Software-gestützte Bedrohungsanalyse durch Angriffsgraphen

Markus Heinrich[1], **Lukas Iffländer**[2]

[1] INCYDE GmbH

[2] Deutsches Zentrum für Schienenverkehrsforschung [beim Eisenbahn-Bundesamt]

1 Einleitung

Die IT- und OT-Sicherheit (=Security) erfordert eine ganzheitliche und regelmäßige Risikobewertung. Ein eigenständiges Produkt, das den Schutz vor Cyberangriffen sicherstellt, existiert genauso wenig wie eine einmalig zu integrierende Lösung. Stattdessen muss der Betrachtungsgegenstand (Asset) regelmäßig einer Risikoanalyse unterzogen werden, die die sich ständig verändernde Bedrohungslage berücksichtigt.

Die einschlägigen Methoden gehen im Kern auf die bekannte Gleichung Risiko = Eintrittswahrscheinlichkeit x Schadensausmaß zurück. Während man in der funktionalen Sicherheit (Safety) von Gefährdungen spricht, wird in der IT-/OT-Sicherheit das Risiko einer Bedrohung betrachtet. Insbesondere die Eintrittswahrscheinlichkeit einer Bedrohung kann dabei häufig nicht durch einen Dezimalbruch angegeben werden, sondern wird auf andere, semi-quantitative Art bewertet (bspw. niedrig, mittel, hoch). Der Eintritt eines IT/OT-Sicherheits-Ereignisses (ein Angriff) folgt keinem stochastischen Prozess, der sich durch eine Wahrscheinlichkeit beschreiben lässt. Die TS 50701 bspw. modelliert die Wahrscheinlichkeit (als Likelihood) über die Attribute Exposition und Verwundbarkeit des betrachteten Systems, die in Stufen von 1 bis 3 bewertet werden. Die DIN VDE V 0831-104 folgt dem Ansatz der IEC 62443 und fordert die Bewertung jeder Bedrohung durch das Wissen, die Ressourcen und die Motivation des Angreifers, was als indirekte semi-quantitative Modellierung der Eintrittswahrscheinlichkeit interpretiert werden kann.

Allen Risikoanalysemethoden ist gemein, dass sie eine Vielzahl von Bedrohungen auf das Asset berücksichtigen müssen, aus der eine umfangreiche Dokumentation resultiert, um die Einschätzung des Risikos aus jeder Bedrohung nachvollziehbar zu machen. Darüber hinaus kann ein hundertprozentiger Schutz vor Angriffen nicht existieren, weil sich die Bedrohungslage stetig ändert und Gegenmaßnahmen aus beschränkten finanziellen und personellen Ressourcen geschöpft werden müssen. Daher ist die Aufgabe der Risikoanalyse und ihrer Dokumentation zu bestimmen, welche Risiken zu mitigieren und welche Risiken zu akzeptieren sind. Damit liefert die Risikoanalyse eine priorisierte Liste von Maßnahmen zur Risikominderung. Gleichzeitig müssen bereits existierende Gegenmaßnahmen abgebildet werden, um eine valide Einschätzung des Risikos zu erhalten.

2 Angriffsgraphen

Zur Unterstützung der Risikoanalyse wird im Forschungsprojekt „Prognose Securitybedarf und Bewertung möglicher Sicherheitskonzepte für das System Bahn“ [1] die Methodik der Angriffsgraphen

[1] Korrespondierender Autor: markus.heinrich@incyde.com

entwickelt und mit Hilfe eines Software-Werkzeuges abgebildet, das die Analyse automatisiert. Durch das Tool werden der Arbeitsaufwand und die Fehleranfälligkeit des Prozesses reduziert sowie die Nachvollziehbarkeit und Aussagekraft erhöht. Eine Analyse bisher existierender Software-Werkzeuge hat gezeigt, dass es keine Software gibt, die die Anforderungen der Angriffsgraphen komplett abbildet. Es wurden sowohl Software aus der IT-Sicherheits-Forschung als auch kommerziell oder frei verfügbare Produkte betrachtet. Daher wurde entschieden, eine Software gemäß den Anforderungen zu entwickeln und quelloffen zur Verfügung zu stellen.

