Integration in einem Systemprojekt mit mehreren Schnittstellenpartnern

Integration into a system project with multiple interface partners

Carsten Sattler

In dem vorliegenden Beitrag werden Erfahrungen in einem Systemintegrationsprojekt, namentlich zur Schnittstelle SCI-CC, die zukünftige einheitliche Bedienschnittstelle im System Bahn bei der DB Netz AG, geschildert. Dabei wird auf die Rahmenbedingungen der Architektur und Aufgabenverteilung eingegangen. Die Erfahrungen werden an aktuellen normativen und verfahrensgestaltenden Dokumenten gespiegelt und erörtert. Schlussendlich wird ein Ausblick hinsichtlich der zukünftigen Vorgehensweise diskutiert, und es werden dazu Vorschläge unterbreitet.

1 Systemkontext

Das vorgestellte Systemintegrationsprojekt zur Schnittstelle SCI-CC (Standard Communication Interface (SCI) – Command and Control (CC)) ist in das Programm „Digitale Schiene Deutschland" der DB Netz AG eingebettet. Wesentliche Treiber für die Anforderungsgestaltung des Betreibers für die Schnittstelle SCI-CC sind:

- Einheitliche Gestaltung von Bedienoberflächen und Arbeitsabläufen für den Fahrdienstleiterarbeitsplatz
- Integration von für den Fahrdienst wesentlichen Informationen umgebender Teilsysteme in die Bedienoberfläche und Nutzung eines einzigen Bedien- und Anzeigemediums
- Ein einheitliches Sicherungsverfahren für Bedienung und Anzeige für den kompletten Bereich der DB Netz AG
- Flexibilität in der Zuordnung von Bedienung in und ggf. zwischen Instandhaltungsbereichen

Die Schnittstellenspezifikation inklusive zugeordneter Funktions- und Verfahrenslastenhefte wird hier synonym unter SCI-CC zusammengefasst.

Für die im Bereich der DB Netz AG zukünftig zur Anwendung kommenden Systemschnittstellen wurden jeweils Referenzprojekte zur Implementierung vereinbart, wo diese Schnittstellen erstmals im Wirkbetrieb gezeigt werden sollen.

Für die SCI-CC wird die Referenzimplementierung im Harz-Weser-Netz durchgeführt. Die Integrationsaufgabe besteht darin, die Teilsysteme, entsprechend der Architekturaufteilung, bezüglich Schnittstellen und übergeordneter Verfahren im Zusammenspiel zu testen und ggf. in Teilsystemen entstandene Regeln zu analysieren und anzuwenden.

Das globale Bild der Aufgabenstellung ist wie in Bild 1 dargestellt (bezogen auf die Situation in Göttingen). Die grobe Aufgabenstellung ist also die Integration der Teilsysteme

1. Bedienstandort (BSO)
2. LST Management Center (LMC)
3. integrierbare Unterzentrale (iUZ)

The experience from the SCI-CC interface system integration project, which is intended as the future unified command and control interface at Deutsche Bahn, is shared. As such, the general conditions that apply to the system architecture and task sharing are discussed. This experience is then discussed with reference to the standards and the process documents. Finally, an outlook is provided for the future integration and some suggestions are made.

1 The system context

The system integration project described here for the Standard Communication Interface Command and Control (SCI-CC) is part of the DB Netz "Digitale Schiene Deutschland" program. The most important requirement drivers within the SCI-CC are:

- the unified design of the user interfaces and the workflows for the operator workplace (OWP)
- the integration of the operationally relevant and connected subsystems into the same human-machine-interface (HMI)
- a unified safety procedure for the vital control and display of the whole DB Netz network
- flexibility in the assignment of the control centre relation within and between the maintenance control areas

The interface specifications, including the function and process requirement specifications, are referred to collectively as the SCI-CC.

All future system interfaces (SCI) used in the DB Netz network will be piloted in so-called reference projects, where they will be used in real operations for the first time.

The reference project for the SCI-CC has been implemented in the Harz-Weser network. The integration task involves testing the subsystems in accordance with the system architecture in order to ensure the interface conformity and the performance of the higher system procedures. The subsystems' application conditions have to be analysed and applied.

The overall picture is given in fig. 1 (in relation to the specific situation in Göttingen). The task description roughly involves the integration of the following subsystems:

1. the integrated control system location (ICS location)
2. the control-command and signalling system management centre (CCSMC)
3. the integrated sub-centre (ISC)

This initially merely specifies the architecture and does not reflect a view of the products. It will have to be further refined. However, the approximate allocation of operating tasks to ar-

