

Effizientes Testen modularisierter und standardisierter Stellwerkskomponenten

Efficient testing of modularised and standardised interlocking components

Mirko Caspar | Daniel Schwencke | Hardi Hungar

Modulare, sicherheitsrelevante Systeme verlangen neue Ansätze für die Verifikation und Validierung mittels Testen – insbesondere, wenn verschiedene Teilsysteme von verschiedenen Herstellern geliefert werden. Am Beispiel von EULYNX, einem Standard für die nächste Generation elektronischer Stellwerke, wird das Konzept des hierarchischen, modularen Testens vorgestellt. Es sieht vor, verschiedene Kombinationen von Teilsystemen generisch zu testen und im Anschluss in verschiedenen spezifischen Anwendungen zu nutzen. Es werden manuelle und automatisierte Verfahren zur Testfallerstellung diskutiert sowie Konzepte für eine effiziente Testausführung aufgezeigt.

1 Einleitung

Derzeit arbeiten viele Infrastrukturbetreiber an der Modularisierung und Standardisierung von elektronischen Stellwerken.

1.1 EULYNX

In Deutschland laufen entsprechende Aktivitäten der DB Netz unter dem Namen DSTW (Digitales Stellwerk), vormals NeuPro (Neuausrichtung der Produktionssteuerung). Das europäische Gegenstück ist die EULYNX Initiative [1], die inzwischen zwölf westeuropäische Infrastrukturbetreiber umfasst. Das Ziel ist in beiden Fällen das gleiche: Es soll die Nutzung von Standardkomponenten (COTS, commercial off-the-shelf) für die Kommunikation zwischen Teilsystemen sowie die Integration von Produkten verschiedener Hersteller für Neusysteme ermöglicht werden. Dies wird erreicht, indem im Rahmen einer Standard-Stellwerksarchitektur einzelne Teilsysteme identifiziert und die Schnittstellen zwischen ihnen standardisiert werden. Bild 1 zeigt die Architektur, die durch EULYNX definiert wurde (nahezu identisch mit derjenigen für DSTW). Das zentrale Teilsystem des Stellwerkskerns besitzt dabei Schnittstellen zu Feldelementen wie Lichtsignal- oder Weichencontrollern, mit denen es über standardisierte IP-basierte Kommunikation Nachrichten austauscht.

Um eine klare und eindeutige Spezifikation der Schnittstellen zu erhalten, wurde ein modellbasierter Ansatz in den Projekten gewählt, der verschiedene Notationen der Systems Modeling Language (SysML) verwendet. Er ist mit einem modellbasierten Systems-Engineering (MBSE)-Prozess hinterlegt, der die einzelnen Schritte definiert, um zu einer Schnittstellenspezifikation zu gelangen. Eine fertige Spezifikation umfasst Use Cases sowie das Schnittstellenverhalten in Form von Diagrammen, ergänzt durch eine detaillierte Beschreibung der über die Schnittstelle ausgetauschten Nachrichten sowie einige Anforderungen, die in textueller Form verblieben sind.

Der gewählte Ansatz weist vielfältige Vorteile gegenüber der bisherigen Praxis der Spezifikation und Beschaffung von Stellwerkssystemen

Modular safety-critical systems require new approaches to verification and validation by testing, especially if different subsystems are provided by different suppliers. This paper introduces the concept of hierarchical, modular testing using the example of EULYNX, the future generation of railway interlocking systems. The intention is to test different combinations of subsystem products generically and subsequently to use them in various specific applications. Manual and automatic approaches to the generation of test cases will be discussed, as well as concepts for efficient test execution.

1 Introduction

Many railway infrastructure managers are currently working on the modularisation and standardisation of interlocking subsystems and the communication among these subsystems.

1.1 EULYNX

In Germany, DB Netz is currently running a project called DSTW (Digitales Stellwerk/Digital Interlocking), which was formerly known as NeuPro (Neuausrichtung der Produktionssteuerung/Renewal of production control). Its European counterpart is the EULYNX initiative [1], which now consists of twelve Western European infrastructure managers. DSTW and EULYNX share the same goal: to enable the use of commercial off-the-shelf (COTS) components for subsystem communication and to permit the integration of solutions made by different manufacturers into newly installed systems. This is achieved by identifying signaling subsystems as part of a standard interlocking architecture and by standardising the interfaces between them. Fig. 1 shows the architecture which is defined by EULYNX (almost identical for DSTW). The central interlocking core subsystem is connected with the field elements, i. e. a light signal or point machine controllers, using standardised IP-based communication channels.

A model-based approach was adopted in the projects using several notations from the Systems Modeling Language (SysML) in order to obtain clear and unambiguous specifications for the interfaces. It is supported by a model-based systems engineering (MBSE) process which defines the sequence of steps which need to be taken in order to complete an interface specification. In the end, the specification contains use cases and interface behaviour in diagrammatic form together with a detailed description of the messages which can be sent via the interface and some requirements which remain in textual form.