Die Angriffsgraphen basieren auf den Angriffsbäumen (Attack Trees). Attack Trees sind eine Methode, die in der Informationssicherheit verwendet wird, um Bedrohungen zu analysieren und Bedingungen darzustellen, die gelten müssen, um aus einer Bedrohung einen erfolgreichen Angriff durchzuführen. Es hat sich jedoch gezeigt, dass es von Vorteil ist, auf einige Eigenschaften von Bäumen aus der Graphentheorie zu verzichten. Zum einen erfordern Angriffsgraphen nicht, dass alle Knoten zusammenhängend sind, sodass voneinander unabhängige Angriffspfade auf ein Asset modelliert werden können. Zum anderen erlaubt der Verzicht auf die Anforderung, dass zwischen zwei Knoten nur genau ein Pfad existieren darf, die Wiederverwendung von Teilschritten eines Angriffes und ihrer Bewertung, die in unterschiedlicher Verkettung auch zu unterschiedlichen Konsequenzen führen können.

Ein Angriffsgraph analysiert genau einen Betrachtungsgegenstand (Asset) auf hinreichend spezifischem Abstraktionsniveau. Ein durch einen Angriffsgraphen analysierter Betrachtungsgegenstand könnte z.B. die intelligente Instandhaltung einer Weiche sein. Bei der intelligenten Instandhaltung (Predictive Maintenance) wird durch Überwachung der Betriebsparameter und maschinelles Lernen vorhergesagt wann mit einem Versagen zu rechnen ist, um rechtzeitig vorher eine Instandhaltung durchzuführen. Die exakte Definition des Assets ist nicht Teil der Angriffsgraphen-Methodik. Das Asset wird im Graphen durch ein Trapez dargestellt (siehe Abbildung 1).

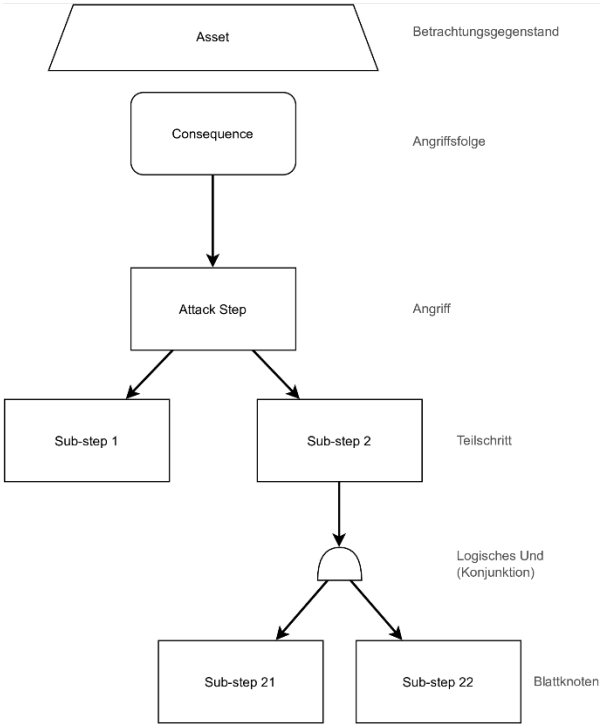

Abb. 1 Beispiel eines Angriffsgraphen für ein Asset

Durch Angriffe auf das Asset entstehen unterschiedliche Angriffsfolgen („Consequence“) oder Schadensereignisse, die im Graphen durch Rechtecke mit abgerundeten Ecken dargestellt werden. Zur Bestimmung der Folgen kommen durch Unternehmen vordefinierte Kataloge von schädlichen Ereignissen, wie z.B. Personenschaden, Reputationsschaden, finanzieller Schaden oder Einschränkung des operativen Geschäfts, in Frage. Genauso erlaubt die Methodik auch die Definition von Folgen durch die Analystin oder den Analysten, falls kein Katalog angewendet werden soll oder eine Erweiterung eines angewendeten Kataloges erfolgen soll.