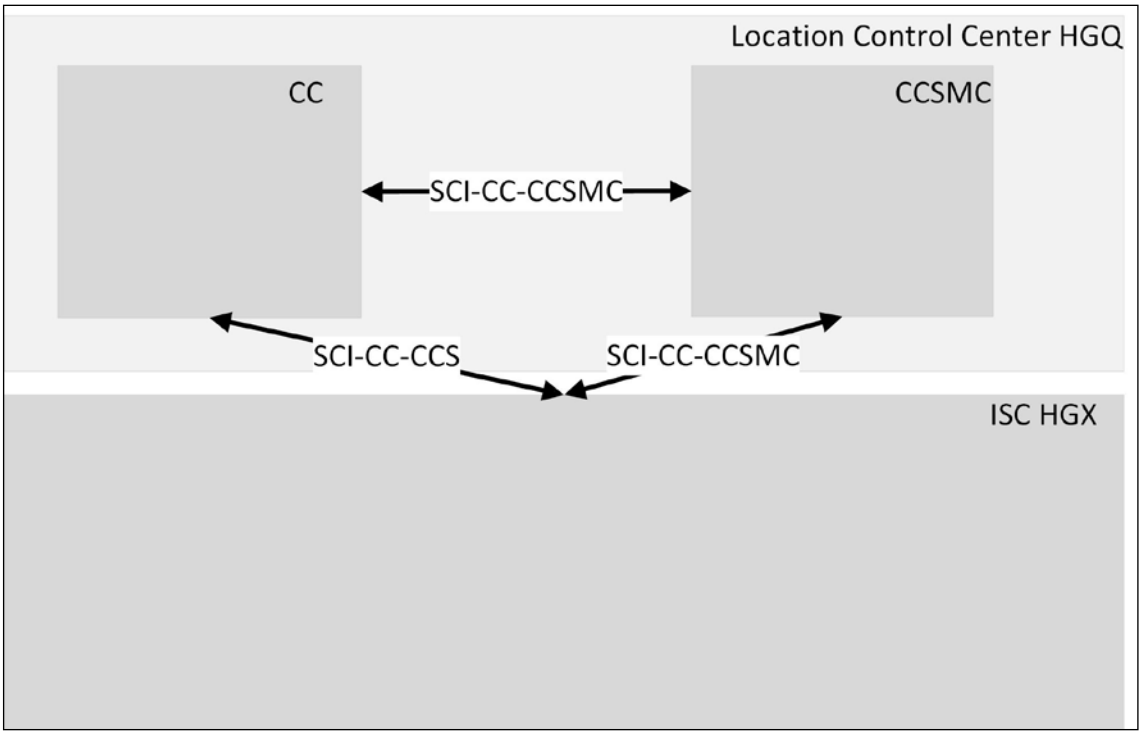

Bild 1: Grobe Architektur
Fig. 1: The high-level architecture

Dabei ist dies zunächst eine architektonische Vorgabe, die noch keine Produktsicht widerspiegelt. Dazu ist eine Verfeinerung notwendig. Man kann aber grob betriebliche Aufgabenstellungen den Architekturelementen zuordnen, und auch die Schnittstellenspezifikation nimmt an dieser Stelle eine grobe Segmentierung vor.
Das LMC realisiert hierbei die Bereitstellung zentraler Dienste für Authentifizierung und Autorisierung bezogen auf Örtlichkeiten, Pflege der Zuordnung von iUZ zu BSO und Bereitstellung eines zentralen Lagebildes hinsichtlich der Instandhaltung. Die Einbettung der zentralen Dienste hinsichtlich der Anlagenverantwortlichkeit muss dabei noch detailliert im Regelwerk erarbeitet werden.
Die BSO werden gemäß ihrer örtlichen Zuständigkeit über die genehmigten und abgenommenen Relationen zugeordnet. Der BSO selbst beherbergt die Bedienung und das zentrale Postamt für die Nachrichtenverteilung (fachlich Broker). Hinsichtlich der Kommunikationsinfrastruktur wurde hier ein Brokerdienst gewählt (wie bereits bei der Standard-Bedienschnittstelle vereinbart), der eine Publish & Subscribe-Architektur realisiert. Der Vorteil einer solchen Architektur ist, dass nicht einzeln Kommunikationsbeziehungen geplant und projektiert werden müssen, sondern ein zentrales Nachrichtenmedium existiert, in das beteiligte Systeme themenbezogen Nachrichten zur Verfügung stellen und abholen. Nachrichten, die von den Systemen für ihre Funktion benötigt werden, werden analog einem Postfach abonniert.
Die iUZ beinhaltet die Sicherungssysteme, Funktionen zur Zuglaufverfolgung und Automatisierung sowie iUZ-bezogene Dienste zur Verwaltung von Zuständigkeiten, Merktexten, Dokumentation und zur Bereitstellung von Projektierungsdaten.
Somit ist eine grobe Clusterung von Anforderungen möglich, und Aspekte der Teilsystemintegration sind in den genannten Teilsystemen selbst möglich, teilweise auch bis an die Schnittstelle, wo ggf. Simulatoren zum Einsatz kommen. Im nächsten Schritt ist die Verfeinerung zu betrachten, die größtenteils bereits durch die mit den Anforderungen des Auftraggebers (AG) übergebene Systemarchitektur festgelegt ist.

