

Sicherheitsnachweisführung und Genehmigung modularer DSTW

Technische Systemintegration in Verantwortung des Betreibers

MARKUS ROTHKEHL | ANDREAS OETTING

Die bei Digitalen Stellwerken (DSTW) zum Einsatz kommende modulare Systemarchitektur bedingt gegenüber monolithischen Lösungsansätzen neue Aufteilungen und Zuständigkeitsabgrenzungen bei der Nachweisführung zur Bestätigung der sicheren Integration. Die DB Netz AG (DB Netz) verantwortet dabei weiterhin den Betrieb. Um sichere Komponenten mehrerer Hersteller in einem DSTW nutzen zu können, übernimmt sie zusätzlich die Rolle des Integrators verschiedener Teil- und Umsysteme des DSTW. Daraus ergibt sich eine Sicherheitsnachweispflicht für neu erstellte DSTW nach den Vorgaben der EN 50126 ff. in Verantwortung der Deutschen Bahn AG (DB). In den folgenden Abschnitten wird der Genehmigungs- und Sicherheitsnachweisführungsprozess für DSTW erläutert.

Einführung

Als Nachfolger des Elektronischen Stellwerks (ESTW) ist das DSTW ein elementarer Bestandteil der Digitalen Schiene Deutschland (DSD) und Teil der Digitaloffensive der DB. Das DSTW ist das Herzstück der Digitalen Leit- und Sicherungstechnik (DLST), die laut der offiziellen Roll-out-Strategie auch darauf abzielt, die Zuverlässigkeit und Wirtschaftlichkeit der Eisenbahninfrastruktur zu verbessern. [1]

In Abb. 1 ist die von der DB spezifizierte DSTW-Systemarchitektur schematisch und auf ihre wesentlichen Inhalte reduziert dargestellt. Dieses zeigt die Möglichkeit der Modularität in der Zukunft. Standardisierte Schnittstellen verbinden die Teilsysteme (rot) und Umsysteme (blau) des DSTW. Die Kommunikation wird über ein von der DB bereitgestelltes Übertragungssystem gesichert, das aus dem bahnbetrieblichen IP-Netzwerk (bbIP), dem Gleisfeld, dazugehörigen Datenetzen und Sicherheitseinrichtungen besteht und standardisierte Schnittstellen und Datenformate nutzt. Der Einsatz des DB-Übertragungssystems führt zu einer Erweiterung der Sicherheitsnachweisführung, da die einzelnen Hersteller von LST-Komponenten Sicherheitsbewertungen ihrer Systeme nur im eigenen Verantwortungsbereich durchführen können. Daher verfolgt die hier vorgestellte Systemintegration den Ansatz, dass die Hersteller ihre Teilsysteme weiterhin unabhängig voneinander nach

bewährten Methoden qualifizieren. Darüber hinaus ergänzt die DB als Integrator des DSTW-Systems entsprechende Integrations-, Sicherheits- und Änderungsnachweise, um zukünftige Änderungen im modularen System beherrschen zu können. Die neuen Aktivitäten für die DB werden unter dem Begriff der Systemqualifizierung zusammengefasst.

Methode

Ziel der Systemqualifizierung ist die Beschreibung des Verfahrens zur Erstellung des Sicherheitsnachweises nach EN 50129 [5] und der Konzeptionierung erforderlicher Legitimations- und Genehmigungsprozesse über mehrere Verantwortungsgrenzen hinweg. Eine Anforderung der DB für diese Lösung ist, dass Aktivitäten und Prozesse für alle Beteiligten der Branche möglichst transparent dargestellt werden und die zu definierenden Verfahren die Bauartbetreuung des Betreibers durch

technische und formale Beherrschung des Systems unterstützen. Die EN 50129 fordert für jedes im Bahnbetrieb eingesetzte sicherheitskritische Produkt einen Sicherheitsnachweis und alle damit verbundenen Integrations- und Verifizierungsmaßnahmen [5].

Gemäß EN 50129 setzt sich die Sicherheitsnachweisführung aus dem generischen Anwendungssicherheitsnachweis (GASC) und dem anwendungsspezifischen Sicherheitsnachweis (SASC) zusammen [5]. Da der Betreiber auch frühere Stellwerkstypen bereits in sein Bahnsystem integriert hat, wird davon ausgegangen, dass sich der Umfang des SASC nicht wesentlich bei modularen DSTW unterscheidet. Für die Anwendung des SASC kann daher auf die bestehenden Verfahren zurückgegriffen werden.

