Auszug aus

Risikoorientierte Systematik zur Bewertung von Rückfallebenenkonzepten des Bahnbetriebs

Von der
Fakultät Architektur, Bauingenieurwesen und Umweltwissenschaften
der Technischen Universität Carolo-Wilhelmina
zu Braunschweig

zur Erlangung des Grades eines
Doktor-Ingenieurs (Dr.-Ing.)
genehmigte

Dissertation

von
Po-Chi Huang
geboren am 12. April 1983
aus Taichung City

Eingereicht am: 06. Dezember 2019
Disputation am: 26. Februar 2020

Berichterstatter/in: Prof. Dr.-Ing. Jörn Pachl
Prof. Dr.-Ing. Birgit Milius

2020

Kurzfassung

Durch die zunehmende Anwendung von Informationstechnik (IT) im Eisenbahnwesen bekommt auch die Frage nach ausreichender und gewährleisteter IT-Security einen neuen und wichtigen Stellenwert. Die Bedrohung der IT-Security und ihre Auswirkung auf den Bahnbetrieb sind mittlerweile durch die gesetzlichen Anforderungen und die IT-Security-Vorfälle der Vergangenheit den Fachleuten sehr bewusst. Unabhängig von den getroffenen Vorkehrungen muss davon ausgegangen werden, dass nicht jeder Angriff tatsächlich festgestellt und abgewendet werden kann. Dies bedeutet, dass der Bahnbetrieb nach einem vermuteten oder tatsächlichen IT-Angriff teilweise oder ggf. komplett in der Rückfallebene betrieben werden muss.

Das Rückfallebenenkonzept des Bahnbetriebs hat die Bestrebung, den Bahnbetrieb trotz des Einflusses der vorgegebenen Unregelmäßigkeiten stets mit einer annehmbaren kollektiven Betriebsqualität aus Sicherheit, Leistungsniveau und Verfügbarkeit zu erzielen. Das heutige Rückfallebenenkonzept des Bahnbetriebs ist darauf ausgelegt, die bisher anzunehmenden betrieblichen Einschränkungen, in der Regel Safety-Ereignisse und deren Folgen, zu beherrschen. Das sind zumeist kleinräumige und kurzzeitig andauernde Störungen. Wird der Kreis der möglichen Ursachen nun um den IT-Angriff erweitert, dann ist zu erwarten, dass der zukünftige Bahnbetrieb nicht nur häufig in der Rückfallebene durchgeführt werden muss, sondern auch häufiger mit Mehrfachausfällen von Betriebsfunktionen sowie großräumigen und lang andauernden Störungsszenarien konfrontiert sein wird.

Um die Qualitäten des künftigen Störungsbetriebs systematisch bewerten zu können, wurde im Rahmen dieser Arbeit, gefördert mit dem Grant der Karl-Vossloh-Stiftung (2017-2019), eine risikoorientierte Systematik zur Bewertung von Rückfallebenenkonzepten des Bahnbetriebs entwickelt. Diese Bewertungssystematik ermöglicht die zusammenhängende Berücksichtigung des Störungsszenarios, der systemtechnischen Auslegung, des dynamischen IT-Umfelds, der Charakteristiken des IT-Angriffs sowie die Auslastung der Menschen. Die Anwendung der Bewertungssystematik verfolgt im Wesentlichen das Ziel, die Anwender bei der Gestaltung und der Entscheidungsfindung von Rückfallebenenkonzepten in einer aktuellen dynamischen Betriebslage durch eine schnelle, aber aussagekräftige Risikoschätzung zu unterstützen.

Abstract

Due to the increased use of information technology (IT) in railway systems, the need for sufficient and ensured IT security for railway operation has gained significance in recent years. The railway experts are currently very conscious of the threat of IT security and its impact on railway operations due to the legal requirements and the incidents that happened in the past. Regardless the precautions it must be assumed that not every attack can be detected and averted. As a result, the railway operation might need to be operated partly or completely in degraded mode in case of an assumed or real IT attack.