chitectural elements is possible and the interface specification can also be split roughly into functional segments.
The CCSMC provides the central services for authentication and authorisation with reference to the locations and the central maintenance of the ISC/ICS relationship and a central process image of the maintenance data from all the connected systems. Additions have to be made to the maintenance and operating regulations in order to embed these central services into the system of local responsibilities.
The ICS locations will be assigned on the basis of the approved and accepted relationships in accordance with their local responsibility. The location itself hosts the command and control and the central "post office" for message distribution (known as the broker). A broker server was chosen for the communication infrastructure (as was already the case for the current command and control interface), in which a Publish & Subscribe architecture is implemented. The advantage of this is that no detailed planning and configuration of the communication connections is needed. A central message service exists where the connected systems can provide and retrieve all the required messages, similar to a mailbox.
The ISC contains all the safeguard systems, the automatic train tracking and route setting functions, as well as all the ISC-related services for the administration of responsibility, interlocking-related memoranda, archiving and the supply of configuration data.
A rough clustering of requirements is therefore possible and aspects of subsystem integration can be performed in the aforementioned subsystems (to some extent also in the interface itself, where simulation tools can be used). Further refinement has to be considered in the next step, but this is mainly determined by the customer's system architecture requirements.
The customer then segmented the structure of the interface specification, which has advantages in terms of integration and certification. Fig. 2 provides a simplified view.