3 Bedrohungskataloge und Threat Mining

Jede Angriffsfolge kann durch einen oder mehrere Angriffe ausgelöst werden („Attack Step“ in Abbildung 1). Diese Beziehung wird im Graphen durch eine gerichtete Kante von der Folge zum Angriffsschritt dargestellt. Durch diese Verknüpfung erhöhen die Angriffsgraphen die Nachvollziehbarkeit der Risikoanalyse, da sie die mögliche n:m-Beziehung zwischen Angriff und Schaden graphisch darstellen können.

Zur Identifikation der Angriffe können existierende Bedrohungskataloge (bspw. die Elementaren Gefährdungen des BSI [2]) und Methoden des Threat Modellings (bspw. STRIDE [3]) herangezogen werden. Das sog. Threat Modelling ist ein Prozess, um strukturiert IT-Sicherheit gezogene Schwachstellen auf ein System zu identifizieren und so seine Angriffsfläche zu bestimmen. Als Angriff ist hier die Realisierung oder Ausführung einer Bedrohung zu verstehen. Im Beispiel der intelligenten Instandhaltung ist ein Angriff die Manipulation der Vorhersage durch den Angreifer und daraus resultierendes Materialversagen ohne rechtzeitige Vorhersage. Die Folge des Angriffes könnte finanzieller Schaden durch Entgleisen eines Zuges wegen der defekten Weiche sein. Die Verwendung von Katalogen und Threat Mining stellt die hinreichende Vollständigkeit der Bedrohungsanalyse sicher. Angriffsgraphen unterstützen die Analyse durch die grafische Aufbereitung und die Zerlegung der Angriffe in Teilschritte (Sub-step 1 und Sub-step 2) zur Verfeinerung der Analyse und der folgenden

Risikobewertung. Teilschritte setzen sich immer durch logische Disjunktion („oder“) und Konjunktion („und“) zusammen, sodass Fallunterscheidungen in den Angriffsschritten modelliert werden können. Die Methodik erlaubt die Verschachtelung der logischen Verknüpfung und ist prinzipiell auf weitere logische Verknüpfungen erweiterbar.

Eine Aufteilung eines Schrittes in Teilschritte wird durch eine gerichtete Kante zwischen den Knoten dargestellt. Für die Darstellung der Disjunktion und Konjunktion werden entsprechende Knoten zwischen zwei Angriffsschritten erstellt (siehe Abbildung 1). Eine direkte Verbindung zwischen zwei Angriffsschritten stellt implizit eine Disjunktion dar. Die Zerlegung der Angriffsschritte wird iterativ fortgesetzt, bis Teilschritte vorliegen, die hinreichend präzise durch die Attribute zur Bewertung der Eintrittswahrscheinlichkeit (bspw. Ressourcen, Wissen, Motivation nach IEC 62443) beschrieben werden können.

4 Risikobewertung

Die Blattknoten der Angriffsgraphen werden in der Analyse durch einen zuvor gewählten Vektor von Attributen bewertet, um die Eintrittswahrscheinlichkeit zu modellieren. Die Attribute können grundsätzlich frei gewählt werden, um sie der gängigen Praxis der betrachteten Domäne, existierenden Standards und der Risikoaffinität der analysierenden Organisation anpassen zu können. Die DIN VDE V 0831-104 verwendet die aus der IEC 62443 bekannten Attribute „Ressourcen“ sowie „Wissen“ und ersetzt die Motivation durch drei bahnspezifische Risikofaktoren, von denen wir den „Ort“ als Beispiel aufnehmen. So ergibt sich der Attributvektor (Ressourcen, Wissen, Ort), der im Beispiel verwendet wird. Die Attribute werden im Software-Werkzeug über einen Dialog für den Angriffsgraphen festgelegt oder aus einer Vorlage übernommen. Die Einschätzung der Belegung der Attribute erfolgt typischerweise in Workshops mit Expertinnen und Experten und wird in den Angriffsgraphen in die Blattknoten eingetragen und mit Hilfe von Icons visualisiert (siehe Abbildung 2 und Legende in Abbildung 3).

