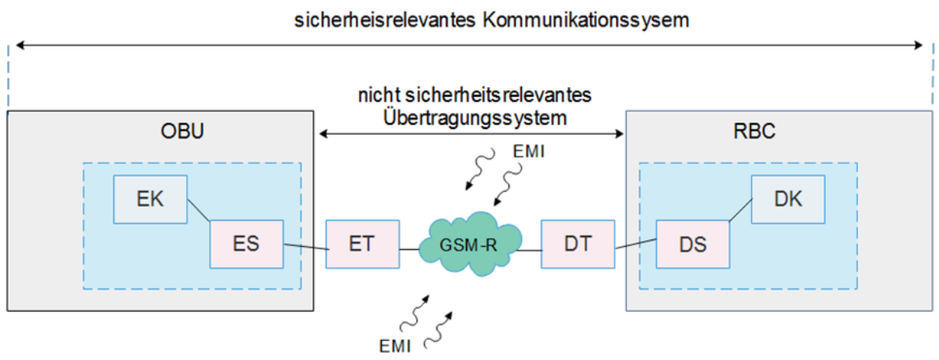
Masterarbeit

Entwurf von technischen Testszenarien zum Nachweis der praktischen Anwendung von ETCS Level 2 mit Hochleistungsblock (HBL) im S-Bahn-Verkehr

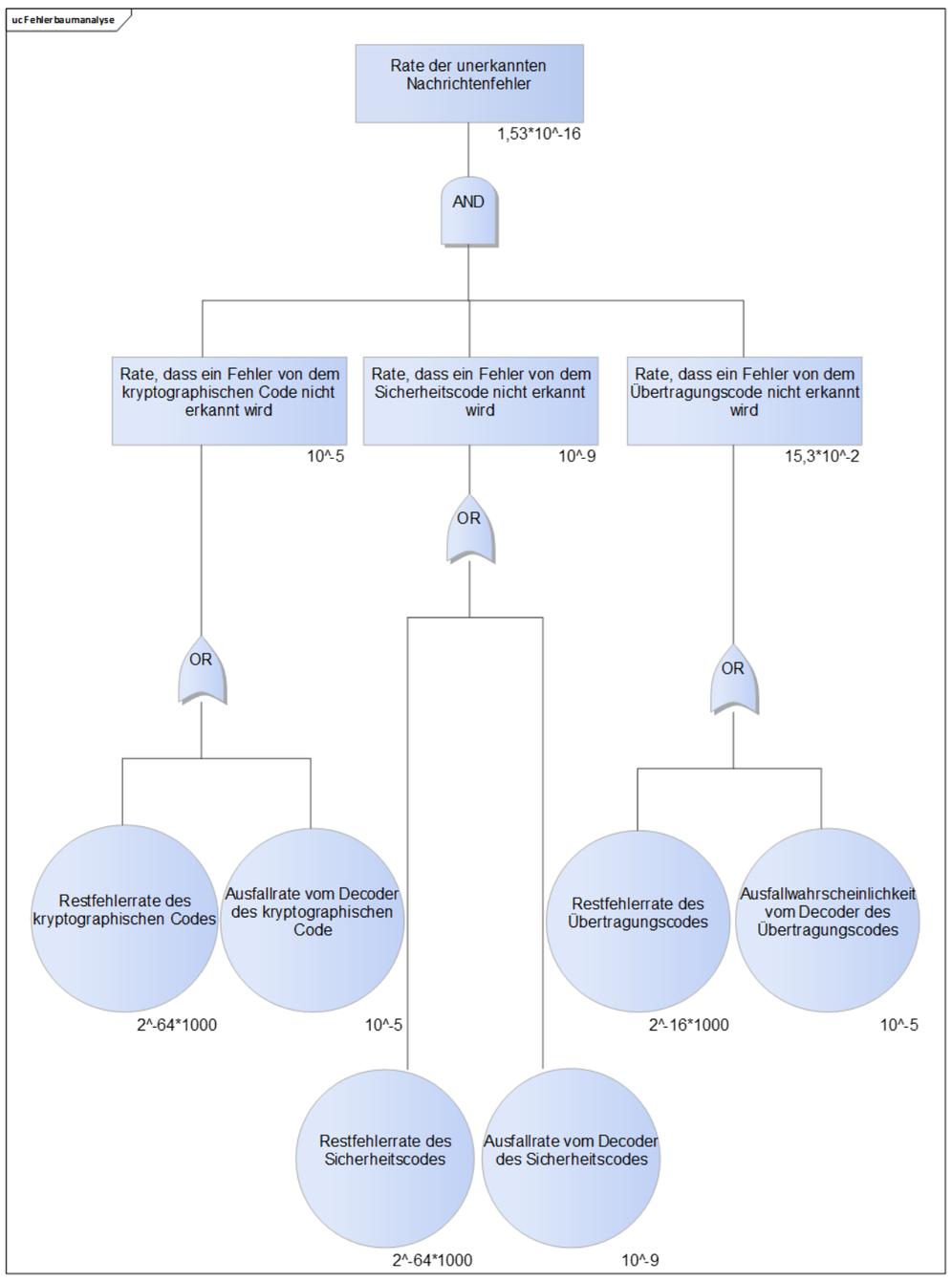
Das Hauptziel dieser Arbeit ist, den Nachweis zu erbringen, dass die Gefährdungsrate der Datenübertragung zwischen OBU (On-Board-Unit) und RBC (Radio-Block-Center) auch bei einer erhöhten Anzahl von Datentelegrammen (im Vergleich zum üblichen ETCS-Betrieb) aufgrund des Einsatzes von ETCS (European Train Control System) im Level 2 mit HBL bei S-Bahnen die vorgegebene maximale tolerierbare Gefährdungsrate nicht überschreitet. Angenommen sind 1.000 Telegramme/Stunde. Die für diesen Anwendungsfall durchgeführten quantitativen Sicherheitsanalysen für zwei Systemarchitekturvarianten mit dem Markov-Verfahren (mit und ohne absorbierenden Zustand) und der Fehlerbaumanalyse haben gezeigt, dass das vorgegebene Sicherheitsziel, bezogen auf die funktionale Sicherheit des ETCS-Systems, auch bei einem Einsatz von ETCS im Level 2 mit HBL bei S-Bahnen erreicht wird. Im Folgenden werden die Ergebnisse der Fehlerbaumanalyse und des Markov-Verfahrens (mit absorbierenden Zustand) für eine Variante dargestellt. Als Top-Ereignis und unklarer Zustand werden hierbei die unerkannten Nachrichtenfehler betrachtet. Die Parameter zur Quantifizierung dieser Methode sind die Rate der zufälligen Hardware-Fehler und die Wahrscheinlichkeiten des Nichterkennens eines Nachrichtenfehlers durch den Code. Außerdem spielt die Rate des Auftretens von Sicherheitsmechanismen beim Markov-Verfahren eine wichtige Rolle.