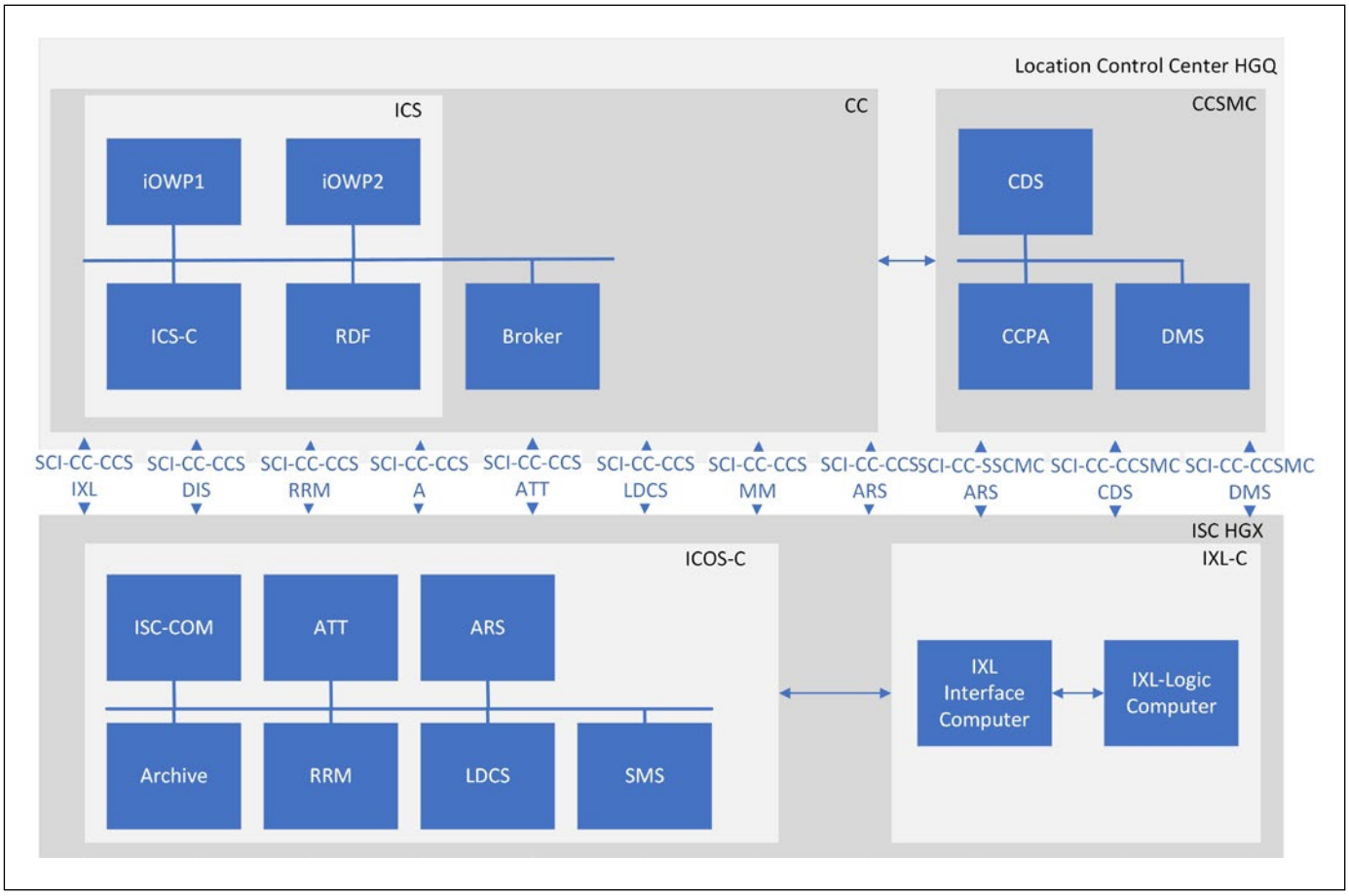

Bild 2: Schnittstellensicht
Fig. 2: An overview of the interface segments

Dabei erfolgte durch den Auftraggeber bereits eine Segmentierung der Schnittstelle, die im Hinblick auf Nachweisführung und für die Integration auch Vorteile bietet. In etwas vereinfachter Darstellung sieht die Schnittstellensicht nun wie in Bild 2 dargestellt aus.
Die einzelnen Schnittstellensegmente und zugeordneten Verfahren sind wie in Tab. 1 dargestellt.
Andere Teile der Schnittstelle sind nicht als dedizierte Telegrammschnittstelle entworfen, sondern durch Rahmenbedingungen in der Nutzung von Standardprotokollen umrissen. Dieses sind im Speziellen X11, Advanced Message Queue Protocol (AMQP) und Lightweight Directory Access Protocol (LDAP). Das betrifft hauptsächlich die Schnittstelle zwischen iBS und LMC, aber auch die Schnittstelle iUZ zu iBS und LMC.

2 Integrationsaufgaben

Grundsätzlich ist die Integration dadurch definiert, dass ein Zusammenspiel eines erstellten Systems in ein übergeordnetes System bzw. das Zusammenspiel mit einem Drittsystem getestet wird [1]. Es gibt aber auch Aufgaben zu lösen, die eisenbahnspezifischer Natur sind und die sich aus der Funktionsaufteilung ergeben. Damit verbundene Aufgaben sind normativ bzw. auch in nationalen Vorschriften, wie z. B. der Sektorleitlinie [4] geregelt. Wenn man vom System Bahn als Gesamtsystem spricht, so ergibt sich als Integrationsaufgabe das Zusammenspiel erstellter Teilsysteme eines oder mehrerer Hersteller mit dem letzten Schritt der Gesamtsystemintegration, die beim Betreiber liegt. Die

The various interface segments and the functions assigned to them are shown in tab. 1.
The other parts of the interface specification have not been designed as a specific datagram interface, but the general conditions for the use of commercial off-the-shelf protocols have been defined. These are specifically X11, the Advanced Message Queue Protocol (AMQP) and the Lightweight Directory Access Protocol (LDAP). This mainly affects the interface between the ICS and the CCSMC, but also the interfaces between the ISC and the ICS and the CCSMC.

2 Integration tasks

Integration is basically defined as testing the interaction of a supplied system within a higher-level system or its interaction with any third-party systems [1]. However, there are railway-specific tasks that result from the distribution of functions. The associated tasks are defined in the standards and the national regulations, such as the railway sector guidelines for safety assessment and certification [4]. If the railway system is considered to be the overall system, integration therefore involves the interaction of all the supplied subsystems with the last integration step, i.e. overall system integration, being the task of the network operator. EN 50126-1 states that Phase 8 integration must prove the fulfilment of the overall system requirements and all the defined RAMS requirements. The standard also adds that the integrated system is installed in a higher-level system and "*therefore, the requirements of this lifecycle phase will apply to both the integra-*

Schnittstellensegment	Verfahren
ESTW (elektronisches Stellwerk)	Geregelt wird das Verfahren in Melderichtung für die Übertragung der ausleuchtungsrelevanten Information in verschiedenen Informationsarten und Elementtypen sowie die Übertragung von betrieblich relevanten Meldungen (Fehler und Störungen). In Kommandorichtung werden die generischen Bedienungen für Fahrstraßen und Einzelelemente festgelegt.
AE (Anzeigesicherung und Eingabesicherung)	Definiert wird das Verfahren für die Übertragung von Information im Zuge von Prozeduren, bei denen temporär eine gesicherte Anzeige zur Bedienung bzw. Erfolgskontrolle erforderlich ist bzw. für Rückspiegelung und Erfolgskontrolle im Zuge der Kommandosicherung bei Hilfshandlungen. Zusätzlich ist das ESTW in diesem Prozess Prüfpartner im Rahmen von erforderlichen Hintergrundprüfungen im Rahmen der Ausfalloffenbarungszeit.
ZRV (Zuständigkeits- und Ressourcenverwaltung)	Hier werden die Verfahren zum Abgleich der iUZ bezogenen Zuständigkeiten geregelt sowie die Verfahren zur Offenbarung von Fehlerzuständen bezüglich der Zuständigkeiten.
DO (Dokumentationsverfahren)	Beschrieben sind hier die Verfahren zum Austausch von protokollierten Informationen in der Dokumentation der iUZ mit dem integrierten Bediensystem (iBS) sowie die Verfahren zum Eintragen protokollierungspflichtiger Informationen des iBS in Richtung der iUZ Dokumentation.
ZMA (Zugnummernmeldeanlage)	In diesem Segment sind die Verfahren zur Einwahl und Fortschaltung von Zugnummerninformationen sowie zum Austausch von ausleuchtungsrelevanter Zugnummerninformation erläutert.
PD (Projektierungsdaten)	Hierin findet man die Mechanismen zum Laden und zum Abgleichen der anlagenbezogenen Projektierungsdaten aus der iUZ.
MT (Merktextverwaltung)	An dieser Stelle wird das Verfahren zum Speichern und Abgleichen der iUZ bezogenen Merktexte definiert.
ZL (Zuglenkung)	Inhalt dieser Spezifikation ist die Schnittstelle zwischen der Zuglenkung (ZL) in der iUZ und iBS sowie Lenkplanversorgung (LPV).
ZVD (Schnittstelle für Bedienrelation)	Hierin wird die Schnittstelle zwischen zentralem Verzeichnisdienst (ZVD) und Stellwerk beschrieben, um Informationen zur Bedienrelationstabelle auszutauschen bzw. um die Bedienrelationstabelle in das ESTW zu laden.
DMS (Meldungen an das Diagnosesystem)	Diese Schnittstelle regelt Format und Inhalte zu sendender Information an eine Diagnosezentrale im LMC. Es ist eine reine Sendeschnittstelle der Quellsysteme.

