Zur Risikobestimmung bei Security-Analysen in der Eisenbahnsignaltechnik

Sebastian Saal[1] Dennis Klar[2] Markus Seemann[3] Michaela Huhn[2]
[1] Institut für Theoretische Informatik, Technische Universität Braunschweig
[2] Institut für Informatik, Technische Universität Clausthal
[3] IC MOL RA R&D, Siemens AG

Abstract: Die CORAS-Methode [LSS11] unterstützt eine systematische, defensive Risikoanalyse, die insbesondere zur Ermittlung von IT-Security-Anforderungen eingesetzt wird. Sie ermöglicht eine Risikobeurteilung auf Basis einer Systemanalyse und der Identifikation der zu schützenden Werte. Dafür wird ein System schrittweise in sogenannten Bedrohungsdiagrammen auf Schwachstellen untersucht. Danach erfolgt die Risikobewertung auf Grundlage des möglichen Schadenausmaßes und der zu erwartenden Häufigkeit von Angriffen.

In einer Fallstudie zur Risikoanalyse von IT-Security-Bedrohungen in sicherheitsrelevanten Systemen haben wir festgestellt, dass sich das Schadenausmaß durch die genaue Identifikation der Schutzziele mit der CORAS-Methode gut ermitteln lässt, während sich die Bewertung der Angriffshäufigkeit als schwierig erweist. Wir schlagen daher vor, die Angriffshäufigkeit durch eine semi-quantitative Klassifikation in mehreren Aspekten zu bewerten. In diesem Beitrag beschreiben wir eine derartige Bewertung, die die Aspekte *Motivation, Mittel und Gelegenheit* berücksichtigt, und diskutieren verschiedene Funktionen zur Kombination der Klassifikationen. Anhand der Fallstudie aus der Eisenbahnsignaltechnik zeigen wir, dass aus dem abgeleiteten Klassifikationschema eine sinnvolle Risikobewertung von IT-Security-Bedrohungen für sicherheitskritische Systeme resultiert.

1 Einleitung

In der Eisenbahnsignaltechnik rückt die IT-Sicherheit zunehmend in den Fokus der Entwicklung. Durch die intensive Vernetzung und neuartige Dienste der Komponenten entstehen neben den zahlreichen Vorteilen, wie neue Funktionen, erhöhte Verfügbarkeit und geringere Kosten, insbesondere auch neue Risiken, die analysiert und behandelt werden müssen. Zusätzliche Schnittstellen, z. B. für die Fernwartung, und die Nutzung offener Kommunikationsnetze (Funkverfahren, öffentliche Netze usw.) bergen neue Möglichkeiten für IT-Security-Angriffe, die auch die funktionale Sicherheit beeinträchtigen können. Daher werden neue Ansätze für entwicklungsbegleitende Risikoanalysen bezüglich der (IT-) Security benötigt.

Der Rahmen für die Security-Analyse wird durch die bahnspezifischen Risikostandards und -normen EN 50129 [CEN03], EN 50159 [CEN10] und den Entwurf eines Schutzprofils in der VDE 0831-102 [VDE13] vorgegeben. Konzepte und Methoden bleiben jedoch domänenspezifisch, so dass viele verschiedene Verfahren mit ihren individuellen Vorteilen

und Nachteilen zum Einsatz kommen. Ein Beispiel sind diverse tabellarische Ansätze, die aber bei größeren Systemen schnell an Übersichtlichkeit verlieren.

Hier wollen wir CORAS [LSS11] einsetzen, eine universellen, modellbasierten Ansatz zur Riskoanalyse. CORAS bietet zwei entscheidende Vorteile: zum Einen eine strikte Methodik mit acht Schritten und einem Leitfaden zur Bearbeitung. Zum Anderen eine graphische Analyse mit spezialisierten Diagrammtypen und Symbolen, die vergleichsweise übersichtlich und leicht verständlich sind. Insbesondere gegenüber tabellarischen Ansätzen werden so die Einflüsse und Wechselwirkungen besser verdeutlicht.

Eine generelle Schwierigkeit bei Risikoanalysen zeigt sich beim Übergang von der informellen Analyse zu einer quantitativen Auswertung. Für die analysierten Ereignisse müssen Eintrittswahrscheinlichkeiten oder -häufigkeiten abgeschätzt werden. Eine direkte Abschätzung ist jedoch, wie auch die CORAS-Autoren feststellen, aus verschiedenen Gründen häufig nicht möglich (vgl. [LSS11] S. 207f.), etwa wenn es keine Erfahrungswerte gibt, weil das System neu oder substantiell verändert ist oder die Einsatzbedingungen abweichen. Ebenso ist es schwierig, wenn ein unerwünschtes Ereignis sehr selten auftritt, gravierende Konsequenzen hat oder sein Eintreten nicht (zuverlässig) detektierbar ist.

Ein weiterer kritischer Punkt im Bereich IT-Security ist der Umgang mit den „technisch-abstrakten“ Größen der Wahrscheinlichkeit oder Häufigkeit an sich. Anders als bei Safety-Analysen müssen menschlich-psychologische Aspekte einfließen. Die Bandbreite einer möglichen Motivation hinter Security-Angriffen ist groß; teils sind sie von rationalen Kosten-Nutzen-Abwägungen geprägt (z. B. Wirtschaftskriminalität), teils extern motiviert oder gar irrational (z. B. „Spieltrieb“ bis hin zu Terrorismus).

Daher verfolgen wir in diesem Beitrag einen Ansatz, der *Einflussfaktoren* wie etwa die Motivation, die Gelegenheit oder die notwendigen Mittel für einen Angriff explizit in die Abschätzung von Security-Risiken – auch in der Systementwicklung – einbezieht. Die Wahrscheinlichkeiten werden aus verschiedenen Einflussfaktoren abgeleitet, die separat qualitativ abgeschätzt werden, z. B. durch begriffliche Einordnung in eine von mehreren Stufen (Levels). Anschließend erfolgt die Verrechnung der Einflussfaktoren mit einer geeigneten Gewichtung zu einem Häufigkeitslevel.