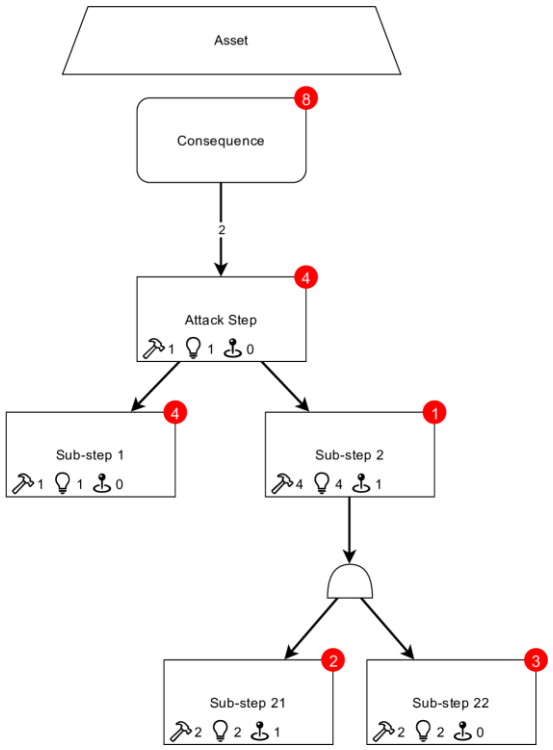

Abb. 2 Angriffsgraph mit erfolgter Bewertung und Aggregation

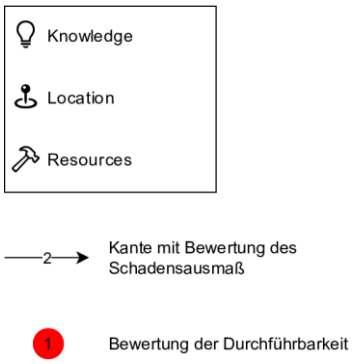

Abb. 3 Legende zum Angriffsgraph

Der Mehrwert der Angriffsgraphen entsteht durch die atomaren Blattknoten, für die sich die Einschätzung der Attribute leichter vornehmen lässt als für komplexere, zusammengesetzte Angriffe. Daraus folgt allerdings die Notwendigkeit, die Bewertung der Blattknoten entlang des Pfades zur Angriffsfolge zu aggregieren, um die Teilschritte wieder zu einer Gesamtbewertung zusammenzusetzen. Das Software-Werkzeug für die Angriffsgraphen unterstützt die Analystin durch vorbereitete und automatisierte Verknüpfung der Teilschritte gemäß der in der Zerlegung definierten logischen Verknüpfungen. Der vorgeschlagenen Disjunktion liegt die Annahme zugrunde, dass sich der Angreifer von mehreren möglichen Teilschritten zur Umsetzung eines Angriffsschrittes für den am leichtesten durchführbaren entscheidet. Eine mathematische Ordnungsrelation über die Attributvektoren erlaubt den Vergleich der Durchführbarkeit der Teilschritte und die Bestimmung der höchsten Durchführbarkeit. In Abbildung 2 ist zu erkennen, dass die Bewertung von „Sub-step 1“ in „Attack Step“ übernommen wird, da er die höhere Durchführbarkeit im Vergleich zu „Sub-step 2“ aufweist.

Aus der Konjunktion mehrerer Teilschritte folgt die erschwerte (geringere) Durchführbarkeit des zusammengesetzten Schrittes. Die für einen erfolgreichen Angriff benötigten Ressourcen sowie das

benötigte Wissen steigen (ähnlich der arithmetischen Addition), wie in Abbildung 2 zu sehen ist. Zur Illustration werden hier über den zwischengeschalteten Und-Knoten die Attribute der Kindknoten „Sub-step 21“ und „Sub-step 22“ addiert.

Das Software-Werkzeug unterscheidet zwischen Aggregationsfunktionen und Funktionen zur Berechnung eines abgeleiteten Attributes. Aggregationsfunktionen dienen zur logischen Verknüpfung der Attributvektoren der Kindknoten zu einem Attributvektor des betrachteten Knotens. Ein abgeleitetes Attribut, wie die Durchführbarkeit, ist ein aus dem lokalen Attributvektor abgeleiteter Skalar (roter Kreis oben rechts im Knoten). Eine mitgelieferte Vorlage für die Angriffsgraphen beinhaltet bereits Vorschläge für die Umsetzung sowohl der Aggregationsfunktionen als auch der abgeleiteten Attribute. Sie sind in der Programmiersprache JavaScript implementiert und können durch die Benutzerin über einen Dialog betrachtet und modifiziert werden. Zur Abbildung eigener Risikoanalysemethoden erlaubt das Werkzeug die Definition eigener Funktionen über die vorgegebenen hinaus. Nach der Hinterlegung global pro Angriffsgraph lassen sich neu definierte Funktionen sowie bestehende für jeden Knoten individuell auswählen. Über eine Namenskonvention werden Knoten zur Dis- und Konjunktion automatisch mit den Funktionen „OR“ bzw. „AND“ belegt.