Foto: Cansu Köse

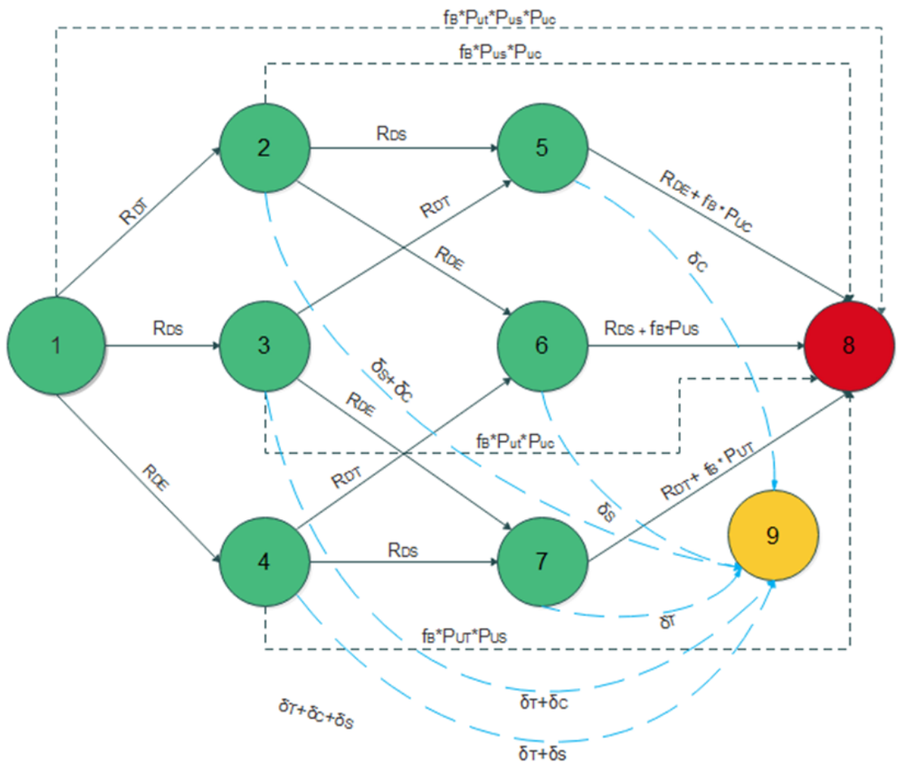


EK: Encoder des kryptographischen Codes
ES: Encoder des Sicherheitscodes
ET: Encoder des Übertragungscodes
EMI: Elektromagnetische Interferenzen
DK: Decoder des kryptographischen Codes
DS: Decoder des Sicherheitscodes
DT: Decoder des Übertragungscodes

Modell des sicherheitsrelevanten Kommunikationssystems



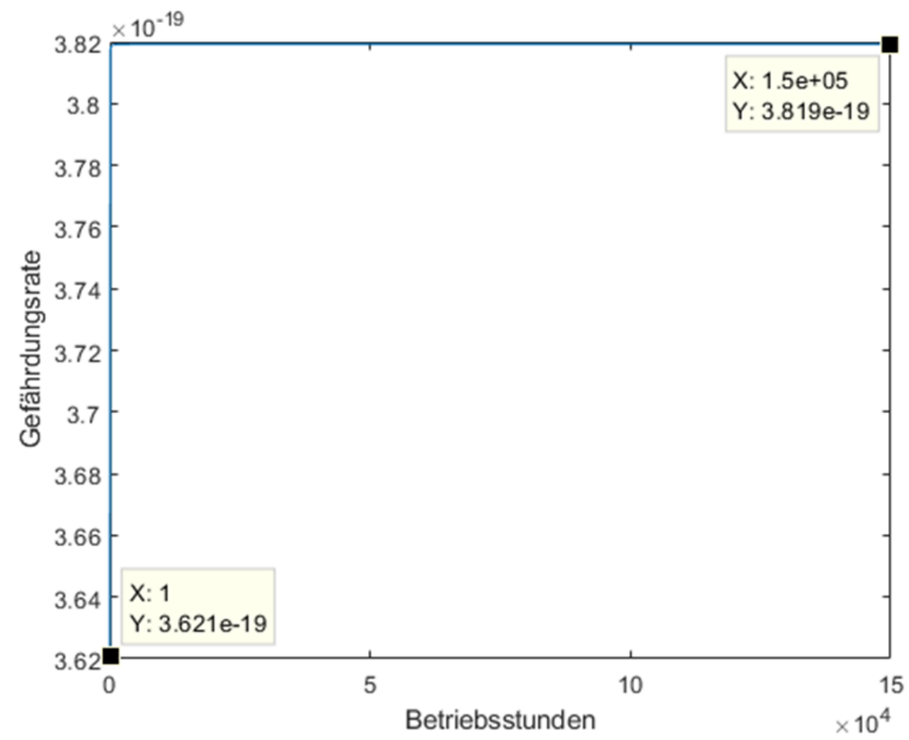
FTA der unerkannten Nachrichtenfehler sowie seiner Basisereignisse



Legende:

betriebsfähiger Zustand; Klarzustand
absorbierender Zustand
nicht verfügbarer Zustand; Unklarzustand

Übergangsgraph des Markov-Verfahrens für Variante 1



Rate der unerkannten Nachrichtenfehler nach Markov-Verfahren

Ergebnis: Das System entspricht dem SIL4. Die Sicherheitsanforderungen werden hiermit für diesen Anwendungsfall erfüllt.

Masterarbeit von cand. M.Sc. Cansu Köse

Betreut von Prof. Dr. -Ing. Ullrich Martin

Praxispartner: Dipl. -Ing Stefan Pröttel

Bearbeitungszeitraum 01 - 06/2018

Vorgelegt an der Universität Stuttgart

Institut für Eisenbahn- und Verkehrswesen

E-2017/08