Betrachtungsrahmen in diesem Beitrag soll die generische Sicherheitsnachweisstruktur sein, da die entscheidende Neuerung des DSTW

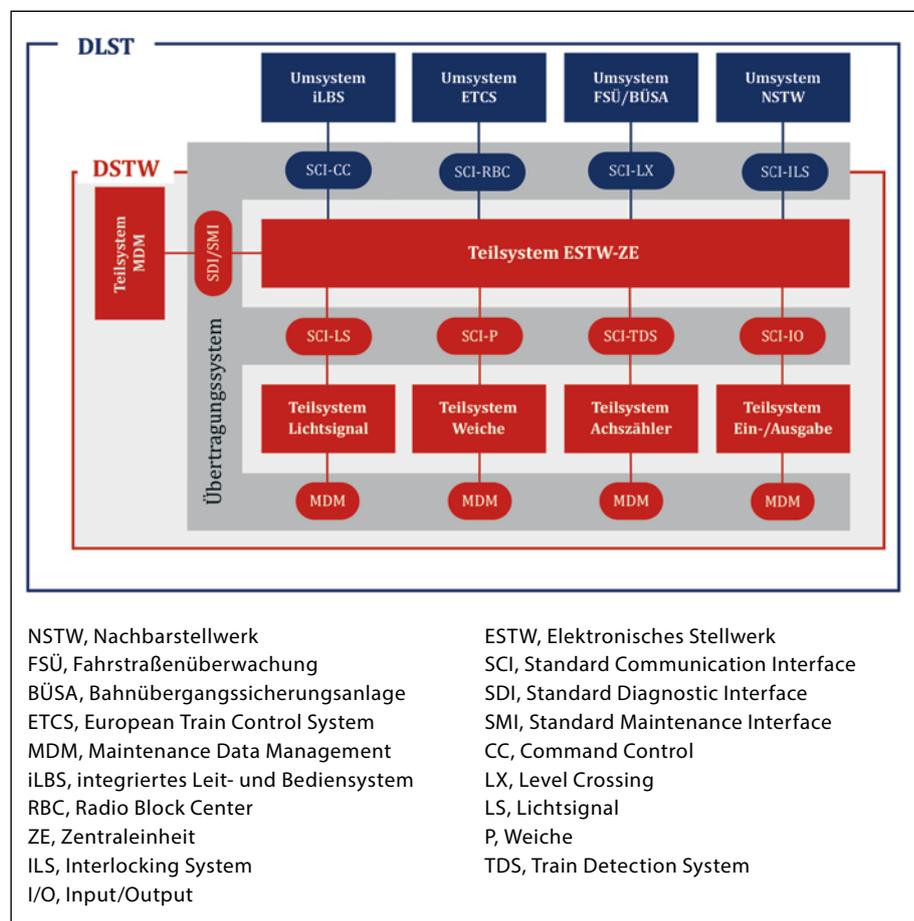


Abb. 1: Schematische Systemarchitektur DSTW



Abb. 2: Struktur des Systemqualifizierungsnachweises
 Quelle: angelehnt an Sicherheitsnachweis gemäß EN 50129

in der Integrationsverantwortung identifiziert wurde, die zwischen der Verantwortung der Hersteller für die Teilsysteme und der des Betreibers des bereits integrierten DSTW liegt. Die Anforderungen an den Sicherheitsnachweis sind in der Norm entsprechend der Einteilung der Sicherheitsintegritätslevel (Safety Integrity Level, SIL) detailliert beschrieben, sodass bekannte Vorgehensweisen auf das modulare DSTW-System adaptiert werden können. Die Erfahrung von Fachexperten wird genutzt, um mögliche Optimierungen oder Anpassungen des DSTW-Verfahrens zu evaluieren. Für die Anwendung auf modulare DSTW werden diese Verfahren anhand einer qualitativen Inhalts- und Dokumentenanalyse identifiziert, angepasst und erweitert, um die Verantwortungstrennung zwischen Betreiber, Integrator und Herstellern zu ermitteln.

Vorbedingungen

Qualifizierung von Teilsystemen des DSTW

Auf Systemebene verfügt das DSTW über keine eigene Hard- oder Software [7]. Hard- und Software und deren Funktionen ergeben sich aus der Summe von Teilsystemen [7]. Der Sicherheitsnachweis der Subsysteme wird vom jeweiligen Hersteller erbracht (Prüfbescheinigung, PB) und bereits legitimiert (Genehmigung zum Inverkehrbringen und Verwenden, GluV), sodass das DSTW von dieser Vorlegitimierung besonders profitieren kann.

Der Sicherheitsnachweis der DSTW trägt den Namen Systemqualifizierungsnachweis (SQN) für die in Kapitel 1 beschriebene Systemqualifizierung. Dieser von der Norm abweichende Begriff hilft, die Aktivitäten des Herstellers von den Aktivitäten des Integrators DB abzugrenzen, da der Integrationsgrad der Teilsysteme und die Wechselwirkungen der Teilsysteme im

System betrachtet werden. Die Vorgaben für den SQN sind im Systemqualifizierungsplan (SQP) definiert und unterteilen die Verantwortlichkeiten von Herstellern, Integratoren und Systembetreibern. Die Struktur des SQP sowie die Struktur des SQN (Abb. 2) leitet sich aus dem aktuellen Stand der Norm EN 50129 ab. Einzelne Prüfasperte sind im SQP mit Verantwortlichkeiten für die Umsetzung und Verifizierung tabellarisch festgelegt. Abb. 3 zeigt einen Ausschnitt von Kapitel 4.2.5 im SQP. Die Validierung kann auf unterschiedliche Weise erfolgen. Funktionale Testasperte lassen sich am besten in Form von Funktionsnachweisen durch Testmaßnahmen im Labor, Feld oder gezielten Erprobungen bestätigen.