Tab. 1: Schnittstellensegmente und grobe Beschreibung

EN 50126-1 sagt zum Thema Integration in Phase 8, dass die Einhaltung der Systemfunktionalität sowie der festgelegten RAMS-Anforderungen nachgewiesen werden muss. Des Weiteren sagt aber die Norm auch, dass das integrierte System in ein übergeordnetes System installiert wird und *„daher müssen die Anforderungen dieser Lebenszyklusphase sowohl auf die Integration der Komponenten und Subsysteme als auch die Einbindung eines Systems in ein übergeordnetes System angewendet werden."* [2]. Somit erstreckt sich die Phase Integration beginnend ab Subsystemintegration bis hin zur fachtechnischen Abnahme inklusive der Abstimmung zu Auflagen und Regelwerken. Die erwarteten Arbeitsergebnisse sind neben den Testaussagen die Fortschreibung von Lebenszyklusdokumenten (s. Kap. 7.9.3), aber insbesondere die Prüfung von Safety Related Application Conditions (SRAC) der integrierten Teilsysteme (s. Kap. 7.9.4) [2]. Für das Thema funktionale Sicherheit sind insbesondere bei Zuweisung von Basisintegrität an sicherheitsbezogene Funktionen die Hinweise des Kapitels 10.2.11 der EN 50126-2 [3] zu beachten. Hier lohnt nun ein Blick in die Sektorleitlinie [4], speziell Kapitel 2.1.10 sowie die Anlagen 4.1, 4.2. und 17. Anlagen 4.1 und 4.2 gehen auf das Thema technische und betriebliche Integration ein, und Anlage 17 widmet sich dem Thema herstellerübergreifende Integration. Eine der wesentlichen Aussagen, die aus der Integration in der Phase Pro-

Interface Segment	Function
IXL (electronic interlocking)	In the message direction, the definition of any messages (especially the display of relevant information) with different information and message types, as well as operationally relevant messages (such as errors and failures). In the command direction, generic commands to the ISC are defined for the single elements and the routes.
Vital procedure (display and input security – DIS)	The information transfer procedure is defined for all the functions that rely on a temporary vital display or where confirmation of success is needed. Additionally, the interlocking is a partner system for all the necessary background evaluation procedures during the failure disclosure time.
RRM (responsibility and resource management)	All the functions required for the information exchange about ISC-related responsibilities are described. The mechanisms for revealing any failure states in relation to the given responsibility are defined.
Logbook, archiving and reporting (A)	The logbook, archiving and reporting functions are defined and the information exchange between those functions and the corresponding functions in the ICS is described.
ATT (automatic train tracking)	This interface segment defines all the functions needed for entering and advancing train numbers and for the display of any relevant train number information.
Local CD (configuration data (LCDS))	The mechanisms for loading and adjusting the location-specific configuration data are explained.
MM (memoranda management)	The procedures for saving and adjusting the ISC-related memoranda are defined here.
ARS (automatic route setting)	This specification contains the interface between the ARS in the ISC and the ICS and the central control plan administration.
CDS (central directory service)	The information exchange between the CDS and the IXL for loading the operating relation table (ORT) is defined.
DMS (diagnostic management system)	This interface specification defines all the information relevant for diagnostics and the datagram format. It is a fire-only interface.