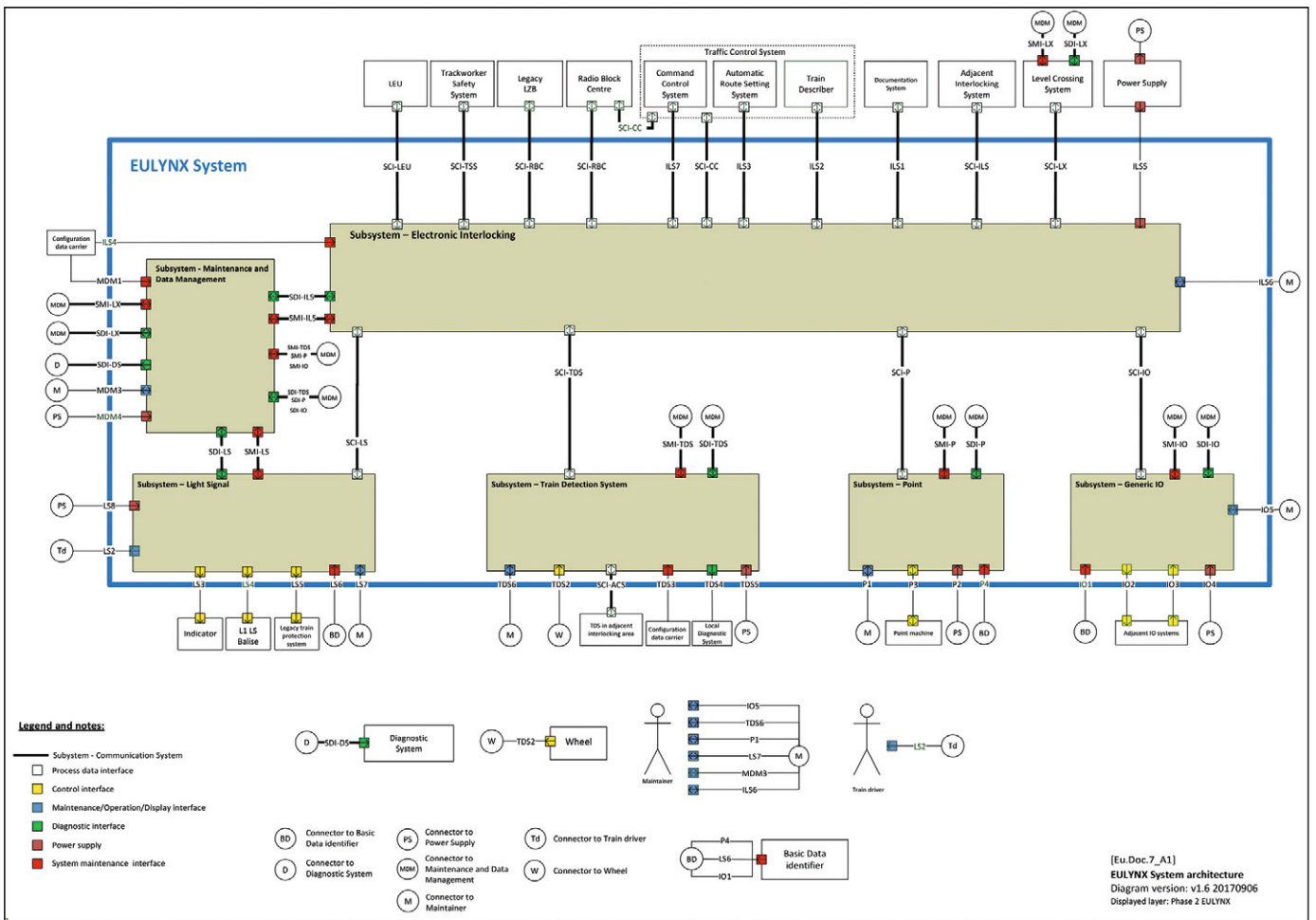


Bild 1: EULYNX Architektur

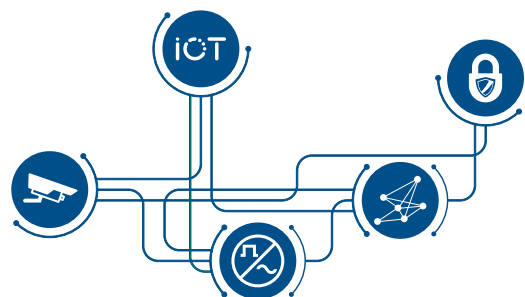
Fig. 1: EULYNX architecture Quelle / source: <https://eulynx.eu/index.php/documents/published-documents/open-availability/02-phase-2/116-20171212-eulynx-system-definition-appendix-a1-v2-0-0-a>

auf. Beispielsweise ist es möglich, verschiedene Teilsysteme eines Stellwerks an verschiedene Hersteller zu vergeben; Teilsystemhersteller haben die Möglichkeit, neue Märkte in Europa zu erschließen; und die Ver-

This approach has many advantages when compared with previous interlocking specifications and procurement practices. For example, it is possible to award different subsystems in an inter-

Digitalisierung erfolgreich gestalten vom Sensor bis zum Service

- Smart KRITIS
- Digitalisierte Bahnhöfe
- Critical Communication & Announcements
- Robust Connectivity



www.euromicron.de

InnoTrans Halle 4.1
Stand 312



Besuchen Sie uns!



euromicron
Deutschland GmbH

MICROSENS
euromicron group



euromicron

haltensmodelle können simuliert werden, um das spezifizierte Verhalten zu validieren [6]. Andererseits stellt die modulare Architektur neue Herausforderungen an den Sicherheitsnachweis und die Zuverlässigkeit jedes einzelnen Teilsystems und des daraus zusammengesetzten Gesamtsystems.

1.2 Herausforderungen für Testen und Zulassung

Testen ist das wichtigste Verfahren zur Verifikation und Validierung (V&V) softwarelastiger Systeme. Traditionell werden elektronische Stellwerke als Ganzes von einem Hersteller geliefert und basieren auf dessen generischen Produkten. Alle notwendigen V&V-Aktivitäten werden durch den Hersteller geplant und ausgeführt. Die Anforderungen hierfür leiten sich aus Standards, vor allem den CENELEC-Normen, und Verordnungen ab. Die Produkte werden in herstellereigenen, meist hochautomatisierten Testlaboren durch generische und spezifische Tests geprüft.

Diese Verfahren ändern sich zwangsläufig, wenn die EULYNX-Architektur und neue Lieferantenaufteilungen durch die Infrastrukturbetreiber eingeführt werden. Verschiedene Hersteller liefern dann Teilsysteme als generische Produkte. Diese werden in Umsetzungsprojekten zu spezifischen Stellwerksanlagen integriert. Je nach vertraglichen und gesetzlichen Regelungen wird der Betreiber selbst für die Integrationsphase und alle damit verbundenen Testprozesse verantwortlich sein.

Für eine Umsetzung dieser Konstellation müssen verschiedene Aspekte berücksichtigt werden:

1. Eine große Anzahl von Produktkombinationen (Teilsysteme verschiedener Hersteller kommunizieren über standardisierte Schnittstellen) ist möglich
2. Das Management der Testprozesse wird deutlich aufwendiger, da sich Tests auf mehrere Labore und Beteiligte verteilen
3. Produktunabhängige Testspezifikationen werden benötigt, die jedoch wiederum an die spezifischen Anforderungen der Produkte und Labore angepasst werden müssen

In den folgenden Kapiteln werden zur Handhabung dieser Aspekte Konzepte vorgestellt und diskutiert.

2 Hierarchisches, modulares Testen

Die mit EULYNX eingeführte Modularisierung der Stellwerke hat auch Auswirkung auf die Kategorisierung von Produkt und Anwendung gemäß der CENELEC-Standards. Nun wird nicht mehr das gesamte Stellwerkssystem als generische Anwendung betrachtet, sondern die Summe der generischen Implementierungen der verschiedenen Teilsysteme. Die spezifische Anwendung ist nach wie vor das projektierte Gesamtstellwerkssystem für eine bestimmte Bahnanlage, das sich nun aus verschiedenen ebenfalls zu projektierenden generischen Produkten verschiedener Hersteller zusammensetzt. Die konkrete Zusammensetzung kann sich somit in verschiedenen Anlagen unterscheiden.

2.1 Ansatz

Entsprechend müssen auch die Testprozesse angepasst werden. Ein Test des Gesamtsystems wäre erst nach Errichtung der Anlage im Feld möglich, da erst hier die Gesamtheit aller Teilsysteme zur Verfügung steht. Die Durchführung sämtlicher Tests zu diesem Zeitpunkt wäre extrem zeitaufwendig, teuer und würde den Bahnbetrieb massiv behindern.

Der Ansatz des hierarchischen, modularen Testens zielt auf die Handhabung derartiger verteilter Architekturen ab. Im Gegensatz zum klassischen V-Modell werden verschiedene Phasen von Tests definiert, bei denen generische Systeme bzw. Kombinationen dieser auf jeweils relevante Eigenschaften getestet werden. Kern des Ansatzes ist die Struk-

locking system to different suppliers, subsystem suppliers have the opportunity to develop new markets in Europe and it is possible to simulate the model in order to validate the specified behaviour [6]. On the other hand, the modular architecture places new demands on the proof of safety and the reliability of each individual subsystem and of the overall system.