Ziel dieses Beitrags ist es darüber hinaus, die Anwendbarkeit von CORAS auf Systeme der Eisenbahnsignaltechnik zu demonstrieren. Dabei soll, im Hinblick auf die typische Anwendung bei Neuentwicklungen, ein auf „*Human Factors*“ basierender Ansatz in die quantitative Risikoanalyse von CORAS integriert werden. In Abschnitt 2 wird zunächst die CORAS-Methode vorgestellt. Abschnitt 3 erläutert die Anwendung von CORAS und die benötigten Erweiterungen. In den Abschnitten 4 und 5 folgt eine Fallstudie und eine Diskussion der Ergebnisse.

2 Risiko-Analyse nach CORAS

Die CORAS-Methode [LSS11] wurde entwickelt, um die Analyse von IT-Security-Risiken und -Bedrohungen zu erleichtern. Die Schwerpunkte sind einerseits einfache Kommunikation und Dokumentation, andererseits eine Formalisierung der Analyse.

2.1 Der CORAS-Ansatz

CORAS orientiert sich an den zu schützenden Werten (Assets), ist defensiv[1] ausgerichtet und implementiert den ISO 31000 Standard [Int09] zum Risikomanagement. Die Durchführung setzt auf „strukturiertes Brainstorming“ und intensive Modellierung.

Der CORAS-Ansatz hat drei Bestandteile: (1) die (graphische) Sprache, die mehrere Diagrammtypen für die Risikomodellierung zur Verfügung stellt, (2) die übergreifende Methode, um Risiken zu identifizieren und zu bewerten, und (3) ein erstes Modellierwerkzeug (Editor) auf Eclipse-Basis.

Die Methode definiert insgesamt acht Arbeitsschritte, die sich wie folgt in drei grobe Phasen einteilen lassen:

1. *Kontext-Ermittlung* (Schritte 1–4): Gegenseitige Einführung in Methode und Zielsystem durch Analysten und Auftraggeber. Erstanalyse der Schutzziele (assets).
2. *Risikoanalyse* (Schritte 5–7): Risiken identifizieren, abschätzen und bewerten.
3. *Risikobehandlung* (Schritt 8): Gegenmaßnahmen finden und bewerten.

CORAS bietet eine eigene Diagrammsprache, die sich an UML-Use-Case-Diagramme und die Idee von Misuse-Case-Diagrammen anlehnt. Insgesamt fünf Diagramm-Typen stehen zur Verfügung: Asset, Threat, Risk, Treatment und Treatment-Overview. Die Diagrammtypen bauen aufeinander auf, d. h. sie werden in den Arbeitsschritten sukzessive abgeleitet und ergänzt. In den Diagrammen werden kausale Zusammenhänge und Abfolgen modelliert, wie ursprüngliche Bedrohungen auf die zu schützenden Werte einwirken können. Abbildung 1 zeigt die zur Verfügung stehenden Modellierungsmittel im logischen Zusammenhang. Im Einzelnen sind das:

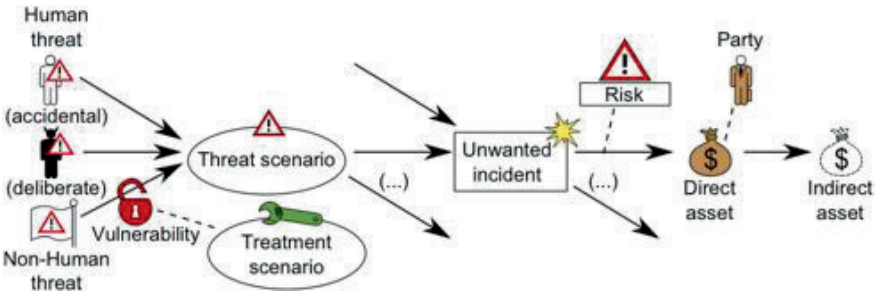


Abbildung 1: CORAS-Symbole im Überblick (©: CORAS [LSS11])

- Alle *Bedrohungen* (threats) gehen von Angreifern aus und sind entweder absichtlicher, unabsichtlicher oder technischer Art.
- Angreifer nutzen *Schwachstellen* (vulnerabilities), um sich Zugriff zu einem System zu verschaffen.

[1] Schutz von vorhandenen Werten, im Gegensatz zur Abwägung von Handlungsoptionen („offensiv“)

- Ein *Bedrohungsszenario* (threat scenario) beschreibt die Art oder den Ablauf eines Angriffs. Es fasst eine Folge von Ereignissen zusammen, die von einer Bedrohung ausgelöst wird und einen Beitrag zu einem unerwünschten Ereignis leistet. Szenarien können weiter zu einem Netzwerk aufgesplittet werden, um das mögliche Zusammenwirken genauer zu erfassen.
- Durch den Angriff wird ein *unerwünschtes Ereignis* (unwanted incident) ausgelöst, z.B. eine Gefährdung tritt ein. Unter Berücksichtigung einer Wahrscheinlichkeit und eines Schadensausmaßes erwächst daraus ein *Risiko* (risk).
- Durch das unerwünschte Ereignis sind unmittelbar die *direkten Schutzziele* (assets) wie Vertraulichkeit, Systemintegrität, usw. bedroht und mittelbar aber auch *indirekte Schutzziele* (z. B. Reputation).
- Eine *Partei* (party) entspricht einem Stakeholder, der ein besonderes Interesse an einem oder mehreren Schutzzielen hat.
- *Gegenmaßnahmen* (treatment szenarios) repräsentieren die Mittel und Abläufe, um Schwachstellen zu behandeln.