Über die Funktionen werden die Attributvektoren automatisch bis zum Angriffsschritt („Attack Step“ in Abbildung 2) vor den Knoten mit den Angriffsfolgen aggregiert (gegen die Richtung der Kanten). Beim Übergang von Angriffsschritt auf Angriffsfolge wird das Ausmaß eines Angriffes oder dessen Einfluss auf eine bestimmte Folge durch Expertinnen und Experten bewertet. Die Bewertung wird als Skalar, als Kantengewicht der Kante zwischen den beiden Knoten dargestellt, sodass die n:m-Beziehung zwischen Angriff und Schaden mit unterschiedlicher Stärke bewertet werden kann. Eine Aggregationsfunktion im Angriffsfolgeknoten nimmt pro Kindsknoten den Attributvektor sowie das Kantengewicht entgegen, verknüpft diese zum Betrag des Risikos und kann somit den Angriff mit dem höchsten Risiko für das im Knoten beschriebene Schadensereignis bestimmen. In Abbildung 2 wird dies beispielhaft mit nur einem Angriffsschritt dargestellt: Risiko = Durchführbarkeit * Schadensausmaß = 4 x 2 = 8.

Die in den Abbildungen gezeigten Werte dienen der Illustration und spiegeln keine konkrete Risikobewertung wider. Die genaue Definition und Feinjustierung der Aggregationsmethodik wird im weiteren Verlauf des Forschungsprojektes vorgenommen.

5 Gegenmaßnahmen

Die Risikoanalyse und Bewertung der Bedrohungen werden zunächst ohne Berücksichtigung der Gegenmaßnahmen durchgeführt. Grundsätzlich sollen im iterativen Prozess der Risikoanalyse jedoch bereits etablierte Gegenmaßnahmen berücksichtigt, bewertet und dargestellt werden. Die Angriffsgraphen und das Software-Werkzeug erleichtern daher auch die Erfassung der Wirkung von Gegenmaßnahmen auf Angriffsschritte. Auch hier ist eine n:m-Beziehung zwischen Angriff und Maßnahme anzunehmen, da typischerweise je nach Fallkonstellation eine einzelne Maßnahme gegen mehrere Angriffe schützen kann und umgekehrt mehrere Maßnahmen zum Schutz vor einem Angriff zur Auswahl stehen können oder erst die Kombination mehrerer Maßnahmen einen wirksamen Schutz darstellt.

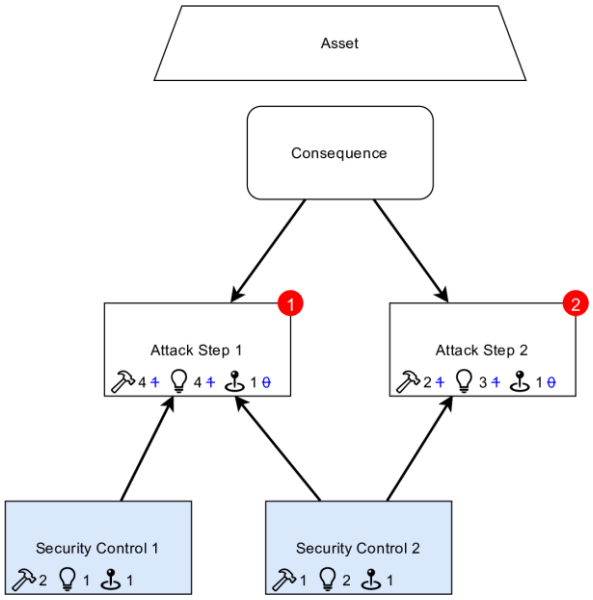

Abb. 4 Angriffsgraph stellt die Wirkung der Gegenmaßnahmen dar.