Tab. 1: The interface segments

tion of the components and subsystems and the incorporation of the system into the superior system."[2]. The integration phase therefore extends from the beginning of the subsystem integration through to the factory acceptance test, including the handling of the application conditions and the coordination of the rules. In addition to the test results, the expected results include the continuation of the lifecycle documents (see Chapter 7.9.3), especially the validation of any safety-related application conditions (see Chapter 7.9.4)[2]. As for functional safety, the remarks in Chapter 10.2.11 of EN 50126-2 [3] on the assignment of basic integrity to safety-related functions must also be considered. Here, it is worth taking a look at the sector-specific guidelines [4], in particular Chapter 2.1.10, as well as Appendices 4.1, 4.2 and 17. Appendices 4.1 and 4.2 provide guidance on technical and operational integration, while Appendix 17 deals with cross-manufacturer integration. The most crucial result to come from the integration phase involves the specific scenarios that can be implemented with the achieved conclusions. If the integrated techniques are to be used in any further projects that are not covered by the test results, the integration must be repeated.

3 The pilot project

Now, the specific aspects of the integration in the Göttingen reference project, which is the first project involving cross-man-

dukt herauskommt, ist, für welche konkreten Anwendungsszenarien in einem Anwendungsprojekt die Aussagen der Integration anwendbar sind. Für den Einsatz in weiteren Projekten, die nicht durch die Konfiguration abgedeckt sind, sind Integrationsschritte erneut durchzuführen.

3 Pilotprojekt

Im konkreten Fall werden Aspekte der Integration im Referenzprojekt Göttingen beschrieben, welches die Erstanwendung der herstellerübergreifenden Integration der Schnittstelle SCI-CC darstellt. Partner sind an dieser Stelle:

- Fa. Scheidt & Bachmann als Hersteller iBS, ZVD und Broker
- Fa. Thales als Hersteller LPV
- Fa. Siemens als Hersteller iUZ (mit iLBS-ZE und ESTW).

Vergleicht man die Situation mit der bauformübergreifenden Bedienung unter Verwendung der Standard-Bedienschnittstelle (SBS), so ist die Situation in Bild 3 im Vergleich zur Ausgangslage SCI-CC dargestellt.

Die Situation in der bauformübergreifenden Bedienung mit SBS kombinierte maximal zwei Hersteller, wobei die Ausgangslage derart war, dass beide Hersteller bereits eine Genehmigung von ESTW mit eigenem Leit- und Bediensystem vorzuweisen hatten. In der Konstellation mit SCI-CC treffen nun mehrere Teilsystemfunktionen verschiedener Hersteller aufeinander, die alle für den betrieblichen Ablauf zwingend erforderlich sind. Die konkrete Herstellerkombination mit den wesentlichen Teilfunktionen ist in der Aufzählung im Kapiteleingang erläutert.

ufacturer integration with the SCI-CC interface, will be described. The project partners are:

- Scheidt & Bachmann, the manufacturer of the ICS, the CDS and the broker
- Thales, the manufacturer of the central control plan administration
- Siemens, the manufacturer of the iCOS-C (with iCOS-C and IXL).

The following fig. 3 shows a comparison of the situation with cross-manufacturer command and control using a standard command and control interface (SBS).

Cross-manufacturer command and control with SBS combines a maximum of two vendors, where the prerequisite is that each vendor already has certification of its own interlocking combined with its own OCS. Different subsystem functions from different manufacturers that are all necessary for operations will now meet in the constellation with the SCI-CC. The specific vendor combinations were introduced at the beginning of the chapter.

Certification is currently only available for the essential element of the ICS and IXL ZSB2000. For the other manufacturers, i.e. the Thales CCPA and the Siemens ISC (especially the IXL Simis D with the SCI-CC), the Göttingen project is the first time that integration is being performed. A two-step-approach has been agreed with the customer for the integration procedure. In the first step, the integration will be performed between all the vendors resulting in the "ready for FAT" statement, which will be followed by the customer's factory acceptance.