Verschiedene High-Level-Modellierungskonzepte und eine formale Semantik komplettieren die CORAS-Methode.

2.2 Behandlung von Wahrscheinlichkeiten in CORAS

CORAS unterstützt die qualitative und quantitative Bewertung der modellierten Bedrohungen. Ziel ist es, die Risiken zu bewerten, die von den unerwünschten Ereignissen ausgehen. Dazu muss für jedes dieser Ereignisse das zu erwartende Schadensausmaß und die Wahrscheinlichkeit oder die Eintrittshäufigkeit bestimmt werden. In Anbetracht der schwierigen Direkt-Abschätzung wird vorgeschlagen, die quantitative Bewertung anhand einer schrittweisen Berechnung auf Basis des Bedrohungsdiagramms vorzunehmen (siehe [LSS11], Kap. 13). Als Best-Practice wird Folgendes vorgeschlagen:

- Den Kanten (initiates-/leads-to-Beziehungen) im Threat-Diagramm soll jeweils eine Wahrscheinlichkeit zugeordnet werden. Der Wert gibt die *bedingte Wahrscheinlichkeit* für eine erfolgreiche Fortsetzung des Angriffs entlang dieser Kante an.
- Für die Knoten, die Bedrohungsszenarien und die unerwünschten Ereignisse, kann dann die Wahrscheinlichkeit oder Häufigkeit abgeleitet werden. Dabei gibt der errechnete Wert an, wie wahrscheinlich - unter den gegebenen Kantenwahrscheinlichkeiten - das Erreichen eines Knotens über einen beliebigen gerichteten Pfad im Threat-Diagramm ist.

Randbedingungen für die Wahrscheinlichkeitsberechnung sind die statistische Unabhängigkeit oder der wechselseitige Ausschluss der Szenarien auf eingehenden Pfaden. Auch die (Un-) Vollständigkeit der Analyse ist zu berücksichtigen. Abbildung 2 zeigt ein Beispiel.

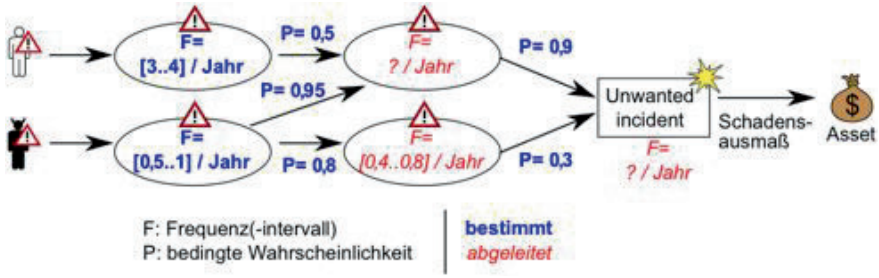


Abbildung 2: Beispiel für die Berechnung von Wahrscheinlichkeiten nach CORAS

3 Einflussfaktoren für die Häufigkeitsbewertung

Die CORAS-Methode ist ein allgemeiner Ansatz zur Risikoanalyse, der in vielen Domänen einsetzbar ist. Allerdings verlangt diese Allgemeinheit auch methodische Verfeinerungen bei der Anpassung an spezielle Aufgabenbereiche.

3.1 Strukturiertes Vorgehen bei der Risikoidentifikation

Im Prozess der Risikoanalyse werden mögliche IT-Security-Bedrohungen für das untersuchte System identifiziert. CORAS verwendet in dieser Phase *Threat-Diagramme*, um den Verlauf und die Auswirkungen auf die festgelegten Schutzziele darzustellen.

Für die Anwendung im Bereich der Eisenbahnsignaltechnik, in der häufig komplexe und verteilte Systeme vorhanden sind, bietet es sich an, den Verlauf eines Signals zu verfolgen: Beginnend an dem Ort des Entstehens (z. B. Sensor am Gleis, siehe Achszähler-Fallstudie in Abschnitt 4) bis zur Verarbeitung der Informationen (z. B. im Achszählrechner). Bei jeder zwischenzeitlich durchlaufenen Komponente muss hinterfragt werden, ob und – wenn ja – wie eines der festgelegten Schutzziele verletzt werden kann. Diese Pfade werden im *Threat-Diagramm* festgehalten, das als Basis für eine Bewertung dienen kann.

3.2 Ein neuer Klassifikationsansatz zur Häufigkeitsbewertung

Das Ziel der Risikoanalyse ist eine Klassifikation für vorhandene Risiken. Das Risiko ist wie auch in risikobasierten Ansätzen zur funktionalen Sicherheit [Int06] definiert als

$$\text{Risiko} = \text{Schadensausmaß} \times \text{Häufigkeit}.$$

Die CORAS-Methode fordert entsprechend, dass jedes unerwünschte Ereignis (*Unwanted Incident*) in einem *Threat-Diagramm* mit einer Wahrscheinlichkeit oder Häufigkeit (Likelihood) und einem Schadensausmaß zu versehen ist. Eine Klassifizierung der zu erwartenden Schäden bei bestimmten Ereignissen ist relativ leicht möglich und ist im Bereich der Safety-Analysen bereits etabliert.