The purpose of railway operational concepts in degraded mode is to achieve an acceptable operational quality while considering the criterion safety, performance and availability despite the impact of known irregularities during operation. Today's operational concepts in degraded mode are generally designed to deal with irregularities in operation resulting non-intentional safety events and their related impacts. Those irregularities are mostly disturbances restricted to a small area with a very short duration. However, if we consider possible irregularities resulting IT attacks in future operation, the railway operation might need to be operated in the degraded mode not only more frequently but also in longer durations, due to facing complex and large-scale disturbances.

In order to evaluate the operational quality of the railway operation in degraded mode systematically, a risk-oriented systematic has been developed within this thesis, which was funded by the Karl-Vossloh-Stiftung (2017-2019). This systematic enables a joint consideration of operational concepts, system design, dynamic IT environment, characteristic of IT attacks and workload of the staff in the degraded operation. The use of this approach aims to provide a simplified risk evaluation process with a meaningful basis for decision making when choosing the operational concept in degraded mode.

Inhaltsverzeichnis

6 Fazit und Ausblick

Durch die zunehmende Anwendung von IT im Eisenbahnwesen bekommt auch die Frage nach ausreichender und gewährleisteter IT-Security einen neuen und wichtigen Stellenwert. Die Bedrohung der IT-Security und ihre Auswirkung auf den Bahnbetrieb sind mittlerweile durch die gesetzlichen Anforderungen und die IT-Security-Vorfälle der Vergangenheit den Fachleuten sehr bewusst. Unabhängig von den getroffenen Vorkehrungen muss davon ausgegangen werden, dass nicht jeder Angriff tatsächlich festgestellt und abgewendet werden kann. Dies bedeutet, dass der Bahnbetrieb nach einem vermuteten oder tatsächlichen IT-Angriff teilweise oder ggf. komplett in der Rückfallebene betrieben werden muss.

Das Rückfallebenenkonzept des Bahnbetriebs hat die Bestrebung, den Bahnbetrieb trotz des Einflusses der vorgegebenen Unregelmäßigkeiten stets mit einer annehmbaren kollektiven Betriebsqualität aus Sicherheit, Leistungsniveau und Verfügbarkeit zu erzielen. Wenn jedoch die Technik nicht mehr oder nur zum Teil funktioniert, dann haben die menschlichen Akteure in der Rückfallebene des Bahnbetriebs die Aufgabe, den Bahnbetrieb in Eigenverantwortung mit oder ohne technische Unterstützung fortzuführen. Das heutige Rückfallebenenkonzept des Bahnbetriebs ist darauf ausgelegt, die bisher anzunehmenden betrieblichen Einschränkungen, in der Regel Safety-Ereignisse und deren Folgen, zu beherrschen. Das sind zumeist kleinräumige und kurzzeitig andauernde Störungen. Wird der Kreis der möglichen Ursachen nun um den IT-Angriff erweitert, dann ist zu erwarten, dass der zukünftige Bahnbetrieb nicht nur häufig in der Rückfallebene durchgeführt werden muss, sondern auch häufiger mit Mehrfachausfällen von Betriebsfunktionen sowie großräumigen und lang andauernden Störungsszenarien konfrontiert sein wird.

Um die Qualitäten des künftigen Störungsbetriebs unter der Bedrohung eines IT-Angriffs systematisch bewerten zu können, wurde im Rahmen dieser Arbeit eine risikoorientierte Systematik zur Bewertung von Rückfallebenenkonzepten entwickelt. Diese Bewertungssystematik ermöglicht die zusammenhängende Berücksichtigung des Störungsszenarios, der systemtechnischen Auslegung, des dynamischen IT-Umfelds, der Charakteristiken des IT-Angriffs sowie die Auslastung der Menschen. Die Anwendung der Bewertungssystematik verfolgt im Wesentlichen das Ziel, die Anwender bei der Gestaltung und der Entscheidungsfindung von Rückfallebenenkonzepten in einer aktuellen dynamischen Betriebslage durch eine schnelle, aber aussagekräftige Risikoschätzung zu unterstützen.