Zum anderen werden analytische Methoden und die notwendigen Berechnungen eingesetzt, um die Systemsicherheit nachzuweisen. Die Nachweisart wird im SQP durch den Eintrag in der entsprechenden Spalte angegeben. Teilsystemnachweise erbringt dabei der Hersteller, und alle Nachweise, die durch die Systemintegration auf Systemebene erbracht werden, erwirkt die DB. Wie von der EN 50129 gefordert, werden alle Teilergebnisse im SQN zusammengefasst bzw. von dort im Sinne eines Systemsicherheitsnachweises referenziert.

Für die einzelnen sicherheitsrelevanten Teilsysteme, die ergänzt um die nicht sicherheitsrelevanten Teilsysteme in Summe das DSTW bilden, wird ein Entwicklungs- und Genehmigungsprozess gemäß EN 50126 ff. und Eisenbahn-Betriebsnahmegenehmigungsverordnung (EIGV) vorausgesetzt, da dadurch die Passfähigkeit der einzelnen Teilsysteme durch normative Prozess- und Nachweisvorgaben in das finale DSTW gegeben ist. Die Sicherheitsnachweisführung eines DSTW-Systems muss zeigen, dass das System die funktionalen und sicherheitstechnischen Anforderungen in der Spezifikation erfüllt, wenn das Teilsystem über seine standardisierten Schnittstellen verwendet wird.

Teilqualifizierung des Übertragungssystems

Besonderes Augenmerk wird auf das systeminhärente Übertragungssystem gelegt, da es bisher keinen Sicherheitsnachweis dafür gibt. Eine Möglichkeit der Integration in die Nachweisführung wäre die Aufnahme entsprechender Nachweise direkt in den Sicherheitsnachweis des DSTW. Dabei würde jedoch außer Acht gelassen, dass die einzelnen Subsysteme des Übertragungssystems im ersten Schritt zum Teilsystem Übertragungssystem integriert werden müssen. Darüber hinaus wird das Übertragungssystem in der Klassifizierung nicht als sicherheitsrelevant angesehen und beschränkt sich auf den Nachweis der Basisintegrität. Die Betrachtungstiefe im SQN müsste für jedes der Subsysteme definiert werden, was einen erheblichen Einfluss auf die Komplexität und deren Abhängigkeiten des Kapitels hätte.

Um die Komplexität zu reduzieren, werden diese Aspekte in einem vorgelagerten Nachweis (in diesem Kontext als Teilqualifizierung definiert) ausgelagert. Ähnlich wie beim SQP für SQN, benötigt das Übertragungssystem einen Teil-Qualifizierungsnachweis (TQN), dessen Anforderungen in einem Teil-Qualifizierungsplan (TQP) entwickelt werden. Ein entsprechender Teil-Qualifizierungsnachweis für das Übertragungssystem (TQN ÜS) könnte abgestuft und aufeinander aufbauend die Integrationsschritte vom Subsystem in das Übertragungssystem sowie vom Übertragungssystem in das DSTW abbilden. Auch würde die Problematik der Behandlung nicht sicherheitsrelevanter Bestandteile im Sicherheitsnachweis des DSTW behoben werden, da ein TQN ÜS die Nachweisführung des sicheren Systems ergänzt. Die Komplexität des SQN bleibt überschaubar, und zukünftige Änderungen können bereits im Vorfeld im jeweiligen TQN berücksichtigt und bewertet werden.

4.2.5 Nachweis der korrekten Funktionalität		Erstellung	Prüfung
Inhalt [EN 50129, Kapitel 7.2, Abschnitt 2.5 und 2.6]	Der Nachweis der korrekten Hard- und Softwarefunktionalität ist nur relevant, wenn für die Systemebene eine eigene Hard- und Software erzeugt wird. Ansonsten erfolgt diese Prüfung beim Hersteller des Teil- oder Umsystems. Da das DSTW-System keine Hard- oder Software besitzt, wird der Fokus auf den Nachweis der korrekten Funktionalität des Gesamtsystems auf Grundlage der Teilsystemfunktionalitäten gelegt. Dies beinhaltet auch Betrachtungen auf Systemebene von abgestuften Funktionseinschränkungen der Teilsysteme.		
Anmerkung	Nachweis durch Teilsystemtests, Integrationstests, Systemtests und Sicherheitserprobung		
Anforderungen	<ul style="list-style-type: none"> Lastenhefte DSTW Systemintegrationsplan Systemvalidierungsplan 	Betreiber	FGV PSV Betreiber
Referenzen	<ul style="list-style-type: none"> Gutachten / Prüfbescheinigungen der Teilsysteme Bestätigungen der technischen Integrierfähigkeit (Teilsysteme) 	Hersteller	PSV Hersteller
	<ul style="list-style-type: none"> Systemintegrationsbericht Sicherheitserprobungsbericht Konformitätsbewertung der Teilsysteme 	Betreiber	PSV Betreiber FGV
Nachweis	<ul style="list-style-type: none"> Systemvalidierungsbericht 	Betreiber	PSV Betreiber

DSTW, Digitales Stellwerk
 FGV, Freigabeverantwortlicher
 PSV, Prüfsachverständiger

Abb. 3: Beispiel aus SQP: Kapitel 4.2.5 – Nachweis der korrekten Funktionalität

Nach Diskussionen und Bewertungen mit Experten wird die Variante der Teilqualifizierung des Übertragungssystems angestrebt und entsprechend in die Sicherheitsnachweisstruktur eingebunden (Abb. 4).