1.2 Challenges in testing and certification

Testing is the main technique used for verification and validation (V&V). Traditional solid state interlocking systems are provided by a single manufacturer and are based upon the manufacturer's generic products. All necessary V&V activities are therefore performed by the manufacturer. The requirements for V&V are based on the regulations implemented by the legal authorities and the standards, especially the CENELEC RAMS cycle (Reliability, Availability, Maintenance, Safety) and the development regulations. In practice, the manufacturers operate test labs where the products are inspected using both generic and specific tests.

This practice needs to be changed when the EULYNX architecture is introduced and a new commercial ordering scheme is employed by the infrastructure manager. If different manufacturers deliver subsystems as generic products, all the necessary instances of these products will need to be integrated into the project-specific interlocking system. The operator will then be responsible for the system integration phase with all its necessary test processes according to the contractual and legal rules. Different aspects need to be taken into account in order for this constellation to be implemented:

1. A large number of product combinations (subsystems from different manufacturers communicating through standardised interfaces) is possible
2. The test process management will become more costly, as the testing of subsystems in different test labs (at different locations) may be necessary
3. Product-independent test specifications are necessary, while the test cases have to be adapted to the specific requirements of the products and the test laboratories

The following chapters introduce and discuss the concepts needed to deal with these challenges.

2 Hierarchical, modular testing

The modularisation of interlocking systems will change the basic categorisation of products and applications according to the CENELEC standards. Instead of the full interlocking system, the sum of the generic implementation of the different subsystems will now need to be approved. The specific application is still the specific realisation of an interlocking system for a dedicated railway system and it might comprise generic products from different manufacturers. Hence, the realisation might be different for different applications. It is no longer a homogeneous, generic product which needs to be configured for the specific infrastructure.

2.1 General approach

The test processes need to be adapted accordingly. Given that the collection of all the different constituents will only be available as a specific installation in the field, it cannot be subjected to a system test beforehand. The execution of intensive and time consuming tests after installation would also certainly be impractical.

The concept of hierarchical, modular testing proposed here aims to deal with modularised architectures. Unlike the ordinary test-

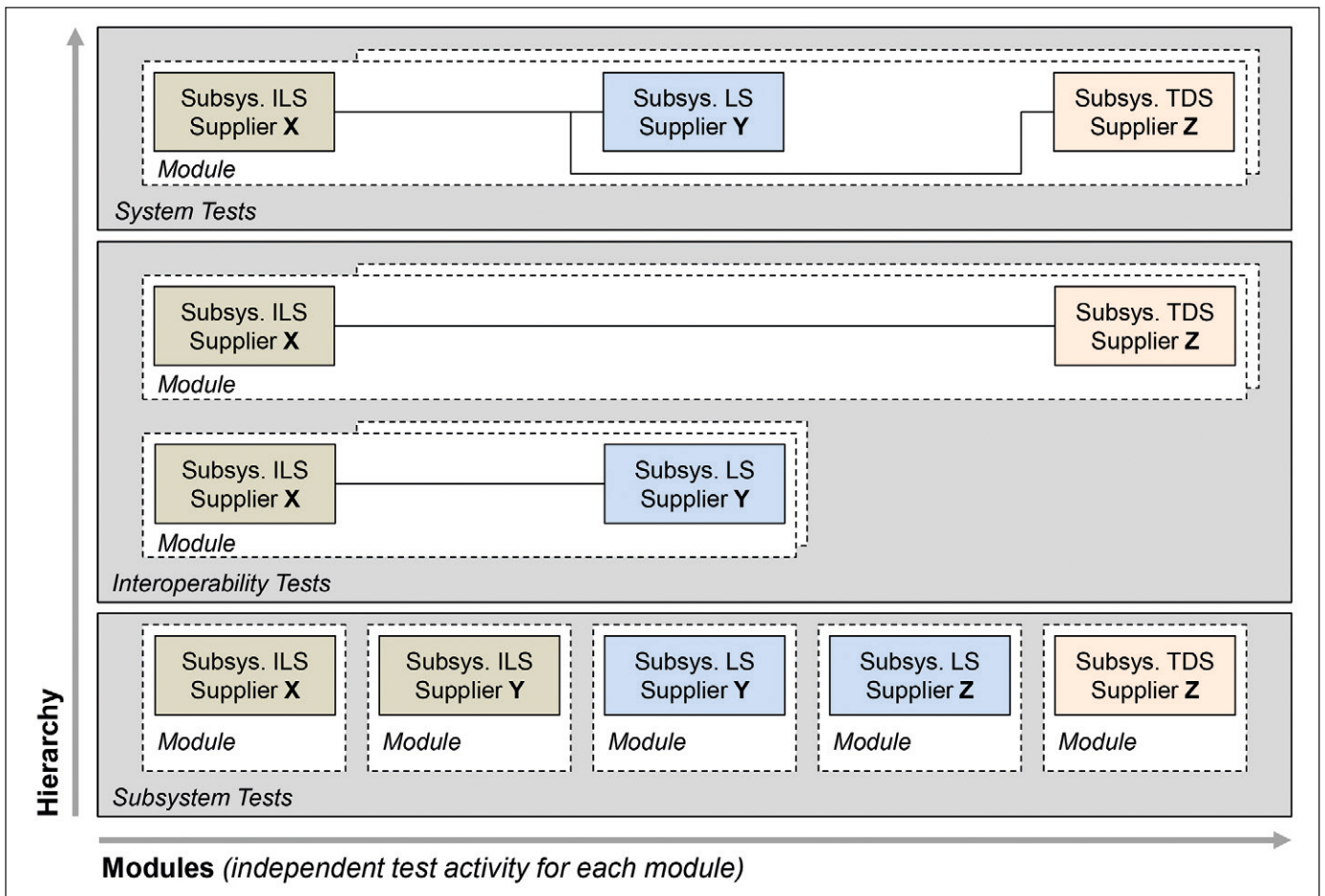


Bild 2: Hierarchisches, modulares Testen am Beispiel der EULYNX-Architektur

Fig. 2: Hierarchical, modular testing – an example of the EULYNX architecture

turierung von Testaktivitäten in sogenannte Module, die dann auf verschiedene hierarchische Testebenen verteilt werden. Bild 2 veranschaulicht dies.

Module sind hierbei Kombinationen aus einem oder mehreren vollständig implementierten Teilsystemen. Sie werden mit dem Ziel kombiniert, eine definierte Menge an Eigenschaften an dieser Konstellation zu testen. Der Aufbau der Module wird von den jeweiligen Testzielen bestimmt und kann ggf. auch von projektspezifischer, zeitlicher Verfügbarkeit der entsprechenden Produkte abhängen.

Alle Module werden im Sinne des Testens als Blackboxes betrachtet, die über eine Menge von logischen Schnittstellen – wiederum eine Untermenge der physikalischen Schnittstellen aller Teilsysteme im Modul – mit der Umwelt kommunizieren.

Im Falle von EULYNX ist genau ein Teilsystem eines Herstellers das einfachste Modul. Zwei Teilsysteme, die über die standardisierten Schnittstellen (SCI) kommunizieren, bilden ein weiteres Modul, das auf einer höheren hierarchischen Ebene eingeordnet wird.