Es gibt auch in der Eisenbahnsignaltechnik bereits Ideen, die Risikoberechnung statt auf Wahrscheinlichkeiten auf mehreren beitragenden Faktoren aufzubauen [BS12]. Diese Idee wird hier übernommen und ein neues Bewertungsmodell entworfen, das sogenannte *Häufigkeitslevel* definiert. Die Bestimmung erfolgt durch Abschätzung von drei Parametern:

- **Parameter Motivation (m)**: Beschreibt die *Motivation* eines potentiellen Angreifers, eine gewisse Handlung auszuführen, um ein bestimmtes *Angriffsziel* zu erreichen. Damit ist auch ein persönlicher *Gewinn* verbunden, den sich der Angreifer von seinem Handeln verspricht.
- **Parameter Werkzeuge (w)**: Kategorisiert die für die Handlungen des Angreifers erforderlichen *Geräte*, *Mittel* oder auch *Fähigkeiten*, die für die Umsetzung seines Vorhabens erforderlich sind. Das beinhaltet auch finanzielle Mittel und Know-how.
- **Parameter Zugang/Gelegenheit (z)**: Bewertet die Zugänglichkeit des Systems für einen Angreifer, der ein bestimmtes Threat Scenario ausführen will. Dazu zählen eventuelle Zugangskontrollen, Hindernisse, Zeitbedarf, Entdeckungsgefahr und andere Risiken für den Angreifer.

Die qualitative Bewertung kennt für jeden dieser Parameter sechs Stufen (von 0 bis 5), wobei höhere Zahlen für wahrscheinlichere Angriffe stehen. Die Null ist ein Sonderfall und bedeutet „nicht vorhanden“ oder „unmöglich“. Die Motivation wird dabei ausgenommen, da sie niemals gänzlich ausgeschlossen werden kann. Die Tabelle 1 gibt einen Überblick über die Stufen. Die Kalibirierung der Kategorien für die einzelnen Parameter („Wann spricht man von einer *hohen* Motivation oder einer *unwahrscheinlichen* Möglichkeit?“) ist pragmatisch für jede einzelne Anwendung vorzunehmen. Für andere Anwendungsbereiche oder vertiefende Analysen sind durchaus weitere Einflussfaktoren oder alternative Interpretationen denkbar.

Kategorie/ Häufigkeitslevel	**Motivation/Ziele (persönl. Gewinn)**	**Mittel, Werkzeuge, Fähigkeiten**	**Gelegenheit (Zugang, Möglichkeit)**
0	–	unmöglich	unvorstellbar
1	sehr gering	sehr schwierig	unwahrscheinlich
2	gering	schwierig	selten
3	mittel	mittel	mittel
4	hoch	einfach	gelegentlich
5	sehr hoch	sehr einfach	wahrscheinlich

Tabelle 1: Kategorien der einzelnen Parameter zur Likelihood-Bewertung

3.2.1 Berechnung eines Gesamthäufigkeitslevels

Von diesen Parametern ausgehend wird ein Gesamthäufigkeitslevel $h(m, w, z)$ abgeleitet, der für die Risikoberechnung (s. o.) genutzt werden kann. Der Wertebereich von h soll dazu wieder sechs Stufen umfassen (0 bis 5). Außerdem sollen die Parameter in gleicher

Gewichtung eingehen, d. h. dass kein Einfluss dominant hervorsticht. Schließlich soll eine Einzelbewertung von Null („unmöglich“) zu $h(m, w, z) = 0$ führen, was die Sonderstellung dieser Stufe betont.

Für die Gewichtung h wurden verschiedene Varianten untersucht [Saa12], u. a. Mittelwert-, Min/Max- oder Wurzelfunktionen. Am besten geeignet für die Fallstudie scheint der quadratische Mittelwert (s. Eq. (1)) mit Sonderregelung für die Stufe 0, der durch die Betonung von Ausreißern eine leicht „pessimistische“ Einschätzung bzgl. der erwarteten Gesamthäufigkeit aufweist. Für andere Anwendungen ist die Gewichtung h anzupassen. Das Ergebnis wird in einer Risikomatrix (Häufigkeitslevel $\times$ Schadenslevel) genutzt, um zu bestimmen, ob das Risiko noch akzeptabel ist.

$$h(m, w, z) = \begin{cases} 0, & \text{falls } w = 0 \ \vee \ z = 0 \\ \left\lfloor \sqrt{\frac{m^2+w^2+z^2}{3}} \right\rceil, & \text{sonst} \end{cases} \tag{1}$$

3.2.2 Anwendung im Threat-Diagramm

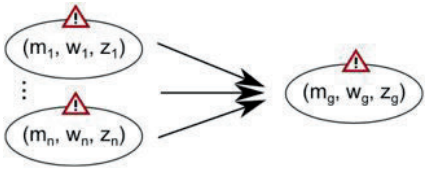
Für die Risikoberechnung mittels CORAS-Threatdiagrammen bedeutet unser neuer Ansatz, dass die Kausalkette eines Angriffs, von der Bedrohung über eine Folge von Bedrohungsszenarien zum unerwünschten Ereignis, nun anders bewertet wird. Für die Knoten im Netzwerk wird statt einer Wahrscheinlichkeit oder einer Eintrittshäufigkeit jeweils ein Häufigkeitslevel bestimmt, was durch Abschätzen der drei Parameter Motivation, benötigte Werkzeuge/Mittel und Zugang/Gelegenheit erreicht wird. Auf (Übergangs-) Wahrscheinlichkeiten an Relationen (vgl. Abschnitt 2.2) wird bei dieser Erweiterung verzichtet.

Die Bewertung läuft iterativ ab. In jedem Schritt muss ein lokales Tupel der Einflussfaktoren (m_g, w_g, z_g) bestimmt werden, und zwar relativ zu den Bewertungen (m_i, w_i, z_i) der unmittelbaren Vorgängerknoten ($i \in [1..n]$). Dazu findet zunächst eine „Initialisierung“ statt: jedem *Threat* wird eine spezifische Motivation (m) zwischen 1 und 5 zugewiesen (sofern zutreffend, sonst „mittel“). Die Anforderungen für benötigte Werkzeuge/Mittel (w) und Zugang/Gelegenheit (z) sind anfangs minimal (höchste Stufe 5). Die eigentliche Bewertung beginnt bei den ersten *Threat Scenarios*, die direkt mit einem *Threat* in Verbindung stehen und nur eingehende *initiates*-Kanten haben.

