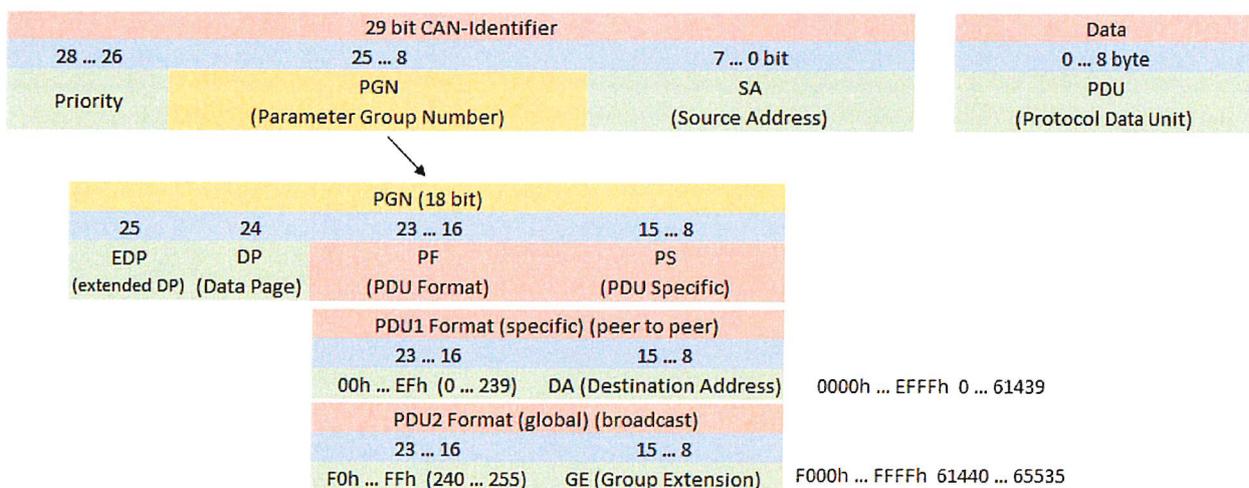


Abbildung 2: Interpretation des 29-Bit-CAN-Identifiziers

Entsprechend Abbildung 2 gibt es zwei Arten von Parameter-Gruppennummern, die durch das PDU Format Feld (PF), das PDU Specific Feld (PS), die Data Page (DP) und die Extended Data Page (EDP) bestimmt werden:

- **PDU1 Format: spezifische PGNs** sind für Parametergruppen bestimmt, die an bestimmte Geräte gesendet werden (peer-to-peer). Der Wert im PDU Format Feld beträgt 239 oder kleiner und der Wert im PDU Specific Feld beträgt 0. Hieraus ergeben sich 240 verschiedene spezifische PGNs innerhalb einer PGN Seite.
- **PDU2 Format: globale PGNs** identifizieren Parametergruppen, die an alle Teilnehmer gesendet werden (Broadcast). Bei globalen PGNs beträgt der Wert im PDU Format Feld 240 oder größer und der Wert im PDU Specific Feld repräsentiert eine Gruppenerweiterung (Group Extension). Hieraus ergeben sich  $16 \times 256 = 4096$  verschiedene globale PGNs innerhalb einer PGN Seite.

### 7.3.3 Sicherheitsrelevante Daten

Um eine sichere Kommunikation zu ermöglichen, unterteilt das Untersuchungsobjekt die über den Bus zu übertragenen Daten in fünf Datentypen (0 bis IV).