Teilqualifizierung von Umsystemen

Der Fokus dieses Beitrags liegt auf der Nachweisführung von modularen DSTW. Ungeachtet dessen wird das DSTW nach der Qualifizierung in das System Eisenbahn eingebunden, und wird auch mit den Umsystemen (wie z. B. ETCS, iLBS, BÜSA, NSTW) koexistieren und interagieren (Abb. 1). Inwieweit die Annahmen für den Sicherheitsnachweis nach EN 50126 ff. auch für ein etwaiges umgebendes System gelten, sollte in weiteren Forschungsarbeiten überprüft werden. In der Sicherheitsnachweisstruktur des DSTW müssen jedoch die Grundsätze für die Anbindung von Peripheriesystemen definiert werden, um eine zukünftige Integration im Eisenbahnsystem zu gewährleisten.

Eine Möglichkeit besteht darin, die Nachweiskomponente direkt in die Sicherheitsnachweisführung von DSTW zu integrieren. Die momentan vorhandenen Umsysteme wurden nach Mü 8004 entwickelt und zugelassen. Die EN 50126 ff. hat aber im Vergleich zur Mü 8004 einen stärker prozessorientierten Entwicklungsansatz, bei dem der Sicherheitsnachweis und das sicherheitsbezogene Ausfallverhalten im Vordergrund stehen [8]. Eine gemeinsame Nachweisführung ist deshalb nicht empfehlenswert.

Eine weitere Möglichkeit ist daher die separate Nachweisführung an der Trennung zwischen DSTW und Umsystemen. DSTW und ihre jeweiligen Umsysteme können weiterhin ihre eigenen Zulassungsverfahren nutzen und Sicherheitsnachweise unabhängig voneinander erstellen. An der Schnittstelle müssen lediglich relevante Informationen und Nachweise bereitgestellt werden, um die Sicherheit und gegenseitige Integration der beiden Systeme nachweisen zu können.

Da es sich hierbei nicht um einen vollständigen Funktionsnachweis der beiden Systeme, sondern um einen Integrationsnachweis, ähnlich wie beim Übertragungssystem, handelt, hat das partielle Nachweisverfahren auch den Vorteil, den Nachweisaufwand bei der Anbindung von Umsystemen zu reduzieren. Wie beim TQN ÜS kann der entsprechende TQN des jeweiligen Umsystems als Ergebnis der Vorbewertung in den Sicherheitsnachweis des DSTW aufgenommen werden.

Systemqualifizierung des DSTW

Beim Entwurf einer Sicherheitsnachweisstruktur nach EN 50126 ff. [2–6] ist es relevant zu wissen, welche normativen Prozesse und Nachweisverfahren bei der Entwicklung des Teilsystems verwendet werden. Entsprechend den Anforderungen des Herstellers und den Vorgaben während des Entwicklungsprozesses kann eine geeignete Auswahl getroffen werden.