Dabei lautet die intuitive Bedingung, dass der Angriff durch die Fortsetzung nicht leichter werden kann. Folglich dürfen die Bewertungen des vorhergehenden Knotens nur übernommen oder reduziert werden. Mehrere eingehende Kanten werden als Oder-Verknüpfung interpretiert.[2] Die Bewertung sollte sich am leichtesten Pfad (mit den höchsten Einstufungen) orientieren. Uneindeutige Fälle müssen abgewogen werden, wobei die Maxima der Parameter m/w/z eine theoretische Obergrenze (siehe Abb. 3) vorgeben. Unabhängig davon ist immer eine situationsabhängige Korrektur nach unten möglich, wenn der Angriff in der Fortsetzung als „signifikant schwieriger“ bewertet wird.

Am Ende der Iterationen besitzen alle *Unwanted Incidents* eine Bewertung in (m, w, z)-Form. Aus diesen Parametern wird mit der im Abschnitt 3.2.1 aufgestellten Formel der

[2] Ein Angriff verläuft nur auf einem der Pfade. Parallele/koordinierte Angriffe werden nicht betrachtet.



$$m_g \leq \max_i m_i \,,$$
$$w_g \leq \max_i w_i \,,$$
$$z_g \leq \max_i z_i$$

Abbildung 3: Iterative Bestimmung der Level für die Einflussfaktoren

Gesamthäufigkeitslevel errechnet. Im Anschluss werden – wie in der CORAS-Methode vorgesehen – die Schadensausmaße festgelegt und für die verbundenen Assets die Risiken eingestuft (mittels Risikomatrix).

4 Fallstudie „Achszählsystem“

Im Folgenden wird exemplarisch ein Achszählsystem hinsichtlich seiner Security-Eigenschaften mit der vorgestellten Methode untersucht.

4.1 Überblick

Das Achszählsystem ist eine wichtige Komponente, die im Zusammenspiel mit anderen Einrichtungen die Sicherheit des Eisenbahnverkehrs gewährleistet. Mit diesem System wird das Freisein von Gleisabschnitten – den sogenannten Gleisfreimeldeabschnitten (GFM-A) – überprüft, so dass das Befahren eines besetzten Gleises durch die Stellwerkslogik verhindert werden kann. Das untersuchte Achszählsystem besteht grundsätzlich aus zwei Teilsystemen:

- **Außenanlage**: Am Gleis befinden sich ein Radsensor (RS), ein Gleisanschlussgehäuse (GAG) und die Kabelverbindung zum Stellwerksgebäude. Anschlussgehäuse und Sensor heißen zusammen auch Zählpunkt (ZP).
- **Innenanlage**: Dieser Teil ist im Stellwerksgebäude angeordnet und setzt sich aus einem oder mehreren Achszählrechnern zusammen. Diese verarbeiten die über die Kabelverbindung der Sensoren eingehenden Signale und werten daraus den Belegungszustand eines GFM-A aus.

In einer Bachelor-Arbeit [Saa12] wurde das Gesamtsystem untersucht. Hier soll die Außenanlage in Auszügen betrachtet werden, um die Anwendbarkeit der vorgestellten Anpassungen der CORAS-Methode darzulegen.

4.2 Modellierung der Außenanlage in einem Threat-Diagramm

Die Kontext-Ermittlung (Phase 1 der CORAS-Methode, siehe Abschnitt 2) liefert die zu schützenden Assets, hier die Systemverfügbarkeit (availability) und Systemintegrität (integrity) bzw. Korrektheit einer Funktion. Die Vertraulichkeit (confidentiality) spielt im vorliegenden Fall keine Rolle. Danach werden die möglichen Bedrohungen (Angreifer), Bedrohungsszenarien und unerwünschten Ereignisse identifiziert.

In Vorbereitung auf die auf Einflussfaktoren basierende Bewertung zur Häufigkeitsabschätzung können bei Bedarf noch die Parameterstufen angepasst werden. Die Stufe 2 soll u. a. für spezielle, aber beschaffbare Werkzeuge/Mittel stehen, die Stufe 5 u. a. für längeren ungehinderten Zugang. Die Stufe 0 entspricht höchsten Anforderungen oder Hindernissen, die die Umsetzung eines Szenarios (nahezu) unmöglich machen.

Die Bewertung wird für ein generisches Achszählsystem durchgeführt. Für exponierte Installationen unter extremen Bedingungen (z. B. bei Castortransporten) ist ggf. eine gesonderte IT-Security-Analyse durchzuführen, wobei einer starken politischen, und damit höheren Motivation einerseits, aber auch einem drastisch verstärkten Anlagenschutz andererseits, Rechnung getragen wird.