- **Datentyp 0**  
nicht sicherheitsrelevant
- **Datentyp I (sicherheitsrelevante Standardnachrichten)**  
Datenfelder, die in der Datenbasis [DOK02] mit Datentyp I gekennzeichnet sind, sind sicherheitsrelevant und werden für Funktionen, Befehle und notwendige Daten verwendet. Die gesendeten Daten dieses Typs sind nur gültig, wenn sie mindestens zweimal identisch empfangen werden.  
*Anmerkung: Entsprechend der Datenbasis [DOK02] wird für Daten des Typs I eine Zykluszeit von 20 ms bzw. 1000 ms festgelegt. Es ist spezifiziert, dass bei Überschreiten der Timeout-Zeit eine sicherheitsgerichtete Reaktion erfolgt.*
- **Datentyp II (sicherheitsrelevante Steuerdaten für z. B. hydraulische Funktionen)**  
Datenfelder, die in der Datenbasis [DOK02] mit Datentyp II gekennzeichnet sind, sind sicherheitsrelevant. Dieser Typ wird z. B. für hydraulische Steuerungen und Werte verwendet, bei denen aufgrund des kontinuierlichen Charakters der Steuerbefehle derselbe Wert nicht immer zweimal identisch übertragen werden kann, ohne dass es zu Verzögerungen kommt. Aufgrund der Trägheit des hydraulischen Systems wird eine falsche Übertragung keine gefährliche Bewegung verursachen. Daher müssen die Daten mindestens zweimal korrekt, aber nicht identisch, innerhalb der Timeout-Zeit empfangen werden.  
*Anmerkung: Entsprechend der Datenbasis [DOK02] wird für Daten des Typs II eine Zykluszeit von 20 ms mit einer Toleranz von +/- 10% festgelegt. Es ist spezifiziert, dass bei Überschreiten der Timeout-Zeit eine sicherheitsgerichtete Reaktion erfolgt.*
- **Datentyp III**  
für z. B. nicht sicherheitsrelevante Sensordaten
- **Datentyp IV**  
für nicht sicherheitsrelevante Nachrichten im CMDT Transport Protocol, enthält Maschinendaten wie z. B. Seriennummer

*Hinweis 4: Die Festlegung des Datentyps erfolgt in der Datenbasis [DOK02]. Diese Festlegung ist von den Komponenten-Herstellern zu berücksichtigen. [DOK02] enthält weiterhin MiC4.0-Nachrichten des Datentyps I (PGN: C000, FF26) ohne die spezifizierte 4-Bit CRC. Dies wird seitens des IFA als Fehler in [DOK02] interpretiert.*

## 7.4 Durchgeführte Untersuchungen

Im Rahmen der Untersuchung wurden folgende Teiluntersuchungen durchgeführt:

- Beurteilung der qualitativen Aspekte der Datenkommunikation (Datentyp I und II) (Maßnahmen zur Beherrschung der anzunehmenden Übertragungsfehler)  
→ siehe Abschnitt 7.4.1,
- Beurteilung der quantitativen Aspekte der Datenkommunikation (Datentyp I und II) (Bewertung der erreichten Restfehlerrate)  
→ siehe Abschnitt 7.4.2,
- Beurteilung der Anforderungen an die die Kommunikation ausführende Steuerung  
→ siehe Abschnitt 7.4.3.

### 7.4.1 Beurteilung der qualitativen Aspekte der Datenkommunikation

*Anmerkung: Für Datentyp I spezifiziert [DOK01] eine zusätzliche fehlererkennende Maßnahme gegen dauerhaft fehlerhafte unterschiedliche Telegramminhalte („Toggeln“).*

#### 7.4.1.1 Übertragungsfehler Wiederholung (en: repetition)

Das Untersuchungsobjekt spezifiziert die Maßnahme Laufende Nummer (en: message counter) zur Beherrschung des Fehlers Wiederholung bei der Übertragung der sicherheitsgerichteten Datentypen I und II.

#### 7.4.1.2 Übertragungsfehler falsche Reihenfolge (en: incorrect sequence)

Das Untersuchungsobjekt spezifiziert die Maßnahme Laufende Nummer (en: message counter) zur Beherrschung des Fehlers falsche Reihenfolge bei der Übertragung der sicherheitsgerichteten Datentypen I und II.

#### 7.4.1.3 Übertragungsfehler Verlust (en: loss)

Das Untersuchungsobjekt spezifiziert die Maßnahme Laufende Nummer (en: message counter) zur Beherrschung des Fehlers Verlust bei der Übertragung der sicherheitsgerichteten Datentypen I und II.

#### 7.4.1.4 Übertragungsfehler Verzögerung (en: delay)

Das Untersuchungsobjekt spezifiziert die Maßnahme Zeiterwartung (en: timeout monitoring) zur Beherrschung des Fehlers Verzögerung bei der Übertragung der sicherheitsgerichteten Datentypen I und II.