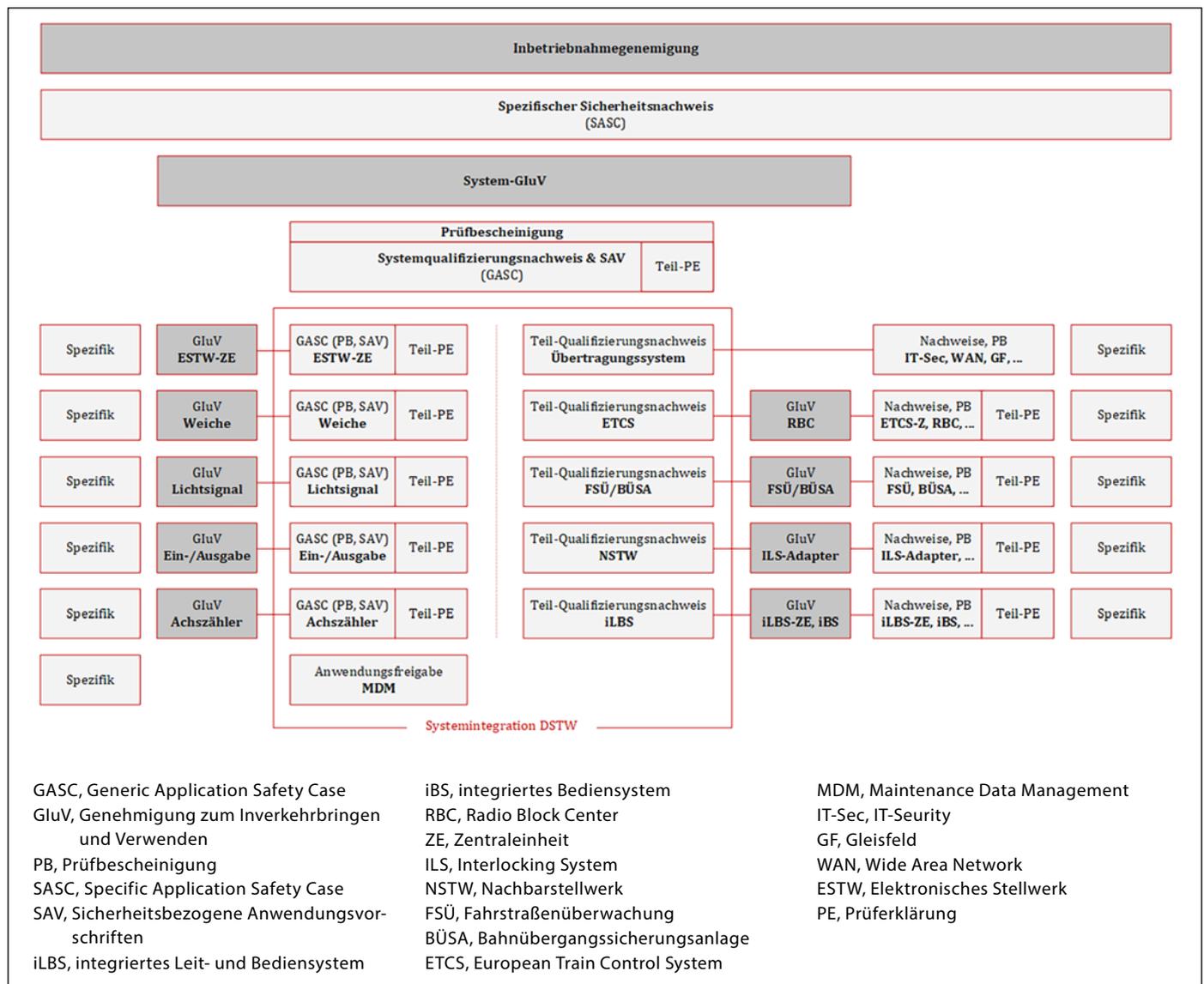


Abb. 4: Sicherheitsnachweisstruktur DSTW

Es wird – unterstützt durch Meinungen von Experten – angenommen, dass die einzelnen sicherheitsrelevanten Teilsysteme, ergänzt um die nicht sicherheitsrelevanten Teilsysteme, einen Entwicklungs- und Genehmigungsprozess gemäß EN 50126 ff. und EIGV umsetzen. Dafür sprechen auch die DSTW-Spezifikationen, die nach EN 50126 ff. erstellt wurden. Die Mü 8004 darf während der Übergangsfrist der EN 50129 nur mit Zustimmung des Eisenbahn-Bundesamtes (EBA) verwendet werden. Darüber hinaus legt die EN 50129 in Kapitel 1 fest, dass Europäische Normen so weit wie möglich für Änderungen und Erweiterungen bestehender Systeme gelten sollen.

Teilsysteme von DSTW werden gemäß der DSTW-Spezifikation neu entwickelt oder zumindest erweitert. Daher wird die Mü 8004 bei der Sicherheitsnachweisführung und Legitimation von DSTW-Systemen nicht mehr berücksichtigt. Die Systemintegration basiert (soweit möglich) auf nach EN 50126 ff. bewerteten Teilsystemen. Da die Zentraleinheit die höchste Komplexität aufweist, formuliert sich hieraus auch der größte Anteil der Nachweisaspekte für die Systemintegration.

Wie in Kapitel 2 beschrieben, hat die DSTW-Systemebene keine separate Hard- und Software. Die vollständige Systemfunktionalität ist in den Teilsystemen enthalten. Die Nachweise des SQN und der einzelnen TQN leiten sich deshalb hauptsächlich aus den Qualifizierungsergebnissen der Teil- und Umsysteme ab, die um integrative Betrachtungen auf Systemebene ergänzt werden. Voraussetzung dafür ist die Umsetzung des Lebenszyklusmodells der EN 50126. Da DSTW und seine Teilsysteme gemäß den Ergebnissen der Risikoanalyse im SIL 4 eingestuft wurden, ist der Hersteller bei seiner Nachweisführung auch verpflichtet, die entsprechenden Anforderungen des SIL 4-Systems einzuhalten. Im zugrundeliegenden Lebenszyklus des Teilsystems erfüllt der Hersteller alle an ihn gestellten Anforderungen.