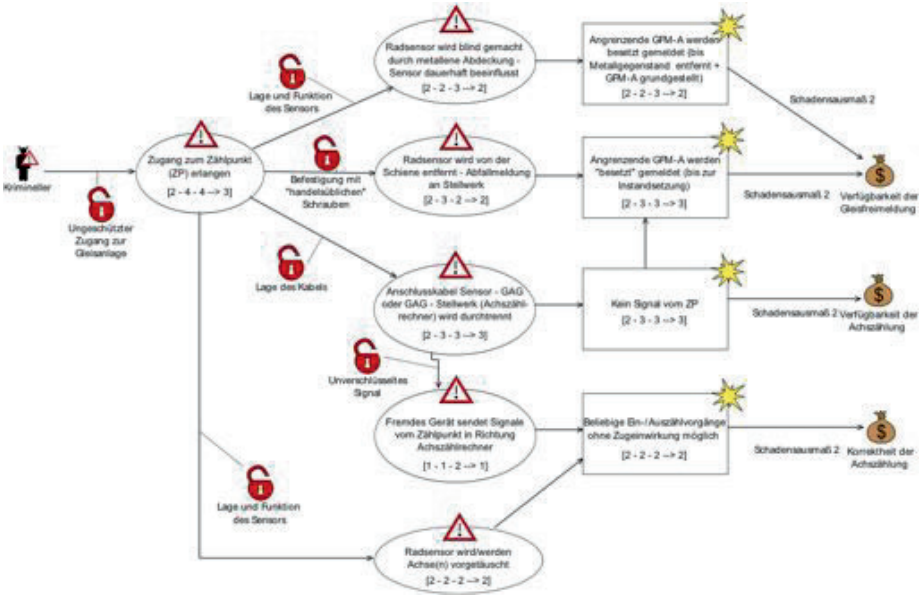


Abbildung 4: Threat-Diagramm der Außenanlage

4.2.1 Identifizierte Bedrohungen

Das Verfahren, dem Signalverlauf in der Anlage zu folgen (s. Abschnitt 3.1), liefert – unter Berücksichtigung der Schutzziele Korrektheit und Verfügbarkeit – ein Threat-Diagramm wie es in Abbildung 4 zu sehen ist. Der Signalverlauf ist dabei so, dass das Signal im Radsensor entsteht – durch eine erkannte Achse – und durch Kabel zum GAG und dann weiter in Richtung Stellwerk (Innenanlage) geleitet wird.

Im Diagramm erkennt man einen „kriminellen“ Angreifer, der beabsichtigt, die Außenanlage zu manipulieren. Zunächst muss die Außenanlage (Bahnstrecke) betreten werden, um Zugriff zum System am Gleis zu erhalten. Von hier aus gibt es mehrere Pfade zu verschiedenen Szenarien.

Der Angreifer könnte eines der Anschlusskabel durchtrennen oder von einem Anschluss abklemmen. Die Lage des Kabels – meist neben den Schienen oder in einem oberirdischen Kabelkanal – begünstigt diese Handlung. Die Nicht-Verfügbarkeit des Zählpunktes (ZP) für das Achszählsystem (*Unwanted Incident* „kein Signal vom ZP“) führt zu einer Besetztmeldung angrenzender Gleisfreimeldeabschnitte, da das System in den sicheren Zustand übergeht. Dies ist eine Beeinträchtigung der „Verfügbarkeit der Achszählung“.

Der Angreifer könnte aber auch weitergehen und, Kenntnisse vorausgesetzt, mit einem selbst hergestellten Gerät die Signale eines Zählpunktes imitieren (Beeinflussungszustand). Letzteres ermöglicht beliebiges Ein- und Auszählen von Achsen für einen Gleisfreimeldeabschnitt, sofern der GFM-A nach der Verbindungsunterbrechung durch den Fahrdienstleiter im Stellwerk grundgestellt wurde. Begünstigt wird dieses Szenario dadurch, dass sowohl zwischen Radsensor und dem Anschlussgehäuse als auch auf der Übertragungsstrecke zum Achszählrechner ein unverschlüsseltes, analoges oder digitalisiertes Signal verwendet wird.

Weitere Angriffspfade, die sich zum Teil auch überschneiden, können aus dem Diagramm abgelesen werden.

4.2.2 Zuweisung der Häufigkeitslevel

Im vorliegenden Diagramm (s. Abb. 4) sind die Parameter zur Bestimmung des Häufigkeitslevels sowie die Schadensausmaß-Kategorien bereits eingetragen. Die Notation der Parameter folgt dem Schema:

[Motivation - Werkzeuge - Gelegenheit --> errechneter Häufigkeitslevel]

Die Bewertung folgt dem Ablauf aus Abschnitt 3.2.2. Dem *Kriminellen* (Threat) wird eine mittlere Motivation (Stufe 3) zugewiesen. Werkzeuge und Zugang werden jeweils mit Stufe 5 initialisiert. Links beginnend wird zuerst das Szenario „Zugang zum Zählpunkt (ZP) erlangen“ bewertet:

Das Betreten der Außenanlage (Bahnstrecke) ist vergleichsweise leicht möglich, da sie nur einfache Barrieren besitzt (Absperrungen, Warn- und Verbotshinweise). Für den Zugang ist eine gewisse „Agilität“ (w=4) notwendig. Das System am Gleis hat keinen zusätzlichen

Schutz gegen unberechtigten Zugriff. Die zu erwartende Zugfrequenz schränkt jedoch die Gelegenheit (z=4) ein. Verbot und Gefahr erzeugen nur eine leichte Abschreckung (m=2) relativ zur Ausgangsmotivation. Insgesamt wird das Szenario mit (2-4-4) bewertet.

Mit dieser Bewertung wird nun die Betrachtung nachfolgender *Threat Scenarios* möglich, wovon wir „Anschlusskabel RS – GAG oder (...) wird durchtrennt“ auswählen. Es bedarf keiner großen Kenntnis der Eisenbahnsicherungstechnik, um zu erkennen, dass eine mit Kabeln angeschlossene Einrichtung wichtig für den Betriebsablauf sein wird. Allerdings wird zum Trennen des Kabels ein Hilfsmittel (w=3) benötigt. Der Zeitaufwand und die Arbeit direkt am Gleis erschweren den Zugang (z=3). Die Motivation ändert sich nicht (m=2). Das führt zu einer Bewertung des Szenarios mit (2-3-3).