In einer Ebene der Testhierarchie werden Module zusammengefasst, die eine vergleichbare logische oder physikalische Struktur haben. Damit ergeben sich vergleichbare Anforderungen an die Testsysteme und die Testspezifikationen auf jeder hierarchischen Ebene.

In der Praxis steigen mit jeder hierarchischen Ebene die technischen und organisatorischen Aufwände für die Testdurchführung. Dies ist insbesondere auf folgende Sachverhalte zurückzuführen:

- Die wachsende Komplexität der Module
- Die steigende Zahl an eingebundenen Organisationseinheiten und Personen

ing scheme following the V-model, various test phases are defined, which can be used to test generic systems or combinations for the relevant properties. The core of this approach involves the structuring of the test activities in so-called modules, which can be divided into different hierarchical tests levels. Fig. 2 illustrates this.

Here, the modules are logical sets of one or more fully implemented subsystems. They are combined in order to test or prove a dedicated set of properties. The module setup depends on the test goals and the availability of the necessary subsystems during the project.

Each module is handled as a black-box which communicates with its environment via a set of interfaces. These interfaces are a subset of the physical interfaces of each subsystem contained within the module.

In the case of EULYNX, the simplest module consists of one subsystem from one manufacturer. The module to be tested at the next hierarchical level consists of two subsystems communicating via a standardised interface.

The modules are pooled in a group which has a comparable logical or physical structure on a level of the hierarchy. The test infrastructure, i.e. the test frames, can be used for each module since these modules have interfaces of a similar structure.

In practice, the technical and organisational effort increases for each level of the hierarchy. Some of the reasons for this are:

- the increasing complexity of the modules
- the increasing number of involved organisations and individuals

- Räumliche Verteilung der Testausführung (mehrere Labore, Feldtest, ...)
- Die steigende Komplexität der Systeme und Schnittstellen erschweren das Herstellen von Testvorbedingungen, die Testausführung und das Prüfen der Nachbedingungen.

Zwangsläufig werden auch die Kosten für die Testdurchführung mit den hierarchischen Ebenen steigen. Demzufolge ist es sinnvoll, eine Eigenschaft auf der technisch bzw. logisch niedrigstmöglichen Ebene durchzuführen und Wiederholungen zu vermeiden.

2.2 Anwendung für EULYNX

Der Ansatz des hierarchischen, modularen Testens dient der effizienten Strukturierung des Testprozesses. Für eine Anwendung auf EULYNX-Projekte müssen einige zusätzliche Aspekte berücksichtigt werden:

- EULYNX Architektur
- Normative und gesetzliche Rahmenbedingungen des jeweiligen Landes
- Vertraglich vereinbarte Lieferantenbeziehungen für Teilsysteme
- Vereinbarte Rollenaufteilung zwischen Lieferindustrie und Betreiber
- Verfügbarkeit von Testsystemen und Testspezifikationen.

Um diese Punkte möglichst allgemein zu berücksichtigen, kann aus dem Ansatz des hierarchischen, modularen Testens ein Testprozess mit vier aufeinanderfolgenden Phasen abgeleitet werden, wie er in Bild 2 (Phasen 1–3) veranschaulicht wird. Jede der Phasen bildet dabei eine Ebene der Hierarchie. Der Übergang von Teilsystemen in eine höhere Ebene ist nur nach erfolgreichem Test auf der aktuellen Ebene möglich. Somit wird die Qualität der zu prüfenden Systeme in den jeweiligen Phasen sichergestellt.

Die Testdurchführung in den Phasen 1 und 2 sowie Teilen der Phase 3 erfolgt im Labor. Damit sinkt der Aufwand für Feldtests erheblich.

Phase 1: Konformitätstests von Teilsystemen

In der ersten Phase bestehen die Module aus einzelnen EULYNX-Teilsystemen, bspw. einem Lichtsignalcontroller. Ziel dieser Phase ist der generische Test auf Konformität zu funktionalen und nichtfunktionalen Anforderungen der Lasten- und Pflichtenhefte.

Da ein Teilsystem üblicherweise von einem Hersteller entwickelt wird, kann auch das Testen dieser Phase in dessen Verantwortung liegen. Der Vorteil ist, dass dann die Testinfrastruktur (Labor, Testgestelle, Software) für eine effiziente, in großen Teilen automatisierte Durchführung der Tests genutzt werden kann [3].

Phase 2: Interoperabilitätstest der standardisierten Schnittstellen

In der zweiten Phase wird die Kommunikation zwischen Teilsystemen betrachtet, indem die Interoperabilität über die standardisierten Schnittstellen (Standard Communication Interface – SCI) geprüft wird. Für verschiedene Teilsysteme existieren jeweils eigene SCI-Spezifikationen, bspw. die SCI-LS für die Kommunikation zwischen Stellwerk und Lichtsignalcontroller.

Die Tests in dieser Phase werden einzeln für jede dieser Schnittstellen spezifiziert und ausgeführt. Die jeweiligen Module bestehen demzufolge jeweils aus dem Stellwerkskern und dem betreffenden Teilsystem. Da beides von verschiedenen Herstellern kommen kann, müssen die Tests ggf. unter Verwendung mehrerer Labore durchgeführt werden. Entsprechend muss die Kommunikation zwischen diesen zur Ausführung der teilsystemübergreifenden Testfälle ermöglicht werden.

Ziel der Tests ist der Nachweis, dass die kommunizierenden Produkte (Teilsystem A von Hersteller X, Teilsystem B von Hersteller Y) interoperabel sind. Die zugehörige Testspezifikation sollte generisch sein, sodass das Ergebnis der Tests die Verwendung dieser Kombination für jede spezifische Anwendung qualifiziert.

- the spatial situation for the test execution (separated labs, field test, ...)
- the increasing complexity of the systems and interfaces complicates the establishing of the test preconditions, the test execution and the checking of postconditions

Accordingly, it can be assumed that the testing costs will increase with the level of hierarchy. It is advantageous to test a feature as early as possible (at a low hierarchical level) and to avoid the repetition of tests at higher levels.

2.2 EULYNX adaptation

The concept of hierarchical, modular testing can be used for the efficient structuring of the test process. Different aspects have to be considered with regard to the adaptation to EULYNX:

- the EULYNX architecture
- supplier contracting for different subsystems
- normative and legal requirements (CENELEC, approval, ...)
- contractual conditions between the infrastructure manager and the supply industry
- the availability of test infrastructure and test specifications.

The result is a test process consisting of four consecutive tests phases as illustrated in fig. 2. Each phase constitutes a level in the test hierarchy mentioned above. The transition to the next phase is realised as a quality gate. The subsystems are only allowed to enter the next phase, if the tests in the previous one have been completed successfully.

Phases 1 and 2, as well as parts of Phase 3, can be realised in the lab. Hence, the on-site testing expenses are minimal.

Phase 1: Conformity tests on the components

In the first phase, the tested module consists of a single EULYNX subsystem, e. g. a light signal controller. The aim of this phase is to generically inspect the conformity with the specifications. This includes functional as well as non-functional requirements.

Since subsystems are typically developed and produced by a single supplier, this testing phase can be realised at the responsibility of the supplier. The test infrastructure (the laboratory, frames and software) can be used efficiently for automated test execution [3].