Das Beispiel in Abbildung 4 zeigt die Wirkung von zwei Gegenmaßnahmen auf zwei Angriffsschritte. Auch die Gegenmaßnahmen werden mit demselben Attributvektor bewertet und nehmen so Einfluss auf den Angriff. Die ursprüngliche Bewertung des Angriffsschrittes wird mit blauer Schriftfarbe und durchgestrichen im Knoten weiterhin dargestellt, während die schwarz gedruckten Werte auch den Einfluss der Gegenmaßnahmen enthalten und so das durch die Maßnahme reduzierte Risiko widerspiegeln. Auf „Attack Step 1“ wirken beide Gegenmaßnahmen mit im Beispiel addiertem Effekt. Auf „Attack Step 2“ hingegen wirkt nur „Security Control 2“, sodass hier bei gleicher Ausgangsbewertung, wie „Attack Step 1“ eine geringere Reduktion der Durchführbarkeit erfolgt.

6 Fazit und Ausblick

Mit dem Software-Werkzeug für Angriffsgraphen lassen sich verschiedene Risikoanalysemethoden abbilden, automatisieren und auf die Bedürfnisse und die Risikoaffinität der analysierenden Organisation abstimmen. Die Angriffsgraphen ermöglichen die explizite Zuordnung von Bedrohungen zu daraus folgenden Schäden inklusive einer Bewertung der Schadenshöhe. Durch die Verfeinerung der Bedrohungen in Angriffsschritte werden die semi-quantitative Bewertung der Eintrittswahrscheinlichkeit sowie der risikomindernde Einfluss von Gegenmaßnahmen mit denselben Attributen, wie ein Angriffsschritt, transparent und nachvollziehbar. Durch diesen Schritt wird ein harmonisiertes Risikomanagement im Unternehmen möglich. Die Semi-Quantifizierung unterstützt IT-Sicherheitsverantwortliche dabei, Maßnahmen für Fachpersonale und Management gleichermaßen nachvollziehbar in ihrer Wirkung darzustellen. Dies erhöht Verständnis, Awareness und Sicherheit in der Qualität der Einschätzung.

Das Werkzeug stellt eine JavaScript-Schnittstelle zur automatisierten Aggregation der Attribute im Angriffsgraphen bereit. Die Definition der Funktionen wird im weiteren Verlauf des Projektes „Prognose Securitybedarf und Bewertung möglicher Sicherheitskonzepte für das System Bahn“ vorgenommen und verfeinert. Das Werkzeug wird in diesem Forschungsprojekt dazu verwendet, eine Risikoanalyse der prognostizierten Anwendungsfälle vorzunehmen und Abuse-Cases für sie zu entwickeln und zu bewerten. Das Software-Werkzeug wurde als Plugin für die frei verfügbare Diagramm-Software

Draw.io [4] entwickelt und steht quelloffen unter der MIT Lizenz auf GitHub zum Herunterladen zur Verfügung [5].

7 Forschungsförderung

Die vorgestellte Lösung entstand im Rahmen des vom Deutschen Zentrum für Schienenverkehrsforschung beim Eisenbahn-Bundesamt beauftragten und finanzierten Projekts „Prognose Securitybedarf und Bewertung möglicher Sicherheitskonzepte für das System Bahn“.

8 Literatur

[1] www.dzsf.bund.de/SharedDocs/Standardartikel/DZSF/Projekte/Projekt_49_Securitybedarf.html

[2] https://www.bsi.bund.de/DE/Themen/Unternehmen-und-Organisationen/Standards-und-Zertifizierung/IT-Grundschutz/IT-Grundschutz-Kompendium/Elementare-Gefaehrdungen/elementare-gefaehrdungen_node.html

[3] https://docs.microsoft.com/en-us/previous-versions/commerce-server/ee823878(v=cs.20)

[4] https://www.diagrams.net/

[5] https://github.com/incyde-gmbh/drawio-plugin-attackgraphs

Abb. 6 Eine von DB Netz definierte Signalanordnung wird je nach Detailierungsgrad (LOD) unterschiedlich genau in 3D dargestellt