#### 7.4.1.5 Übertragungsfehler Einfügung (en: insertion)

Das Untersuchungsobjekt spezifiziert die Maßnahme Laufende Nummer (en: message counter) zur Beherrschung des Fehlers Einfügung bei der Übertragung der sicherheitsgerichteten Datentypen I und II.

#### 7.4.1.6 Übertragungsfehler Nachrichtenverfälschung (en: corruption)

siehe Abschnitt 7.4.2

#### **7.4.1.7 Übertragungsfehler Maskerade (en: masquerade)**

Das Untersuchungsobjekt spezifiziert folgende Maßnahmen zur Beherrschung des Fehlers Maskerade bei der Übertragung der sicherheitsgerichteten Datentypen I und II:

- Geschlossenes proprietäres Kommunikationsprotokoll, d.h. es dürfen nur MiC 4.0 Teilnehmer miteinander kommunizieren
- Laufende Nummer (en: message counter)

#### **7.4.1.8 Übertragungsfehler Adressierung (en: addressing)**

Das Untersuchungsobjekt spezifiziert folgende Maßnahmen zur Beherrschung des Fehlers Adressierung bei der Übertragung der sicherheitsgerichteten Datentypen I und II:

- Geschlossenes proprietäres Kommunikationsprotokoll, d.h. es dürfen nur MiC 4.0 Teilnehmer miteinander kommunizieren
- Laufende Nummer (en: message counter)

#### **7.4.2 Beurteilung der quantitativen Aspekte der Datenkommunikation**

[DOK01], 8.2.8 berechnet eine Restfehlerrate  $\Lambda = 0,9 \times 10^{-8} \text{ [h}^{-1}\text{]}$  für die Übertragung der sicherheitsgerichteten Datentypen I und II. Die vorliegende Berechnung ist nachvollziehbar dargestellt. Für die Übertragung der sicherheitsgerichteten Datentypen I und II erreicht das Untersuchungsobjekt eine für Performance Level d ausreichend niedrige Restfehlerrate einer logischen Verbindung zur Realisierung von Sicherheitsfunktionen.

#### **7.4.3 Beurteilung der Anforderungen an die die Kommunikation ausführende Steuerung**

Das Untersuchungsobjekt legt keine Anforderungen an die erforderliche funktional sichere steuerungstechnische Realisierung der Hard- und Software aller an der Ausführung des Kommunikationsprotokoll beteiligten Komponenten fest. Hierbei sind die Anforderungen nach [1] zu berücksichtigen.

*Hinweis 5: Gemäß [DOK01], Bild 8 sind die Telegramm bildenden Komponenten Teil der Sicherheitsschicht und damit in einer für das zu erreichende Sicherheitsniveau geeigneten Steuerungsstruktur zu realisieren.*

## 8 Technische Dokumentation

Folgend gelistet ist die für die Erstellung des Untersuchungsberichts wesentliche technische Dokumentation des Herstellers:

- [DOK01] Spezifikation „Draft\_Spec\_Attachment-Interface\_MiC (009)\_20240617.pdf“, Version 009, 17.06.2024, 201 Seiten,
- [DOK02] Spezifikation Datenbasis „MiC\_Database\_V046.xlsx“, V0.4.6, 11.06.2024,
- [DOK03] Spezifikation „MiC Message Layout\_V031.xlsx“, V0.3.0, 10.10.2023.
- [DOK08] Präsentation „MIC40\_Überblick.pdf“, 17.06.2021, 8 Seiten,
- [DOK09] Beschreibung „MIC4 - Cluster 7 Anbauwerkzeuge - Veröffentlichung\_NeueTimeline.pdf“, ohne Datum, 3 Seiten.

Weitere IFA interne Dokumentation zum Protokoll SAE J1939:

- [DOK10] Wikipedia SAE\_J1939.pdf,
- [DOK11] Vector\_Introduction\_to\_J1939.pdf,
- [DOK12] SAE J1939.docx.

Für die Untersuchungsergebnisse  
*For the research results:*



Dipl.-Ing. Karl-Heinz Büllsbach



Dr. Andreas Schmid