Anders verhält es sich beim nächsten Szenario „Fremdes Gerät sendet Signale (...)“. Für diese Aktion ist die Fertigung eines speziellen Geräts notwendig, das die gesendeten Daten eines Zählpunktes imitiert. Dieser Angriff erfordert erheblich mehr Vorbereitung und technische Kompetenzen als die vorausgehenden Szenarien, u.a. Expertenwissen über die Anlage und den Betrieb (w=1). Die Gelegenheit wird herabgestuft, da die Installation eines eigenen Gerätes einige Zeit in Anspruch nehmen wird (z=2). Währenddessen besteht die Gefahr, von einem vorbeifahrenden Zug gesehen oder gar erfasst zu werden. Auch ein durch den Fahrdienstleiter herbeigerufenes Instandsetzungsteam die Manipulation entdecken (nach dem Verlust des Signals vom ZP und dem Übergang in den sicheren Zustand und nach erfolglosen Grundstell-Versuchen des Gleisfreimeldeabschnitts).

Die Motivation für das Threat-Scenario wurde auf 1 reduziert. Es ergibt sich zwar die Möglichkeit für einen Angriff auf die Korrektheit der Achszählung – mit einem „manipulierbaren Zählpunktimitator“ kann nach dem Einfahren eines Zuges in einen Gleisabschnitt dieser *scheinbar* am Ende ausgezählt werden – die Achszählung gibt dann nicht mehr den realen Belegungszustand wieder. Allerdings wird die Manipulation an einem *einzelnen Zählpunkt*[3] durch verschiedene Konsistenzprüfungen (Signalverläufe, Abgleich mit benachbarten Zählpunkten) sicher aufgedeckt. Insgesamt wird das Szenario daher mit (1-1-2) bewertet.

Analog wird bei der Bewertung der Häufigkeitslevel der anderen *Threat Scenarios* verfahren. Es verbleiben noch die *Unwanted Incidents*: Hier wurden die Bewertungen unverändert übernommen, da in dieser Fallstudie die unerwünschten Ereignisse stets eine direkte Folge der vorangehenden Szenarien sind. In zwei Fällen wurden die leichteren Pfade (mit den höheren Bewertungen) ausgewählt.

4.2.3 Schadensausmaße

Für das Achszählsystem werden folgende Kategorien für das Schadensausmaß festgelegt: 0 entspricht einer korrekten Meldung des Ist-Zustands, 1 beschreibt kurze Inkorrektheiten, die zum sicheren Zustand führen, und Kategorie 2 eine länger anhaltende, inkorrekte Achszählung, die auch in den sicheren Zustand führt und ggf. kleinere Reparaturen erfordert. Die höheren Kategorien 3 und 4 sind einer inkorrekten Achszählung vorbehalten, die in einen unsicheren Zustand führen (können).

[3] Für die Security-Analyse der übergeordneten Gleisfreimeldung ist auch die Manipulation von hintereinanderliegenden Zählpunkten zu betrachten.

Für alle *Unwanted Incidents*, die die Verfügbarkeit betreffen, wurde die Kategorie 2 gewählt. Diese Ereignisse verursachen Schäden, die innerhalb der Reparaturzeit behoben werden können, da sie vergleichbar mit einem möglichen technischen Defekt und dem damit verbundenen Austausch von Bauteilen sind.

Das Schadensausmaß für das Ereignis „Beliebige Ein-/Auszählvorgänge ohne Zugwirkung möglich“, das die Korrektheit der Achszählung beeinträchtigt, ist auch in der Kategorie 2 angesiedelt, da – wie zuvor beschrieben – das Auszählen von Achsen und die Freimeldung eines besetzten Abschnittes auf Ebene des einzelnen Achszählers nicht zu einer weitergehenden Gefährdung führt und die inkorrekte Achszählung aufgedeckt wird.

4.3 Analyseergebnisse

Die Beurteilung der Risiken erfolgt aus den Kategorien für das zu erwartende Schadensausmaß und den Häufigkeitslevel, wie in Tabelle 2 dargestellt. Diese Risikomatrix ist als *provisorischer Entwurf* zu verstehen, da es diesbezüglich in der Eisenbahnsignaltechnik noch keine einheitlichen Vorgaben für IT-Security gibt und die fundierte Ableitung einer solchen Matrix weit über den Rahmen dieses Beitrags hinausgeht. Eine Validierung außerhalb der Fallstudie steht noch aus.

In der üblichen Interpretation gilt das Risiko für die grünen Felder als akzeptabel, für die roten als inakzeptabel und für die gelben ist es eine Ermessenentscheidung im Einzelfall. Da die Schadensausmaße 1 und 2 nicht in einen unsicheren Zustand führen, wurde entschieden, dass das Risiko auch für höhere Häufigkeitslevel noch im gelben Bereich ist oder akzeptiert werden kann. Die Bewertungen aller vier Unwanted Incidents liegen hier im grünen Bereich (Schadensausmaß 2 und Häufigkeit 2 bzw. 3, siehe Abbildung 4)

		Schadensausmaß				
		0	**1**	**2**	**3**	**4**
Häufigkeitslevel	**0**					
	1					
	2					
	3					
	4					
	5					

Tabelle 2: Entwurf einer Risikomatrix zur Fallstudie Achszählsystem

Das interessanteste Ergebnis ist die Bewertung des unerwünschten Ereignisses „Beliebige Ein-/Auszählvorgänge ohne Zugwirkung möglich“: Der Wert 2 für die Häufigkeit *und* das Schadensausmaß spiegelt wider, dass trotz des hohen Aufwands für einen Zählpunktimitator kein größerer Schaden erreicht werden kann. Dieser Teil der Analyse rechtfertigt, dass auf weitere Schutzmaßnahmen wie die Verschlüsselung von Signalen verzichtet werden kann.