4 Fazit und Ausblick

BIM ist als Arbeitsmethode und technologischer Rahmen für die künftige Abwicklung von komplexen Infrastrukturprojekten bei der DB und darüber hinaus gesetzt und weitgehend auch gewollt. Derzeit findet der Übergang von den klassischen Prozessen zu den BIM-relevanten Prozessen statt, was naturgemäß nicht reibungs- und problemlos verläuft. Bei allen Beteiligten wird durch Information und Schulung die Transitionsphase so gut wie möglich gestaltet und allmählich ist ein Umdenken und ein grundlegendes Verständnis für BIM in der Fläche und auf allen Unternehmensebenen erkennbar. Auch wenn aktuelle Projekte die neuen Verfahren und Organisationsstrukturen bereits in Form der BIM-Dokumente AIA und BAP vorgeben und einüben, so sind viele technische, vertragliche und rechtliche Details noch unklar. Das gilt sowohl speziell in den einzelnen Gewerken als auch in den gewerkeübergreifenden Prozessen und insbesondere in der Verwendung des 3D-Koordinationsmodells. Hier ist zu erwarten, dass die DB Netz die nötigen Vorgaben in einer Vielzahl von Richtlinien und technischen Mitteilungen definieren und entsprechend einfordern werden, so wie sie es im Kontext der PlanPro-Datenschnittstelle bereits getan hat.

Allerdings ist bei der Verwendung des 3D-Koordinationsmodells das Ende der Möglichkeiten bzw. der Anwendungsfälle noch nicht einmal in Sicht. Man kann zwar vermuten, dass mindestens alle realen Anwendungsfälle einer Baustelle auch ihr Pendant im Digitalen Zwilling finden, aber das virtuelle Modell macht auch Darstellungen und Aktivitäten möglich, die in der realen Welt nicht gehen. Hier sei als Beispiel das virtuelle Darstellen von Zufahrtsstraßen genannt, anhand derer man sich die Situationen in den verschiedenen Bauphasen vorlegt und etwaige Fahrstraßenausschlüsse erkennt und diskutiert.

Generell erscheinen aus den bisherigen BIM-Erfahrungen die folgenden Aspekte wichtig und erfolgsrelevant:

- Letztlich produziert der Mensch immer den Mehrwert, die Maschinen können nur unterstützen.
- Mit einer flexiblen und transparenten Kollaboration muss auch eine vertragliche Transparenz und Fairness einhergehen. Das erfordert insbesondere die Überwindung von statischen Honorarmodellen wie z.B. die der HOAI zugunsten von flexibler und leistungsgerechter Entlohnung.
- Infolgedessen erscheint der statische Werksvertrag und die damit einhergehende Bieterbewertung „Der Billigste gewinnt“ deutlich überkommen und wenig zielführend im Kontext BIM.

