# Automatisierung im Schienenverkehr? Am besten mit Ende-zu-Ende-Absicherung!

*Gastbeitrag von Jens Lehmann*

Daten, die für die Sicherheit von Fahrzeugen und der Infrastruktur relevant sind, können dabei helfen, den Betrieb zu verbessern und Wartungen effizienter zu gestalten. Dazu zählen Anwendungsfälle auf der Grundlage von Funktionszyklen, Laufzeiten oder Positionsdaten. Um solche Daten jedoch ohne weitere manuelle Prüfung und somit kosteneffizient bereitzustellen, muss deren Vertrauenswürdigkeit während der gesamten Verarbeitung gewährleistet werden. Eine fachgerechte und normkonforme Entwicklung der entsprechenden Anwendungen ist notwendig, um ihre langfristige und nachhaltige Nutzung zu ermöglichen. Dafür braucht es jedoch auch mittel- bis langfristige Planungssicherheit und einheitliche Standards. Dieser Beitrag skizziert einen Ansatz für die Absicherung sicherheitsrelevanter Daten von Systemen auf Fahrzeugen oder der Infrastruktur, der sogenannten Operational Technology (OT), und deren Verarbeitung mit Cloud-Technologie.

## Normen geben Entwicklungsprozess vor

Sicherheitsrelevante elektronische Systeme und entsprechende Software sind im Anwendungsbereich der Bahn gemäß der Normen EN 50129 bzw. EN 50716 zu entwickeln. Techniken und Maßnahmen im Bereich der Datenkommunikation sind gemäß der Norm EN 50159 festzulegen. Das anzuwendende Sicherheits-Integritäts-Level (SIL) sowie das Security-Level (SL) sind bereits im Vorfeld gemäß der Normen EN 50126 bzw. EN 50701 herzuleiten. Auf der Grundlage von SIL und SL sind gemäß der Normen EN 50159, EN 50129 und EN 50716 wiederum die Techniken und Maßnahmen festzulegen, die während der Entwicklung von Elektronik und Software anzuwenden sind. Dazu zählen Methoden zum Management der Entwicklung sowie aufeinander abgestimmte Methoden für den Entwurf und zur Prüfung. Dabei ist es möglich und sinnvoll, die normkonformen Entwicklungsprozesse mit agilen Methoden zu kombinieren. Hingegen ist eine nachträgliche Qualifikation von Elektronik oder Software praktisch ausgeschlossen.

## Effizienz nur mit richtiger Methode

Die Auswahl der Methoden spielt bei der normkonformen Software-Entwicklung eine entscheidende Rolle. So erlaubt die Norm EN 50716, beziehungsweise bereits deren Vorgänger EN 50128 beziehungsweise EN 50657, durchaus eine Spezifikation beziehungsweise einen Entwurf ohne umfängliche Modellierung. Jedoch bilden Datenmodell, Datenfluss und Kontrollfluss die Grundlage für den Entwurf und die Analyse von Software. Werden diese erst spät im Rahmen der Vorbereitung von Analysen oder Tests hergeleitet, können Fehler entsprechend spät erkannt werden.

## Sichere Datenreise vom Zug zur Cloud

Die normkonforme Entwicklung sicherheitsrelevanter Systeme für Fahrzeuge und Infrastruktur ist Voraussetzung für deren Zulassung und seit Jahrzehnten gängige Praxis. Bisher sind solche Systeme für einen weiteren Datenaustausch gegebenenfalls noch etwas eingeschränkt.

Doch wie verhält es sich mit der Verarbeitung sicherheitsrelevanter Daten in Systemen wie einer Cloud, für die der Nachweis einer normkonformen Entwicklung nicht erbracht werden kann? Im Folgenden soll eine Möglichkeit skizziert werden, wie Daten aus einem sicherheitsrelevanten System in einer Cloud weiterverarbeitet und deren Integrität erhalten werden kann. Von einer Echtzeitverarbeitung zur Beeinflussung sicherheitsrelevanter Funktionen von Fahrzeugen oder der Infrastruktur wird dabei abgesehen.

Die Notwendigkeit, die Datenintegrität zu gewährleisten, ergibt sich aus der weiteren Verwendung der Daten. Dabei ergibt es Sinn, auf Standardisierung und Synergien zu setzen und nicht einzelne Anwendungsfälle singulär zu betrachten. Bei der Wertermittlung sollten eine lange Nutzungsdauer, eine Reduktion manueller Prüfungen sowie ein potenziell höherer Automatisierungsgrad berücksichtigt werden.