5 Diskussion

Zur Berechnung des Risikos für die Schutzziele müssen, wie in Abschnitt 3.2 beschrieben, neben dem zu erwartenden Schadensausmaß auch die Auftrittshäufigkeiten der möglichen Bedrohungen bestimmt werden. Mit quantitativen Wahrscheinlichkeiten bzw. Frequenzen sind seltene Ereignisse (nicht nur in der Eisenbahnsignaltechnik) schwer abzuschätzen. Leichte Variationen der Randbedingungen oder alternative Interpretationen können schnell zu Abweichungen von mehreren Zehnerpotenzen führen, welche sich durch die Multiplikation von Einzelwerten noch verstärken. Obwohl die Plausibilität des Gesamtergebnisses kaum überprüft werden kann, entsteht ein trügerisches Gefühl „exakter“ Berechnungen.

In Verbindung mit CORAS haben wir uns mit den auf Einflussfaktoren basierenden Häufigkeitsleveln für einen qualitativen Ansatz entschieden, der sich mit seiner groben Stufeneinteilung an den Grad der Genauigkeit und Verfügbarkeit von Referenzdaten anpasst. Dabei haben wir uns auf drei Hauptfaktoren (Motivation, Werkzeuge/Mittel, Zugang/Gelegenheit) konzentriert, wie sie z.B. auch von der *OCTAVE*-Methode für IT-Security-Risikomanagement verwendet werden (siehe [AD02] Kap. 9.5) Andere Ansätze, z.B. für die Netzwerksicherheit, verwenden spezialisierte Faktoren wie die Reproduzierbarkeit oder Detektierbarkeit von Angriffen auf bekannte Schwachstellen. Unsere Methode kann bei Bedarf um neue Einflussfaktoren und eine neue Gewichtungsfunktion erweitert werden.

Nach einer Normalisierung können positiv-antreibende Faktoren (Motivation $(+)$) und negativ-hindernde Faktoren (benötigte Werkzeuge $(-)$, Zugang $(-)$) zu einem Häufigkeitslevel verrechnet werden. Das heißt, dass während des Bewertungsprozesses die verwendeten Parameter jeweils von hohen Stufen (sehr große Vorteile, sehr geringe Nachteile) iterativ nach unten (sehr geringe Vorteile, sehr große Nachteile) angepasst werden. Eine umfangreiche Abwägung wird auch in [BS12] verwendet, wo der Nutzen (aus Sicht des Angreifers) aus den Erwartungen bzgl. Gewinn $(+)$, Aufwand $(-)$, eigenem Risiko $(-)$ und weiteren Faktoren bestimmt wird. Im Rahmen der Fallstudie hat sich gezeigt, dass der auf Einflussfaktoren basierende Ansatz die Bewertung deutlich transparenter macht, und die Auswahl und Priorisierung von Schutzmaßnahmen erleichtert.

In der praktischen Anwendung überwältigt CORAS zunächst mit seiner Vielzahl an Diagrammtypen (Asset-, Risk-, Treatment-Diagramme usw.), wovon hier nur das wichtige Threat-Diagramm verwendet wurde. Bei den anderen Diagrammtypen handelt es sich im Wesentlichen um alternative *Sichten* mit gemeinsamer Symbolik. Mit der graphischen Modellierung lassen sich Abhängigkeiten zwischen Bedrohungen, Szenarien und Assets gut visualisieren. Ab einer gewissen Systemgröße wird jedoch eine Aufteilung auf mehrere Diagramme notwendig, z. B. getrennt nach Schutzzielen. CORAS besitzt bereits eine Semantik zur hierarchischen Dekomposition von Szenarien. Eine echte Modularisierung der Analyse steht aber noch aus.

6 Zusammenfassung und Fazit

In diesem Beitrag haben wir die Anwendbarkeit der graphischen CORAS-Methode zur IT-Security-Risikoanalyse auf Systeme der Eisenbahnsignaltechnik demonstriert und durch ein alternatives Verfahren zur Abschätzung von Häufigkeiten ergänzt. In einem iterativen Prozess werden Häufigkeitslevel auf Basis von qualitativ abgeschätzten Einflussfaktoren bestimmt, wodurch die Nachvollziehbarkeit der Gesamtergebnisse verbessert wird. Für den Praxiseinsatz ist eine spezifische Kalibrierung der Parameter und ihrer Bewertung sowie eine weitergehende Integration mit existierenden Methoden und Standards notwendig.

Literatur

[AD02] Christopher Alberts und Audrey Dorofee. *Managing Information Security Risks: The OCTAVE Approach*. Addison-Wesley, 2002.

[BS12] Jens Braband und Markus Seemann. On the relationship of hazards and threats in railway signaling. In *Proceedings of The 7th IET System Safety Conference incorporating the Cyber Security Conference, Edinburgh, UK, 15.-18. October 2012*, 2012. (to be published).

[CEN03] CENELEC. EN 50129: Railway applications, Communication, signaling and processing systems – Safety-related electronic systems for signaling, 2003.

[CEN10] CENELEC. EN 50129: Railway applications, Communication, signaling and processing systems – Safety-related communication in transmission systems, 2010.

[Int06] International Electrotechnical Commission. DIN IEC 61508-4: Funktionale Sicherheit elektrischer/elektronischer/programmierbar elektronischer sicherheitsbezogener Systeme, 2006.

[Int09] International Organization for Standardization. ISO 31000: Risk management – Principles and guidelines, 2009.

[LSS11] Mass Soldal Lund, Bjørnar Solhaug und Ketil Stølen. *Model-Driven Risk Analysis: The CORAS Approach*. Springer, 2011.

[Saa12] Sebastian Saal. Erweiterung der CORAS-Methode zur strukturierten Ermittlung von IT-Security-Anforderungen an Systeme der Eisenbahnsignaltechnik. (Bachelorarbeit) Technische Universität Braunschweig, Institut für Theoretische Informatik, 2012.

[VDE13] VDE. VDE 0831-102 (draft): Electric signalling systems for railways – Part 102: Protection profile for technical functions in railway signalling, to be issued, 2013.