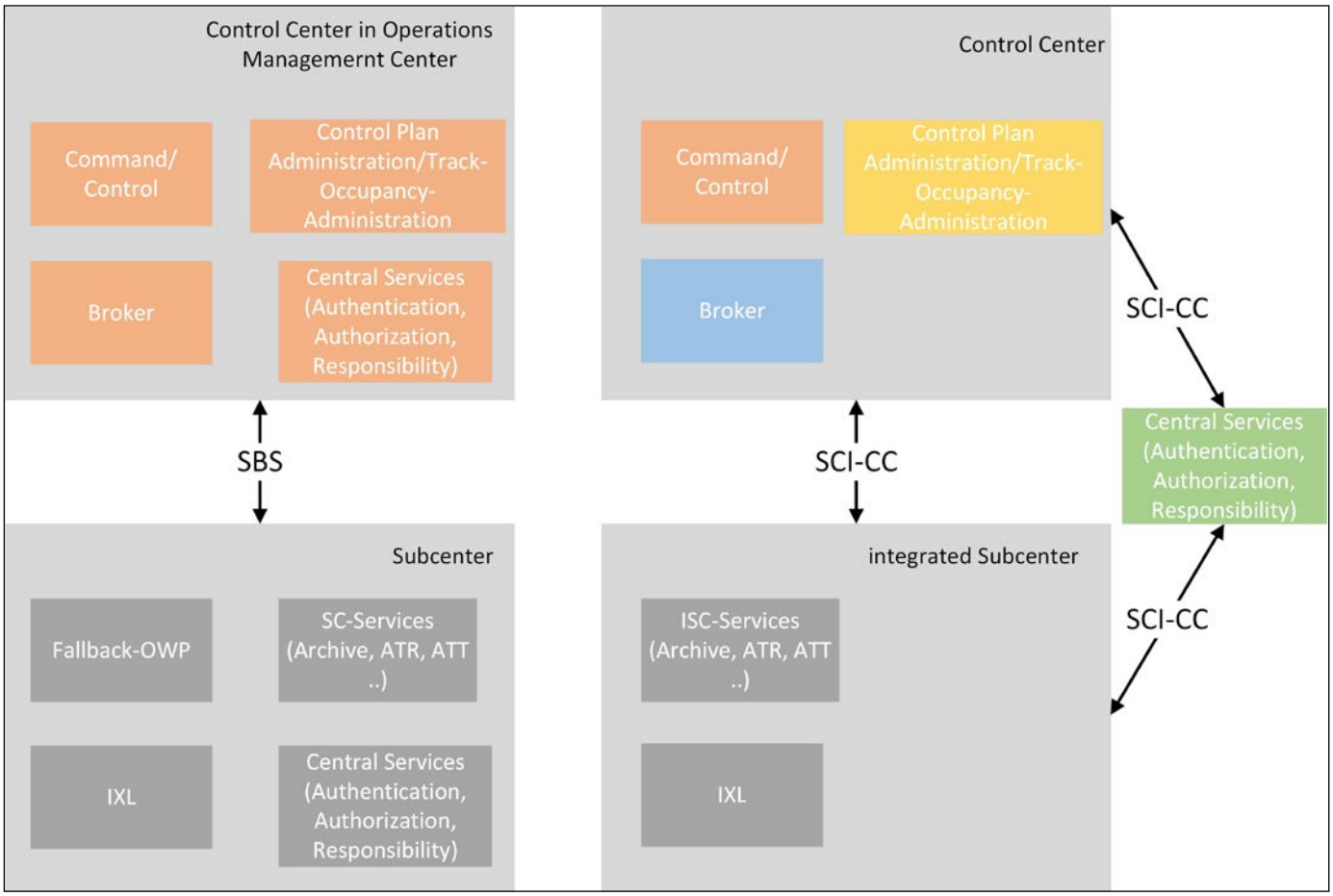

Bild 3: Vergleich Ausgangssituation SBS und SCI-CC
Fig. 3: A comparison of the SBS – SCI-CC situation

Als wesentlicher Baustein liegt aktuell nur für die Kombination iBS mit ESTW ZSB2000 des Herstellers Scheidt & Bachmann eine Genehmigung vor. Für die Hersteller Thales LPV und Siemens mit iUZ (insbesondere Stellwerk Simis D mit SCI-CC) erfolgt im Rahmen des Referenzprojektes die Erstintegration, wobei für die sichere Integration nur Aussagen für iBS, ZVD und ESTW benötigt werden. Hinsichtlich des Vorgehens zur Integration wurde mit dem Betreiber ein zweistufiges Integrationsvorgehen vereinbart. Zuerst erfolgt eine Integration zwischen den Herstellern verbunden mit der Aussage „fertig für fachtechnische Abnahme" und anschließend die fachtechnische Abnahme durch den Betreiber.

Zur Abbildung der konkreten Projektsituation wurde eine Integrations- und Testumgebung (ITU) inklusive der Kopplung der Herstellerlabore eingerichtet. Dabei befinden sich iBS, Broker und ZVD am Standort in Melsdorf bei Scheidt & Bachmann, die LPV am Standort Thales in Berlin und die iUZ mit iLBS-ZE und ESTW am Standort Siemens Mobility in Braunschweig. Die Laborkopplung erfolgt über Security-Komponenten der Fa. Scheidt & Bachmann, inklusive der erforderlichen Netzwerkkomponenten, die das Transfernetz als geroutetes Netz zur Broadcast-Trennung bilden. An das System iBS-Z sind in Melsdorf Bedienplätze für den Test vor Ort angeschlossen sowie abgesetzte Bedienplätze in den Herstellerlaboren und beim Auftraggeber in Berlin.

Für die Nutzung der zentralen Komponenten am Standort Melsdorf stellt die Fa. Scheidt & Bachmann einen Web-Server zur Verfügung, auf dem Abstimmungsunterlagen und insbesondere die Testanlagenbelegung hinterlegt sind. Für die Tests speziell zur Integration von ESTW, iLBS-ZE mit iBS (inkl. ZVD, Broker) wurde darüber hinaus ein eigenes Versionierungsrepository eingerichtet, welches im Wesentlichen folgende Themen beinhaltet:

- abgestimmte Testfälle
- Listen zur Fehlerverfolgung
- Versionsprotokollierung der aufgebrachten Softwarebausteine der Teilsysteme
- Liste offener Punkte.