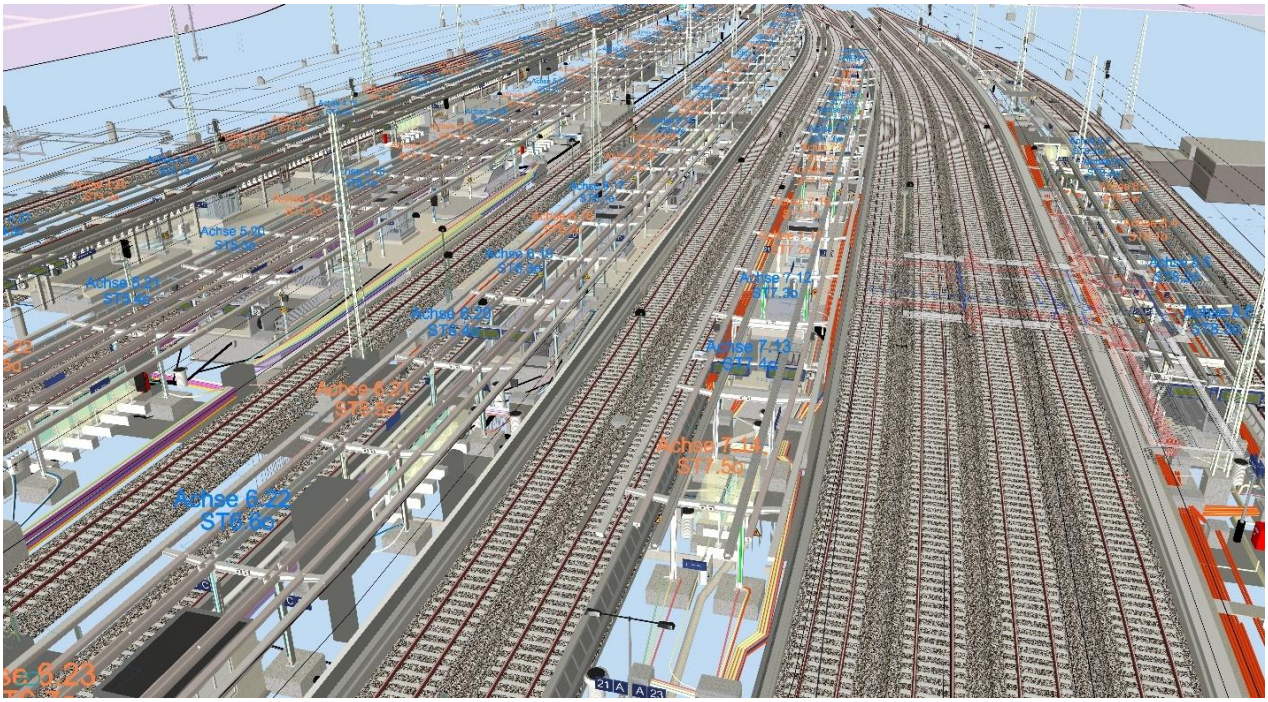

Abb. 7 Gesamtmodell des Hauptbahnhofs Dortmund in der BIM-Software KorFin. [5]

5 Abkürzungen

Tab. 1 Abkürzungen

Abkürzung	Bedeutung
AIA	Auftraggeberinformationsanforderungen
BAP	BIM Abwicklungsplan
BIM	Building Information Modeling
BÜSA	Bahnübergangssicherungsanlage
D3iP	Digitale durchgehende Datenhaltung in der Planung
DB	Deutsche Bahn
DSD	Digitale Schiene Deutschland
DSTW	Digitales Stellwerk
ESTW	Elektronisches Stellwerk
ET	Elektrotechnik
ETCS	European Train Control System
HOAI	Honorarabrechnung für Architekten und Ingenieure
IFC	Industry Foundation Classes
KIB	Konstruktiver Ingenieurbau
KTB	Kabeltiefbau
LOD	Level of Detail
LST	Leit- und Sicherungstechnik
OLA	Oberleitung
PDF	Portable Document Format
TK	Telekommunikation
VST	Verkehrsstationen
XLM	Extensible Markup Language
ZN/ZL	Zugnummern/Zuglenkung

6 Quellenangaben und Literaturverzeichnis

[1] Bildquelle: Uminski, Klaus, EI November 2021, S. 12

[2] Bildquelle: DB Netz Projekt D3iP

[3] Bildquelle: WSP Software ProSig

[4] WSP Software ProSig, DB Netz Projekt D3iP und A+S Software KorFin

[5] Bildquelle: A+S Software KorFin

[6] Bormann, A., König, M., Koch, C., Beetz, J. Hrsg. (2021), Building Information Modeling, Technologische Grundlagen und industrielle Praxis. Verlag: Springer Vieweg.

[7] Bundesregierung Homepage, Bundesverkehrsminister Alexander Dobrindt stellte in Berlin einen Stufenplan zur schrittweisen Einführung dieser digitalen Planungsmethode bei Infrastrukturprojekten und großen Bauvorhaben vor. Available at (accessed 12.04.2022): https://www.bundesregierung.de/breg-de/aktuelles/erst-virtuell-dann-real-bauen-454736

[8] Uminski, V., Klaus, C., Fachartikel im „Der Eisenbahningenieur “(EI November 2021). Digitale LST-Planung im Kontext Digitale Schiene Deutschland und BIM. Available at (accessed 12.04.2022):http://www.prosig.de/fileadmin/user_upload/202111_El_LST_im_Kontext_Digitale_Schiene_und_BIM.pdf