Mit der genannten Zielsetzung begann die Arbeit in Kapitel 2 mit der grundlegenden taxonomischen Differenzierung zwischen Safety und Security sowie deren Bedeutung im Bahnbetrieb. Um die Herausforderung des künftigen Störungsbetriebs unter dem Einfluss eines IT-Angriffs im Vorfeld zu verstehen, wurden als Erstes die Charakteristiken des IT-Angriffs analysiert und deren Unterschiede zu dem bisherigen Safety-Ereignissen in den Punkten Wahrscheinlichkeit, Offenbarung, Ausmaß, Priorität und Dauer herausgestellt. Anschließend wurden die grundlegende Aufgabe, die Bestandteile und die Struktur des Bahnbetriebs sowie

dessen Rückfallebenen aus den funktionalen, gesellschaftlichen und rechtlichen Aspekten eingehend hergeleitet.

Kapitel 3 schließt an mit dem theoretischen Hintergrund der Bewertungssystematik. Beginnend mit der Herleitung der Anforderungen an die Bewertungssystematik, damit sichergestellt werden kann, dass die Variablen und die Aussagen der Bewertungssystematik die wesentlichen Eigenschaften des künftigen Störungsbetriebs angemessenen berücksichtigen. Das Ergebnis einer Ursache- und Wirkungsanalyse hat gezeigt, dass im künftigen Störungsbetrieb tendenziell häufiger komplexe, großräumige und lang andauernde Störungsszenarios zu erwarten sind und dies eine höhere Auslastung der Menschen im Störungsbetrieb verursachen kann. Das System Bahn, als Kritische Infrastruktur, hat aber neben dem sicheren Transport auch die Aufgabe, die Funktionalität und Stabilität der Gesellschaft durch ein angemessenes Leistungsniveau zu gewährleisten. Aufgrund dessen wurde das Konzept Risiko-Budgetierung aus dem Finanzwesen adaptiert und in der vorliegenden Arbeit zur proaktiven Steuerung von Betriebsrisiko sowie zur Erhöhung der Gestaltungsfreiheit von Rückfallebenenkonzepten vorgestellt. Die risikobasierte Bewertungssystematik zur Ermittlung des Betriebsrisikos besteht nach dem Risikomodell aus sieben Strukturteilen. Dazu gehören das Betriebsszenario, das Funktionsmodell, das Versagenspotenzial, die Anzahl der Versagen, das IT-Manipulationspotenzial, der Reduktionsfaktor und das Schadensausmaß. Um die Betriebsqualitäten von unterschiedlichen Rückfallebenenkonzepten intuitiv vergleichen zu können, werden die maßgeblichen Ergebnisse der Bewertung als Index dargestellt. Der Risikoindex zeigt die Sicherheit des Rückfallebenenkonzepts, der Leistungsindex bildet das Leistungsniveau des Rückfallebenenkonzepts ab und der Verfügbarkeitsindex stellt den Stand der technischen Verfügbarkeit dar.

Die Anwendung der Bewertungssystematik wurde anschließend in Kapitel 4 anhand einer großräumigen und lang andauernden Störung der Gleisfreimeldeanlage auf der freien Strecke zwischen zwei Zugmeldestellen demonstriert. Ausgehend von der Festlegung der grundlegenden Parameter des Betrachtungsbereichs und der Definition des Störungsszenarios wurden insgesamt zehn Basisvarianten und vier kombinierte Varianten von Rückfallebenenkonzepten für das vorliegende Störungsszenario konzipiert und anhand der Bewertungssystematik untersucht. Das Ergebnis des Variantenvergleichs hat gezeigt, dass der Bahnbetrieb unter der heutigen verfahrenstechnischen Einschränkung bzw. des heutigen Rückfallebenenkonzepts bei einer derartigen Störung, deren IT-Manipulationspotenzials sehr gering ist, zwar auf Dauer durchgeführt werden kann, jedoch nicht mehr leistungsfähig ist.