Phase 2: Interface interoperability testing

The communication between the subsystems is the focus of the second phase. The interoperability of two or more components needs to be checked. The exchanged messages are standardised as “Standard Communication Interfaces” (SCI) by different requirement specifications, e. g. the SCI-LS as the protocol between the electronic interlocking system and the light signal controller. The tests are specified and executed one by one for each single SCI. Therefore, a module consists of the electronic interlocking subsystem and one additional subsystem. Since the module’s subsystems may be supplied by different manufacturers, the communication must be realised between different test architectures or labs.

The goal of the test is the proof that the communicating products (subsystem A from manufacturer X and subsystem B from manufacturer Y) are interoperable. The test specifications should be generic, so that the test results are valid for any specific realisation of this combination of products.

Phase 3: The system test

Unlike the previous phases, Phase 3 is part of a specific project test. The overall system, which has been configured to

Phase 3: Systemtest

Im Gegensatz zu den bisher beschriebenen Phasen ist der Systemtest in Phase 3 Teil der spezifischen Projekttests. Alle beteiligten Systeme werden wie in der Zielanlage projektiert und getestet. Demzufolge müssen alle Instanzen der Teilsysteme sowie das Übertragungssystem physisch verfügbar sein. Kann dies noch nicht bewerkstelligt werden, können Simulatoren oder Emulatoren helfen, einen Teil der Anlage nachzubilden. Ziel des Systemtests ist es, die Gesamtsystemanforderungen, in erster Linie also die betrieblichen Anforderungen, zu prüfen. Folglich wird nicht nur die Implementierung eines jeden Produktes getestet, sondern auch die Projektierungen und Einstellungen. Des Weiteren wird indirekt die Konsistenz und Korrektheit der Anforderungsspezifikationen an Teilsysteme im Verhältnis zu den Anforderungen auf Gesamtsystemebene geprüft.

Es ist prinzipiell möglich, Teile des Systemtests im Labor durchzuführen. Da dort in vielen Fällen das Gesamtsystem aufgrund der Menge einzusetzender Teilsysteme nicht komplett zur Verfügung steht, wird ein Teil der Tests mit sämtlichen Teilsystemen im Feld stattfinden müssen.

Phase 4: Betriebserprobung

Gesetzliche Zulassungsprozesse bedingen meist die Prüfung verschiedener, operativer Parameter. Deshalb muss das finale, in Betrieb befindliche System entsprechend überwacht werden. Relevante Parameter sind bspw. die Zuverlässigkeit bzw. Verfügbarkeit sowie die Bewertung von Umwelteinflüssen.

Die Überprüfung dieser Parameter erfolgt nicht durch klassisches Testen, sondern wird durch Auswertung von Betriebs- und Instandhaltungsdaten realisiert. Im Falle von EULYNX kann das Teilsystem Maintenance and Data Management (MDM) hilfreich sein, da hier zahlreiche standardisierte Diagnosedaten der Teilsysteme zentral gesammelt werden.

3 Testfallerstellung

Um die Module der verschiedenen hierarchischen Ebenen effizient testen zu können, sind entsprechend angepasste Testsuiten notwendig.

3.1 Standardisierte und produktspezifische Testsuiten

Für den Test eines Teilsystems (Phase 1 in Abschnitt 2.2) ermöglichen es die standardisierten Teilsystemschnittstellen, einen Teil der Testfälle

the given railway infrastructure, is tested there. As such, instances of each subsystem as well as the transmission system must be physically available. Simulators or emulators can be used to emulate part of the system, if this cannot be accomplished, but the physical communication system must be available.

The aim of the system test is to check the overall system requirements, especially the railway operation safety. Hence, not only the implementation of each product is checked, but also the site data and the configuration of each of the subsystems. Additionally, the consistency and correctness of the requirement specifications can be validated.

It is possible in principle to execute part of the tests in the laboratory. Given, however, that the complete system (all the instances of the subsystems) may not be fully available due to the large amount of used subsystems, some of the tests will have to take place in the field with all the subsystems.

Phase 4: Field operation testing

Legal authorisation processes require the approval of several operational parameters. Hence, the final overall system needs to be monitored during daily operations. The main parameters are availability or reliability and the environmental influences.

The inspection of the parameters is not a classical test with sets of inputs and outputs, but it is mainly realised through the evaluation of operational parameters. For EULYNX, the Maintenance and Data Management (MDM) subsystem may help with the evaluation since standardised diagnostic information from all the subsystems is collected there centrally.

3 Test design

Adapted test suites are necessary in order to test the modules efficiently at the different hierarchical levels.

3.1 Standardised and product-specific test suites

When testing a subsystem (Phase 1 from Section 2.2), it becomes possible to formulate part of the test cases independently of the specific product due to the standardised sub-

EISENBAHNTECHNIK HAUTNAH ERLEBEN

BBR
VERKEHRSTECHNIK



ELEKTRONISCHE STELLWERKE
FUNKAUFWERTUNG

ZUGBEEINFLUSSUNG
RGB-LED TECHNIK

FAHRGASTINFORMATION

Halle 4.2, Stand 107



le unabhängig vom konkreten Produkt zu formulieren. Folglich kann, basierend auf der Anforderungsspezifikation (Lastenheft) des Teilsystems, eine standardisierte Testsuite erstellt und auf Produkte verschiedener Hersteller angewendet werden. Ein anderer Teil der Testfälle wird jedoch weiterhin vom Design des einzelnen Produktes abhängen, d.h. diese Testfälle basieren auf der Entwurfsspezifikation (Pflichtenheft). Generell sollte diese produktspezifische Testsuite so klein wie möglich gehalten werden in dem Sinne, dass jedes Testziel, das durch einen standardisierten Test erreicht werden kann, nicht durch die spezifische Testsuite geprüft werden sollte. Während die spezifischen Tests für jedes Produkt durch den Hersteller zu erstellen sind, ist es bei den standardisierten Tests möglich, dass sie nur einmalig und federführend durch den Infrastrukturbetreiber (als Auftraggeber) spezifiziert werden. Für das Testen der Schnittstelleninteroperabilität (Phase 2) müssen die Testfälle für jede Schnittstelle derart spezifiziert werden, dass jede vorgesehene Nachricht mit angemessenen Variationen ihrer Parameter zwischen den Teilsystemen geprüft wird. Auch unterschiedliche Abfolgen der Nachrichten müssen betrachtet werden. Sowohl in Phase 2 als auch Phase 3 sollten die Tests vollständig von Implementierungsdetails abstrahieren, sodass die Testsuiten produktunabhängig sind und für Kombinationen von Produkten desselben Typs wiederverwendet werden können. Da der Systemtest (Phase 3) die real umzusetzende Projektierung verwendet, muss hier eine abstrakte, parametrisierte Testsuite zu einer konkreten instanziiert werden, z.B. indem nicht benötigte Testfälle entfernt oder andere auf alle Instanzen einer bestimmten Teilsystemkombination oder alle möglichen Fahrstraßen angewendet werden.