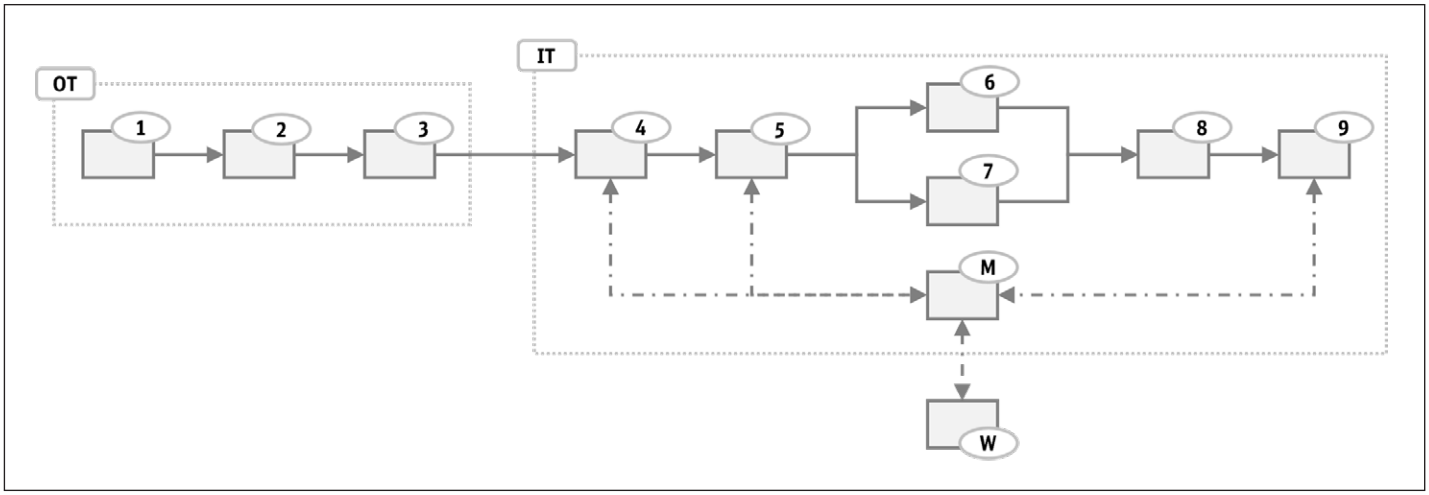


BILD: DB SYSTEMTECHNIK

Der Lösungsansatz leitet sich aus der Norm EN 50159 ab und dient prinzipiell der Erkennung und Beherrschung von Fehlern. Die folgenden Erläuterungen dazu können in der Grafik nachvollzogen werden. Werden Daten auf dem Fahrzeug oder der Infrastruktur (OT) mit einer definierten Datenintegrität gewonnen (1), so müssen diese für die weitere Übertragung und Verarbeitung mit zusätzlichen Sicherheitsdaten und einem Sicherheits-Code (2) ergänzt werden. Anschließend sind diese Daten, vorzugsweise durch eine spezifische Einheit, mit einem kryptographischen Verfahren zu verschlüsseln (3) und an die Cloud (IT) zu übertragen. Nach der Übertragung und vor einer weiteren Verarbeitung in der Cloud sind die Daten zu entschlüsseln (4) und, auf Grundlage der Sicherheitsdaten und des Sicherheits-Codes, zu prüfen (5). Für die weitere Verarbeitung (6) wird eine geeignete Plausibilisierung (7) und (8) gefordert. Daran schließen sich wiederum die Ergänzung von Sicherheitsdaten und eines Sicherheits-Codes (9) an.

Es ist zu beachten, dass die Anwendungs-Software normkonform entwickelt werden muss. Dies schließt auch die weiteren Funktionen bzw. Software-Einheiten ein, welche die Verarbeitungssequenzen beziehungsweise den Datenfluss zur Laufzeit überwachen. Diese Überwachung (M – Monitoring) in der Cloud muss wiederum durch eine wechselseitige Überwachung (W – Watchdog) mit einer vollständig normkonform entwickelten Einheit abgesichert werden, beispielsweise auf der Grundlage eines Prozessrechners außerhalb der Cloud.

Von einer Entwicklung gemäß Basisintegrität wird hier generell abgesehen, da sich eine angemessene Datenintegrität aufgrund der anzuwendenden Techniken und Maßnahmen kaum ableiten lässt.

Als eine ideale Datenquelle kann das European Train Control System (ETCS) verstanden werden. Da eine flächendeckende Ausrüstung aktuell jedoch nicht absehbar ist, soll folgend eine Möglichkeit skizziert werden, die Integrität von Positionsdaten auf einem Fahrzeug abzusichern und zur weiteren Verarbeitung bereitzustellen. Dabei wird davon ausgegangen, dass weder die Hardware noch die Software entsprechender Empfänger normkonform entwickelt wurden. Die Umstände bzw. die Eignung für eine Integration in ein Fahrzeug sind vorab zu betrachten. Der Empfänger wird hier als Sensor abstrahiert, und es wird davon ausgegangen, dass die Positionsdaten nicht für eine direkte Beeinflussung sicherheitsrelevanter Funktionen des Fahrzeugs verwendet werden.

## Ende-zu-Ende-Absicherung – am Beispiel ETCS

Der Fokus liegt auf der Fragestellung, wie solche Daten durch eine geeignete Plausibilisierung abgesichert werden können. Hier kommen als weitere Datenquellen beispielsweise ein terrestrisches Zeitsignal, ein Modell der Gleise sowie fahrdynamische Eigenschaften des Fahrzeugs in Betracht. Die Plausibilisierung ist auf einer normkonform entwickelten Einheit durchzuführen. Die so gewonnenen Daten sind dann wie beschrieben abzusichern, an die Cloud zu senden und dort wiederum zu prüfen. Eine daran anschließende Plausibilisierung mit gesicherten Planungsdaten geben letztlich Aufschluss über die Integrität der Positionsdaten. Das Ergebnis der Plausibilisierung ist wiederum wie beschrieben abzusichern. =

Jens Lehmann ist CDO für Digitale Produkte und Services bei der DB Systemtechnik GmbH in München.