Im Rahmen der Teilsystemqualifizierung werden die Anforderungen an das Teilsystem verifiziert und bewertet. Kann eine Anforderung auf dieser Ebene nicht bestätigt oder nicht ausreichend erfüllt werden, liegt ein Nachweisdefizit für die Erfüllung der Anforderung vor, und die Anforderung muss auf Systemebene basierend auf den Ergebnissen der Teilsystembewertung weiterbearbeitet werden. Abweichungen von der geforderten Spezifikation und eventuelle Gefährdungen werden von den Herstellern als sicherheitsbezogene Anwendungsvorschriften (SAV) an das übergeordnete DSTW-System weitergegeben. Die Auflösung dieser SAV ist Teil des Integrationsauftrags der DB. Dieses Vorgehen ist auch bei ESTW üblich. Der Unterschied beim DSTW ist jedoch, dass es sich nicht mehr nur um SAV an den Betrieb des Stellwerks handelt, sondern zudem auch SAV an das technische System und der Integration des Systems gerichtet sind. Die DB verantwortet nicht nur den Be-

trieb, sondern auch die technische Systemintegration. Die wesentlichen Systemnachweise für das DSTW werden innerhalb der Systemintegration und -validierung erbracht und funktional in einem System- und Integrationstest in Zusammenschaltung aller Komponenten nachgewiesen.

Das Qualitäts- und Sicherheitsmanagement muss in allen Phasen klar ausgestaltet und im gesamten Entwicklungsprozess dokumentiert werden. Hard- und Softwareänderungen können zu Regressionen führen und sind in der Auswirkungsanalyse in den Release Notes auf Plausibilität zu prüfen.

Genehmigungsverfahren des DSTW

Die entstandene Nachweis- und Integrations-tiefe wurde mit viel Aufwand geschaffen und sollte für Folgeprojekte mit ähnlichen Konstellationen fortgeführt werden können. Um dies zu gewährleisten, ist ein Verfahren erforderlich, das gemeinsame Aspekte überträgt, die von Änderungen nicht betroffen sind. Entsprechend der Vorgaben der EIGV und den Vorgaben aus der Sektorleitlinie besteht im § 27 EIGV die Möglichkeit einer GluV, die im weitesten Sinne einer generischen Zulassung entspricht. Durch die Integration der Teilsysteme mit dem systeminhärenten Übertragungssystem entsteht ein neues System, das auch den Zulassungsanforderungen genügt. Daher können Integratoren von DSTW beim EBA die GluV des gewünschten DSTW-Systems erwirken. Diese GluV ist optional und der obligatorischen (spezifischen) Inbetriebnahmegenehmigung (IBG) vorgelagert (Abb. 4). Der Vorteil im Weglassen einer GluV liegt sicherlich darin, dass einige Nachweise erst später im Projektverlauf benötigt werden. Allerdings müssen dann in Folgeprojekten erneut Nachweise erbracht und in jedem Fall geprüft und bewertet werden. Dies wird den Wiederverwendbarkeitsanforderungen nicht gerecht. Das Weglassen der System-GluV sollte jedoch erwogen werden, wenn das integrierte System nur einmal verwendet werden soll. Hier empfiehlt es sich, die Nachweise direkt in die IBG einzuspeisen. Es wird daher bei einer mehrmaligen Verwendung des modularen DSTW vorgeschlagen, eine GluV zu beantragen.

Um die GluV der Teil- und Umsysteme besser unterscheiden zu können, wird in der diesem Beitrag zugrundeliegenden Arbeit der Begriff System-GluV eingeführt. Zur Verdeutlichung, wie die jeweiligen Nachweise, PB, Gutachten und Genehmigungen ineinandergreifen, wurden diese in Bild 4 in ihren Abhängigkeiten dargestellt. Die erforderlichen Genehmigungen durch das EBA sind dunkelgrau hervorgehoben. Die finale PB für das generische DSTW-System und die folgende System-GluV kann unabhängig vom konkreten Bauvorhaben erlangt werden. Die Trennung der generischen Zulassung des DSTW von der spezifischen IBG des Bauvorhabens schafft die notwendige Standardisierung gleichermaßen für alle Systemkombinationen und bietet die Möglichkeit, den

Geltungsbereich der System-GluV jederzeit zu erweitern. Für den Serien-Roll-out der DSTW ist sie deshalb ein wesentlicher Baustein.

Da das MDM keine Sicherheitsrelevanz hat, wird in Abb. 4 eine Anwenderfreigabe für den Einsatz im System seitens des Betreibers vorausgesetzt. Der Hersteller stellt ersatzweise notwendige Dokumentationen zur Umsetzung der Anforderungen aus der Nachweisführung bereit. Mit Fertigstellung und Begutachtung des SQN wird die korrekte technische Systemintegration der generischen Anwendung bestehend aus den eingesetzten Teilsystemen und Umsystemen bestätigt. Das technische System (DSTW) liegt in der Verantwortung des Integrators und kann bei Bedarf neue oder zusätzliche SAV für den Betrieb benennen. Daher ist, wie bisher auf Teilsystemebene, der Betreiber gemäß Anlage 9 der Sektorleitlinie einzubinden, um das technisch integrierte DSTW einschließlich seiner SAV für den Einsatz im Betrieb zu prüfen. Ein Freigabeverantwortlicher (FGV) erstellt zur Bestätigung der betrieblichen Systemintegration eine Teil-Prüferklärung (Teil-PE), die wiederum in die PB eines Prüfsachverständigen (PSV) eingeht. Der PSV führt die Ergebnisse der Integration von technischen und betrieblichen Systemen zusammen, um die sichere Integration des DSTW-Systems durch Ausstellung einer PB zu bestätigen.