Klassischerweise werden Testfälle manuell erstellt. Um die dann folgende Ausführung der (meisten der) Testfälle oder Testsequenzen zu automatisieren, müssen die Testfälle bzw. -sequenzen in ein maschinenlesbares Format gebracht werden. Dieses Format hängt von der vom Hersteller verwendeten Testumgebung ab. Für die standardisierten Testsuiten für die Teilsysteme ist es daher vorteilhaft, sie in fertig zusammen-

system interface(s). As such, a standardised test suite can be specified and applied to products from different suppliers based on the subsystem's requirement specifications. However, some tests will still depend on the design of the particular product, i.e. they are based on the design specifications. Generally, this product-specific test suite should be kept as small as possible in the sense that each test goal which can be reached using a standardised test should not be tested with a specific test suite. While the specific tests need to be specified for each product by the supplier, the standardised ones are specified only once and possibly by someone else.

When testing interface interoperability (Phase 2), the test cases for each interface need to be defined in such a manner so that each specified telegram with appropriate parameter coverage is transmitted between the components. Different sequence orders have to be considered, too. In both Phase 2 and Phase 3, the tests should be fully abstracted from the implementation details, so that the test suites are product-independent and can be reused for combinations of products of the same type. Since the system test (Phase 3) uses the actual configuration which is to be implemented, an abstract, parameterised test suite needs to be instantiated here as opposed to a specific one, e. g. by removing unnecessary test cases or by applying others to all instances of a certain subsystem combination or to all possible routes.

Test design is usually realised manually. In order to automate the following execution of (most) test cases or test sequences, the test cases or sequences must be converted into a machine-readable format. This format depends on the test environment used by the supplier. As such, it is favourable to provide the standardised test suites for the subsystems in a readily composed test sequence and in a supplier-independent machine-readable format. The tests can either be executed in an independent laboratory which supports that format (e.g. the "test system" mentioned in Section 4 below) or in a supplier's lab, if the supplier provides an adapter for its proprietary format. The European Train Control System (ETCS) Subset 076 [2] test cases for ETCS on-board units can serve as orientation for the creation of such a format. Those test cases are interface-centred just like the ones which should be created for the EULYNX subsystems.

3.2 Towards automation

Different model-based approaches are increasingly being used in other industries as an alternative to manual test design in order to automate the test design process. They require a model to be created in a modeling language (often a fragment of the Unified Modeling Language UML or of SysML) and a software tool which generates test cases from that model (fig. 3) which meet predetermined coverage criteria. Since a large part of the EULYNX interface specifications have already been created using a model-based approach (see Section 1.1), model-based testing becomes particularly attractive here [5]. The greatest benefits in terms of automation can be expected from generators which use a sophisticated combination of formal methods in order to generate complete test cases, including test data and test oracles, from an abstract system model.

The use of model-based testing means that the main effort shifts to model creation. The initial effort required to handle a modelling tool, to comply with the restrictions imposed by a generator tool and to find the right level of abstraction of the model may be high, while the model creation may require de-

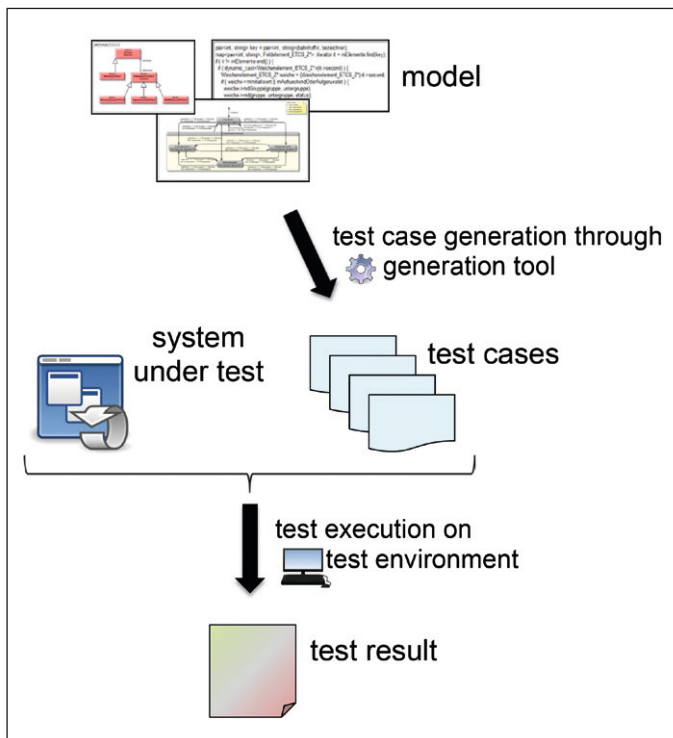


Bild 3: Testautomatisierung unter Nutzung der Testfallgenerierung aus einem Modell

Fig. 3: Test automation using test case generation from a model

gestellten Testsequenzen und in einem herstellerunabhängigen, maschinenlesbaren Format bereitzustellen. Die Tests können entweder in einem unabhängigen Labor ausgeführt werden, das dieses Format unterstützt (z. B. auf der in Abschnitt 4 weiter unten erwähnten „Testsystemarchitektur“), oder im Labor eines Herstellers, wenn dieser einen Adapter zu seinem proprietären Format bereitstellt. Für die Erstellung eines herstellerunabhängigen Formats können die Subset 076 [2]-Testfälle für On-board-Rechner des europäischen Zugsicherungssystems ETCS als Vorbild dienen. Diese Testfälle sind ebenso schnittstellenorientiert wie diejenigen, die für die EULYNX-Teilsysteme zu erstellen sind.

3.2 Ein Automatisierungsansatz

Als Alternative zur manuellen Testfallerstellung werden in anderen Industrien zunehmend verschiedene modellbasierte Ansätze verwendet, um die Testerstellung zu automatisieren. Grundlage hierfür ist die Erstellung eines Modells in einer Modellierungssprache (oft eine Untermenge der Unified Modeling Language UML oder von

veloper skills rather than classical tester skills. However, the model-based approach starts to pay off during the model creation stage, because the model provides an integrated view of the whole test suite and forces the modeller to be quite concise. Another advantage involves the much easier handling of changes which occur during development and maintenance and in new product versions: only the central model needs to be adapted, while the whole test suite is simply updated by regeneration. The automation of the test design may also enable an earlier start to testing.

The most important criterion is of course the quality of the resulting test suite: the requirements are usually linked in the model and then automatically traced so that the requirement coverage can be ensured in the same way as for manually created suites. However, in addition to that, the test suite is generated systematically in order to fulfil a well-defined structural coverage criterion such as transition coverage for

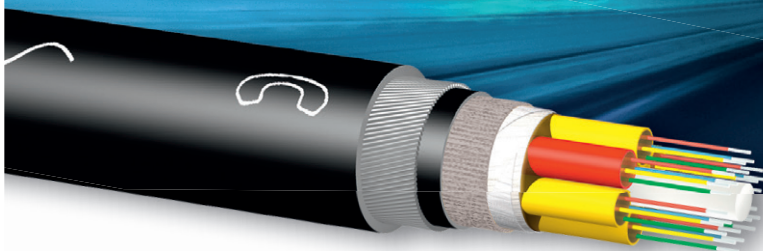
Bayka
seit 1885

Aus *Liebe* zum Kabel

www.bayka.de

Menschenleben schützen

Mehr Sicherheit durch Brandschutzkabel.