Abschließend wurde in Kapitel 5 die Optimierungsmöglichkeit der Betriebsqualitäten in Bezug auf die Anwendung der Bewertungssystematik diskutiert. Ebenfalls wird das Konzept einer temporären Räumungsprüfstelle auf der freien Strecke, mit der die Betriebsdichte einer Strecke im Fall einer großräumigen Störung ohne die Änderung der Beförderungsgeschwindigkeit erhöht werden kann, eingehend vorgestellt und analysiert. Das Ergebnis der Untersuchung zeigte, dass das Konzept nach den bestehenden Regelwerken betrieblich realisierbar ist, insofern die zugehörigen technischen Systeme es funktionell unterstützen.

Insgesamt ergibt sich, als Schlussfolgerung dieser Arbeit, dass die vorgestellte Bewertungssystematik ihren Anwendern ermöglicht, künftig bei der Gestaltung von Rückfallebenenkonzepten neben dem Störungsszenario, auch das dynamische IT-Umfeld, die Charakteristiken des IT-Angriffs, die menschliche Auslastung und die systemtechnische Auslegung zusammenhängend zu berücksichtigen. Die Bewertungssystematik unterstützt den Anwender bei der Gestaltung und Entscheidungsfindung von Rückfallebenenkonzepten mit einer schnellen, aber wissenschaftlichen fundierten Qualitätseinschätzung. Sollte der künftige Bahnbetrieb unter der Bedrohung eines IT-Angriffs tatsächlich häufig in den komplexen, großräumigen und lang andauernden Störungsszenarios durchgeführt werden müssen, dann lassen sich eine risikoorientierte Gestaltung von Rückfallebenenkonzepten und eine proaktive Steuerung von Betriebsrisiken durch die Anwendung dieser Bewertungssystematik realisieren.

Als Ausblick für zukünftige Forschung und die Praxisanwendung der Bewertungssystematik steht nach wie vor die Herausforderung, wie das menschliche Versagenspotenzial in den Rückfallebenen genau einzuschätzen ist, aus. Da die Menschen im Vergleich zu den technischen Systemen in der Regel ein deutlich höheres Versagenspotenzial haben, werden die Lösungsräume der Rückfallebenenkonzepten aufgrund des risikoorientierten Bewertungsansatzes von dem Versagenspotenzial der Menschen wesentlich beeinflusst. Im Angesicht der zunehmenden Automatisierung, Digitalisierung, Virtualisierung und der daraus resultierenden Änderung des menschlichen Arbeitsverhaltens im Bahnbetrieb muss hinterfragt werden, ob und wie lange die heutigen Kenntnisse über das menschliche Versagenspotenzial im Bahnbetrieb noch gelten werden.

Trotz allem, stellt das IT-Manipulationspotenzial im Bahnbetrieb mit seiner Unberechenbarkeit den größten Unsicherheitsfaktor bei der Einschätzung des Betriebsrisikos dar. Da das Thema IT-Security zum jetzigen Zeitpunkt im Bahnbereich noch recht neu ist und es bisher keine umfassenden Kenntnisse über das tatsächliche Geschehen auf einer komplett digitalisierten Bahninfrastruktur gibt, muss der Einfluss des IT-Angriffs auf das Betriebsrisiko künftig im Laufe der technischen Migration noch weiter verfolgt und genau untersucht werden. Letzten Endes besteht künftig weiterhin die Herausforderung einer gesellschaftlichen Debatte über die Qualitätsanforderung der Bahn als Kritische Infrastruktur, in der auch das Thema Risiko-Budgetierung einzuschließen ist. Wird der künftige Bahnbetrieb unter der Bedrohung des IT-Angriffs häufig mit der großräumigen und lang andauernden Störung konfrontiert, dann ist eine genaue Abwägung zwischen dem Funktionieren und dem Risiko des Bahnbetriebs nach der gesellschaftlichen Wertvorstellung unerlässlich.