Alternativ kann der PSV die technische und betriebliche Systemintegration gleichermaßen in einem Prüfschritt bewerten. Hier erscheinen jedoch langjährige Erfahrungen mit FGV wünschenswert, da sie auch betriebliche Integrationsaktivitäten auf Teilsystemebene bewerten und Erfahrung im Umgang mit der Integration mit Bahnsystemen haben. Darüber hinaus können Verantwortlichkeiten klar zwischen Technik und Betrieb getrennt werden. Eine Vier-Augen-Prüfung schließt blinde Flecken auch weitestgehend aus. Mit einer PB für das generische DSTW-System und einem Nachweis der sicheren Integration kann die System-GluV gemäß der Verfahren der Sektorleitlinie entsprechend der EIGV beim EBA erwirkt werden. Dies eröffnet die Möglichkeit, vorgelegte Nachweise in Folgeprojekten mit gleicher Konstellation wieder verwenden zu können. Unabhängig davon wird die IBG nach Abschluss der generischen und anwendungsspezifischen Sicherheitsnachweisführung durch das EBA ausgestellt.

Zusammenfassung

Die durch eine qualitative Inhalts- und Dokumentenanalyse analysierten Normen und Vorschriften ergeben eine Grundstruktur für die Genehmigungs- und Sicherheitsnachweisführung modularer DSTW, die durch Expertenwissen um neue Elemente der Systemintegration ergänzt werden kann. Der Nachweis von Umsystemen sollte in Teil-Qualifizierungsnachweisen gebündelt werden. Abb. 4 bietet dem Leser einen Leitfaden zur Einordnung der Nachweisebene und zum Verständnis für den Ablauf der Nachweisführung des DSTW.

Durch die zuvor beschriebenen iterativen Verfahrensschritte zur Systemqualifizierung erhält der Sektor Erweiterungen für die gleichzeitige Integrator- und Betreiberrolle der DB. Darüber hinaus beschreiben SQP und TQP die Prüf- und Nachweisschritte für die sichere Integration des modularen Systems mit dem Übertragungssystem der DB.

Unterdessen entwickeln LST-Hersteller ihre Teilsysteme entsprechend den Anforderungen und der Systemarchitektur weiter. Die Entwicklung ist vor der Systemintegration abzuschließen und durch eine PB eines PSV je Teilsystem zu bestätigen. Abweichungen werden dem Betreiber als SAV übergeben, die dieser sowohl technisch als auch betrieblich in der Systemintegration auflösen muss.

Im SQN des DSTW-Systems, der dem Sicherheitsnachweis nach EN 50129 entspricht, werden die Qualifizierungsergebnisse der Teilsysteme und die TQN der angrenzenden Umsysteme aufgenommen und um den Nachweisaspekt auf Systemebene erweitert. Die System-GluV vervollständigt die Systemqualifizierung und ermöglicht die Mehrfachnutzung des generischen integrierten DSTW-Systems.

Ausblick

Da die Systeme der DSD sehr umfangreich sind, soll im nächsten Schritt das Verfahren der Teilqualifizierung auf Umsysteme, wie z. B. ETCS, Bahnübergänge, Leit- und Bediensystem und Anbindung von Nachbarstellwerken adaptiert werden. Dazu gibt es eine gemeinsame Forschung der DB und der Technischen Universität Darmstadt, um zu ermitteln, wie Umsysteme, die zum Teil aus früheren Normen wie Mü 8004 abgeleitet sind, systemkompatibel in das nach EN 50126 ff. entwickelte DSTW integriert werden können, und wie die Nachweisführung richtig gestaltet werden kann. In zukünftigen Veröffentlichungen werden die vorliegenden Inhalte des Beitrags ergänzt. ■



Markus Rothkehl, M. Sc.

Systemqualifizierungs- und Zulassungsmanager für DSTW
DB Netz AG, Frankfurt am Main
markus.rothkehl@deutschebahn.com