Besuchen Sie uns auf der InnoTrans!
18. - 21. September | Halle 12 / Stand 104

Kontaktieren Sie uns für Ihr Messticket: marketing@bayka.de

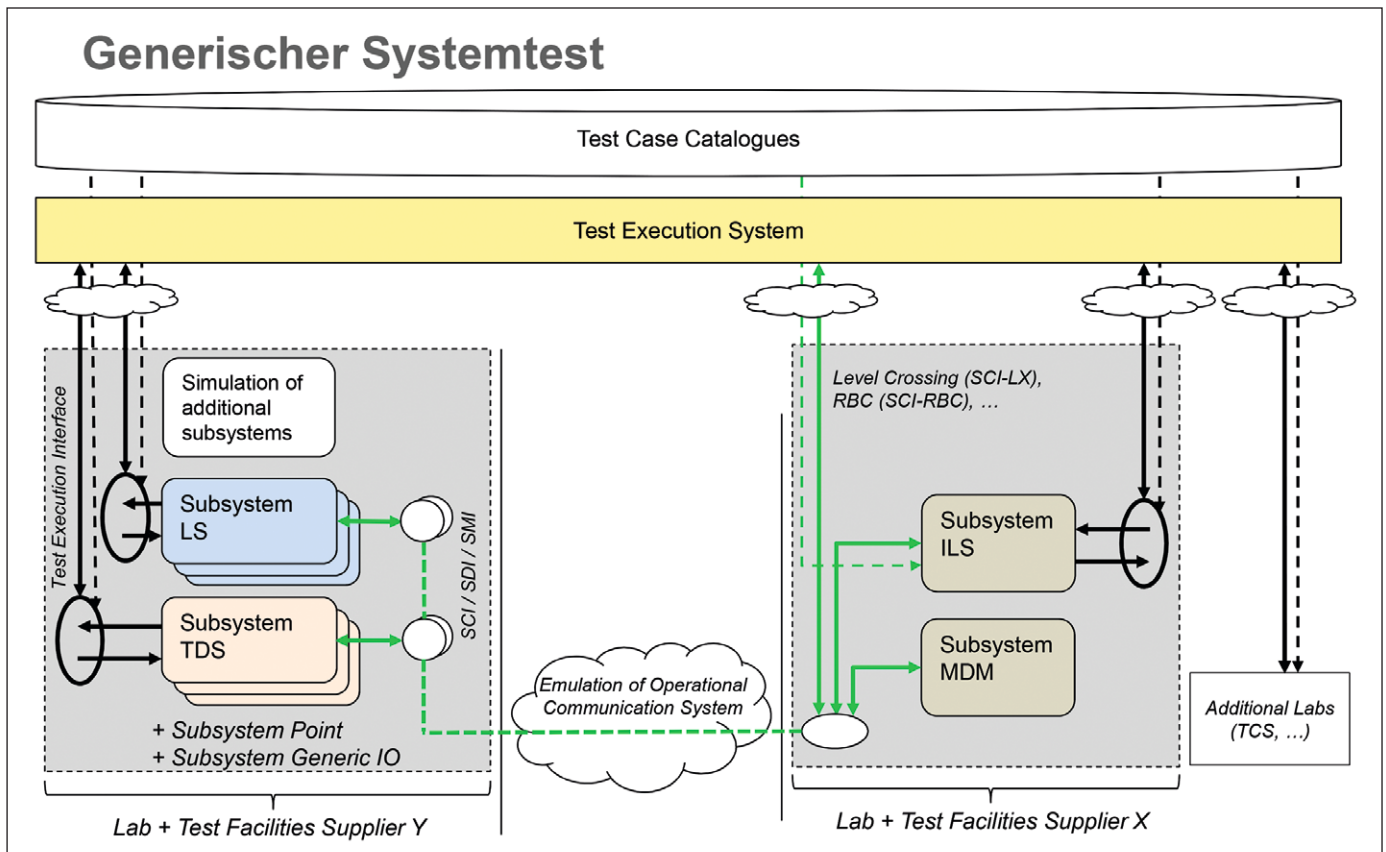


Bild 4: Basisarchitektur für die automatisierte Testausführung unter Nutzung mehrerer, heterogener Testlabore
 Fig. 4: Basic architecture for test execution using several, heterogeneous test labs

SysML) und ein Softwarewerkzeug, das aus diesem Modell Testfälle generiert (Bild 3), die vorgegebene Abdeckungskriterien erfüllen. Da im Falle von EULYNX große Teile der Schnittstellenspezifikationen bereits unter Nutzung einer modellbasierten Herangehensweise erstellt wurden (siehe Abschnitt 1.1), ist es hier besonders attraktiv, modellbasiert zu testen [5]. Die größten Vorteile durch die Automatisierung sind von Generatoren zu erwarten, die eine ausgefeilte Kombination formaler Methoden verwenden, um aus einem abstrakten Systemmodell vollständige Testfälle zu erzeugen, inklusive Testdaten und Testorakel.

Wird modellbasiert getestet, verschiebt sich der Hauptaufwand des Testens zur Modellerstellung. Der initiale Aufwand, um ein Modellierungswerkzeug zu beherrschen, durch das Generierungswerkzeug bedingte Einschränkungen im Modell zu berücksichtigen und das richtige Abstraktionslevel des Modells zu finden, kann hoch sein. Zudem verlangt die Modellerstellung eher Entwicklerfähigkeiten als klassische Kompetenzen eines Testers. Dennoch beginnt sich der modellbasierte Ansatz bereits während der Modellerstellung auszuzahlen, da das Modell eine integrierte Sicht der gesamten Testsuite bietet und ein hohes Maß an Präzision erzwingt. Ein weiterer Vorteil ist der wesentlich vereinfachte Umgang mit Änderungen, die während der Entwicklung, Wartung oder im Rahmen neuer Produktversionen auftreten: Es muss lediglich das zentrale Modell angepasst werden, und die gesamte Testsuite wird anschließend neu generiert. Die Automatisierung der Testerstellung ermöglicht es daneben, früher mit dem Testen zu beginnen.

Das wichtigste Kriterium ist die Qualität der resultierenden Testsuite: Normalerweise werden die Anforderungen im Modell referenziert und im Weiteren automatisch deren Nachverfolgbarkeit unterstützt, sodass Anforderungsabdeckung ebenso wie für manuell erstellte Suiten si-

state diagrams. Possible issues with test case generation may include a (overly) high number of resulting test cases (or unacceptable generation time), sub-optimally chosen input values or a high degree of redundancy in the test suite. Understanding and trying out generator options or the appropriate prioritisation of test cases can help to overcome such problems.

The German Aerospace Center (DLR) is currently investigating the applicability of model-based testing to signaling subsystems or their interfaces. A major challenge concerns the fact that, on the one hand, the subsystem or interface model should be generic (i.e. independent of a specific piece of railway infrastructure), while, on the other hand, the subsystems need to be configured with some specific railway infrastructure in mind in order to be able to execute and test them.

4 The road to test execution

The proposed concept of hierarchical, modular testing and its adaptation to the EULYNX architecture represents a structured process in support of V&V. According to the challenges listed in Section 1.2, it is possible to

1. qualify each combination of products using generic interoperability testing (Phase 2),
2. use the manufacturers' existing test facilities for efficient subsystem testing (Phase 1), and
3. efficiently define formalised test specifications for any phase from the requirement specifications.