QUELLEN

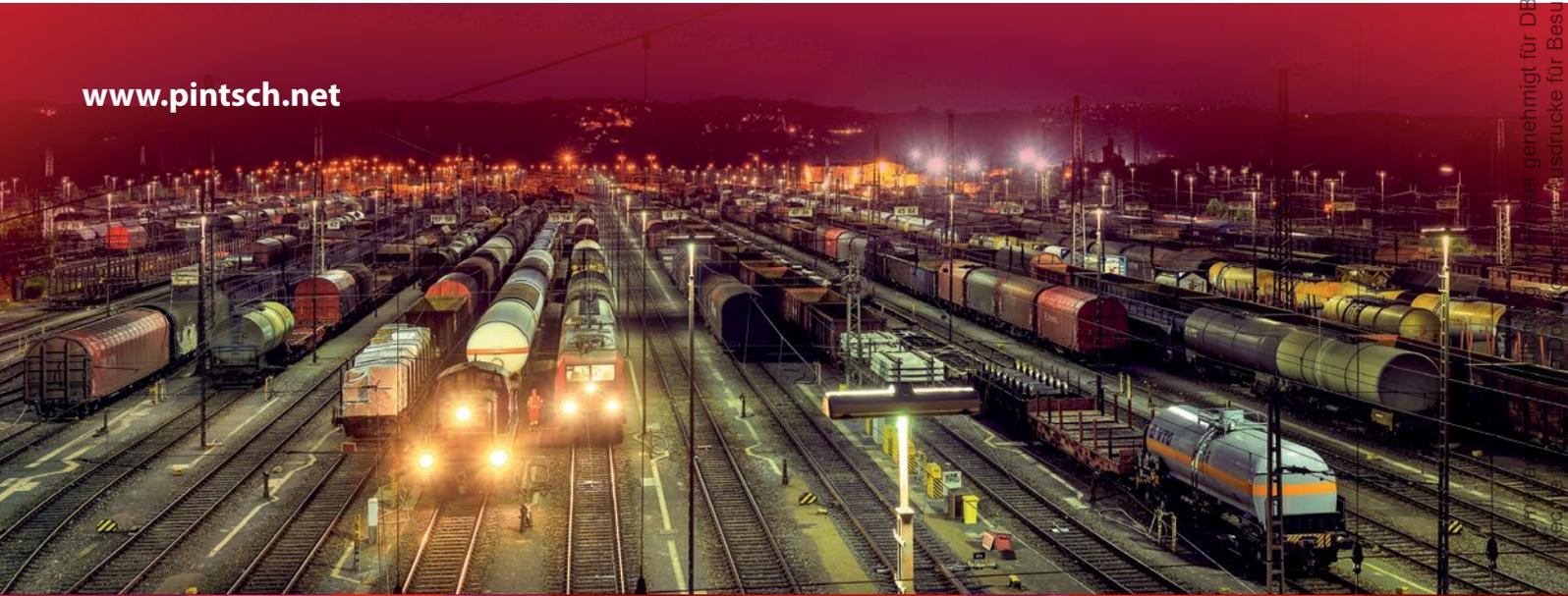
- [1] https://fahrweg.dbnetze.com/fahrweg-de/kunden/nutzungsbedingungen/digitale_1st/allgemein-3084902, 15.06.2021 um 08:41 Uhr
- [2] Norm EN 50126 – Bahnanwendungen: Spezifikation und Nachweis von Zuverlässigkeit, Verfügbarkeit, Instandhaltbarkeit und Sicherheit (RAMS) – Generischer RAMS-Prozess; CENELEC, 01-2017
- [3] Norm EN 50126 – Bahnanwendungen: Spezifikation und Nachweis von Zuverlässigkeit, Verfügbarkeit, Instandhaltbarkeit und Sicherheit (RAMS) – Systembezogene Sicherheitsmethodik; CENELEC, 02-2017
- [4] Norm EN 50128 – Bahnanwendungen: Telekommunikationstechnik, Signaltechnik und Datenverarbeitungssysteme / Software für Eisenbahnsteuerungs- und -überwachungssysteme; CENELEC, 08-2019
- [5] Norm EN 50129 – Bahnanwendungen: Telekommunikationstechnik, Signaltechnik und Datenverarbeitungssysteme / Sicherheitsrelevante elektronische Systeme für Signaltechnik; CENELEC, 06-2019
- [6] Norm EN 50129 – Bahnanwendungen: Telekommunikationstechnik, Signaltechnik und Datenverarbeitungssysteme / Sicherheitsrelevante elektronische Systeme für Signaltechnik; CENELEC, 06-2019
- [7] Wallasch, S. (2017): Systemdefinition ESTW-NeuPro, Frankfurt a. Main. NeuPro.22, Baseline 4.0
- [8] Uhlig, T.; Wenzek, L.: Migration des Zulassungsprozesses von Mü 8004 zu CENELEC am Beispiel des Achszählsystems ACS 2000, SIGNAL+DRAHT



Univ.-Prof. Dr.-Ing. Andreas Oetting

Leitung
Institut für Bahnsysteme u. Bahntechnik
TU Darmstadt, Darmstadt
andreas.oetting@tu-darmstadt.de

www.pintsch.net



Systemlösungen für die Bahninfrastruktur

- | | |
|----------------------------------|-------------|
| ● Bahnübergangstechnik | PINPROTEGIO |
| ● Achszähltechnik | PINCLIRIO |
| ● Stellwerks- und Rangiertechnik | PINMOVIO |
| ● Weichenantrieb | PINMOVIO |
| ● Signale | PINLUXON |
| ● Fördertechnik | PINPOSITON |
| ● Weichenheizungen | PINCALIO |
| ● Diagnose | PINDIAGON |