However, there are some challenges which need to be faced. The main question is how the test cases can be efficiently executed using two or more test labs (Phases 2 and 3).

chergestellt werden kann. Doch zusätzlich wird die Testsuite systematisch so erzeugt, dass ein definiertes strukturelles Abdeckungskriterium, wie z.B. Transitionsabdeckung für Zustandsdiagramme, erreicht wird.

Mögliche Probleme bei der Testfallgenerierung können eine (zu) hohe Anzahl resultierender Testfälle (oder eine inakzeptable Generatorlaufzeit), nicht optimal gewählte Testdaten oder ein hoher Grad an Redundanz in der Testsuite sein. Das Verstehen und Ausprobieren von Testgeneratoroptionen oder eine passende Priorisierung von Testfällen können helfen, derartige Probleme in den Griff zu bekommen.

Das Deutsche Zentrum für Luft- und Raumfahrt (DLR) untersucht zurzeit die Anwendbarkeit des modellbasierten Testens auf Teilsysteme der Leit- und Sicherungstechnik bzw. deren Schnittstellen. Eine bedeutende Herausforderung stellt dabei dar, dass einerseits das Teilsystem- bzw. Schnittstellenmodell generisch (d. h. unabhängig von einer spezifischen Eisenbahninfrastruktur) sein soll und andererseits die Teilsysteme für eine spezifische Infrastruktur projektiert werden müssen, um sie ausführen und testen zu können.

4 Auf dem Weg zur Testdurchführung

Der vorgestellte Ansatz des hierarchischen, modularen Testens sowie die Adaption auf die EULYNX-Architektur bieten einen strukturierten Prozess zur Unterstützung von V&V. Gemäß den Anforderungen, die in Abschnitt 1.2 aufgeführt sind, ist es damit möglich:

1. jede Produktkombination durch generischen Interoperabilitätstest zu qualifizieren (Phase 2),
2. die existierenden Testsysteme der Hersteller für effizientes Testen der Teilsysteme zu nutzen (Phase 1) und
3. einheitliche und formale Testspezifikationen für jede Phase aus den Lastenheften abzuleiten.

Dennoch müssen einige weitere Herausforderungen betrachtet werden. Eine der Kernfragen besteht darin, wie die Tests in den Phasen 2 und 3 effizient koordiniert und durchgeführt werden können, wenn zwei oder mehr Labore beteiligt sind.

Zum Ersten ist es hierfür notwendig, die Prozessdaten (SCI, Diagnose, ...) zwischen den Teilsystemen in den Laboren möglichst verlässlich und mit geringen Latenzen zu übertragen. Für bestimmte Tests ist es auch zielführend, die Strukturen des Übertragungssystems mit in die Kommunikationspfade zwischen den Laboren zu integrieren, bspw. durch ein weiteres Labor, das sternförmig per geeigneter Übertragungsleitungen mit den anderen Laboren verbunden ist. Auf diese Weise können Einflüsse des Übertragungssystems auf das Systemverhalten zum Teil bewertet werden.

Zum Zweiten ist es auch notwendig, die Ausführung von Testfällen in den beteiligten Laboren zu koordinieren. Im einfachsten Fall erfolgt die direkte Abstimmung der Tester per Telefon. Die Qualität und Effizienz dieses Ansatzes ist jedoch nicht hinreichend – vor allem bei der Ausführung einer großen Zahl an Testfällen. Ein Ansatz zur automatischen Testausführung unter Nutzung mehrerer Labore unterschiedlicher Architektur ist also notwendig. Bild 4 illustriert eine generische Architektur hierfür.

Das DLR arbeitet derzeit an der Ausgestaltung und Umsetzung einer solchen Testsystemarchitektur [4]. Das Ziel ist, eine verteilte Lösung anzubieten, bei der die Adaptierung der Bestandssysteme in den betreffenden Laboren möglich ist und die Koordinierung zwischen den Laboren zentral erfolgt.

Das im Aufbau befindliche Labor wird später für Forschung im Bereich der Testautomatisierung und -formalisierung genutzt und auch Industriepartnern zur Durchführung kommerzieller Testkampagnen zur Verfügung stehen. ■

This requires the provision of communication channels for the exchange of all operational data (SCI, maintenance and diagnostic) between the subsystems in the involved labs. In the best case, the communication architecture which has been planned for the field operation is used as part of the interconnection of the labs as well. A suitable solution could be to connect the EULYNX subsystem labs directly to a dedicated communications system lab.

It is necessary to coordinate the execution of the test cases in the labs as well. Another communication channel is necessary to this end. In the simplest case, the testers in the labs can talk by telephone and coordinate their activities in the given test cases and the derived test instructions. However, the quality and efficiency of this approach may not be suitable. A solution for the automated execution of tests in separate and heterogeneous labs is needed. Fig. 4 illustrates an accordingly generic architecture.

DLR is currently working on the configuration and realisation of such test system architecture [4]. The aim is to provide a generic solution which can be used in different labs with different equipment, while the coordination between the individual labs is provided centrally.

The offered test system architecture will be used for research in the area of test automation and formalisation as well as for the commercial test campaigns of industrial partners. ■

LITERATUR | LITERATURE

- [1] EULYNX Webseite, <https://eulynx.eu>, zuletzt aufgerufen am 07.06.2018 um 14:41 Uhr
- [2] European Railway Agency ERTMS Unit: Scope of the test specifications. Subset-076-7, Version 3.1.0, 30.06.2015
- [3] Spaltmann, F.; Pietz, E.; Rieder, M.: Testarchitektur für BÜSA/ESTW, SIGNAL+DRAHT 9/2012
- [4] Hungar, H.; Asbach, L.; Meyer zu Hörste, M.: Laborarchitekturen für den Test von Stellwerks-Schnittstellen, Eisenbahn Ingenieur Kalender, 2016
- [5] Hungar, H.; Asbach, L.; Meyer zu Hörste, M.: Ableitung von Testfällen für LST-Schnittstellen, EI – Der Eisenbahningenieur 1/2017
- [6] Schwencke, D.: Integrating a Signaling Component Model into a Railway Simulation, in: Riebisch, M.; Huhn, M.; Hungar, H.; Voss, S. (Hrsg.): Modellbasierte Entwicklung eingebetteter Systeme XIV (MBEES 2018), Seite 87-98

AUTOREN | AUTHORS

Dr. Mirko Caspar

Verifikations- und Validierungsmethoden /
Verification and Validation Methods
E-Mail: mirko.caspar@dlr.de

Dr. Daniel Schwencke

Verifikations- und Validierungsmethoden /
Verification and Validation Methods
E-Mail: daniel.schwencke@dlr.de

PD Dr. Hardi Hungar

Leiter der Gruppe Verifikations- und Validierungsmethoden /
Group Leader Verification and Validation Methods
E-Mail: hardi.hungar@dlr.de

Alle Autoren / *all authors:*

Deutsches Zentrum für Luft- und Raumfahrt e.V.,
Institut für Verkehrssystemtechnik

Anschrift / *Address:* Lilienthalplatz 7, D-38108 Braunschweig