Darüber hinaus verfügen die Hersteller über eigene Ablagen der eigenen Teilsystemtests, ggf. aber unter Nutzung der Teilsysteme anderer Hersteller bzw. unter Nutzung von Simulatoren. Zusätzlich wurde eine Ablage beim Betreiber insbesondere im Hinblick auf die bevorstehende fachtechnische Abnahme angelegt. Es wurde seitens der Hersteller die Möglichkeit genutzt, entwicklungsbegleitende Tests durch den Betreiber durchführen zu las-

An integration test environment that included the interconnection of the vendor test laboratories has been set up in order to emulate the real situation at the customer site. The ICS, the broker and the CDS are located at the Scheidt & Bachmann test centre in Melsdorf, the CCPA is at the Thales test centre in Berlin and the ISC (with the ICOS-C and the IXL) are at the Siemens Mobility test centre in Braunschweig. The interconnection has been achieved using security components from Scheidt & Bachmann (including all the network components that constitute the transfer network and the routing network for separating the broadcast domains). The ICS is located at the test centre in Melsdorf with local operator workplaces and remote workplaces at various other vendor and customer sites.

Scheidt & Bachmann provides a web server in Melsdorf that hosts the common documents and especially the test centre reservation file for the use of the central components.

A dedicated versioning repository has especially been created for the integration of the IXL and the ICOS-C with the ICS (including the CDS and the broker). It contains the following:

- the common test cases
- the error reporting lists
- the records of the installed software component versions
- the list of open issues.

Furthermore, all the vendors have their own test environments for subsystem integration and their own file stores for testing, in some cases using the systems of other vendors or simulators. Additionally, a file store has been created at the customer site, mainly to hold the reporting lists for the FAT.

All the vendors have taken the opportunity to use the tests performed by the customer during development. The results are also located at the file store mentioned above.

The confirmations of conformity with the vendor specifications have been finalised. Some application conditions have been drawn up to be included in the future operating rules as part of the operator involvement in the integration. The integration phase between the manufacturers will soon come to an end to be followed by the start of the factory acceptance test. Finally, the questionnaire contained in the appendices of the sector-specific guideline (4.1, 4.2, 17) [4]) must also be looked at. The application conditions from the integration of operations during the specification phase are largely addressed to the network operator. The questions from Appendix 4.1 are relevant

sen. Die Ergebnisse und gefundenen Auffälligkeiten liegen ebenfalls auf der genannten Ablage.
Die Konformitätsbestätigungen zu den Pflichtenheften liegen bei den Herstellern vor. Im Rahmen der Betreiberbeteiligung für die betriebliche Integration sind noch Auflagen für die noch zu erstellenden Regelwerke zu erfüllen. Die Integrationsphase der Hersteller nähert sich dem Ende, und der Zeitpunkt der fachtechnischen Prüfung durch den Betreiber rückt näher. Dabei sind insbesondere die Fragestellungen der genannten Anlagen der Sektorleitlinie (4.1, 4.2, 17) [4] für die Zulassungsbewertung zu berücksichtigen. Die Auflagen aus der betrieblichen Integration aus der Pflichtenheftphase gehen im Wesentlichen an den Betreiber, ggf. unter Zuarbeit der Hersteller. Für die Hersteller sind die Fragen der Anlage 4.1 relevant. In Bezug auf die beispielhaften Szenarien der Anlage 17 greift keines der genannten, wobei Kapitel 4.4 der Anlage 17 dem Thema am nächsten kommt. Für das Thema sichere Integration liegt die besondere Aufmerksamkeit auf dem Sicherungsverfahren Anzeigesicherung (AnSi) / Eingabesicherung (EiSi). Hier erfolgte durch den Betreiber eine Zuscheidung einer Total Functional Failure Rate (TFFR) im Bereich Basisintegrität für den Hersteller iBS und für den Hersteller ESTW im Bereich Safety Integrity Level (SIL) 4. Gemäß Kapitel 10.2.11 ergeben sich hier für den Hersteller des iBS Aufgaben für den Nachweis der Rückwirkungsfreiheit. Das Thema Angemessenheit der Zuteilung muss im Gesamtsystemsicherheitsnachweis verarbeitet werden, und es ergeben sich Aufgaben für den Zeitraum der Erprobung und des Betriebes, ggf. unter Auflagen für die Instandhaltung.

4 Abschließende Bemerkungen

Die Realisierung der Schnittstelle SCI-CC im Referenzprojekt Göttingen ist aufgrund einer umfangreichen Spezifikation und einer verteilten Architektur ein komplexes Unterfangen. Vorteile im Projekt bieten eine gewisse Modularität der Schnittstellenspezifikation insbesondere hinsichtlich des Themas sichere Integration. Ein weiterer organisatorischer Vorteil ist durch den kooperativen Ansatz im Projekt gegeben. Es zeichnet sich ab, dass auch für zukünftige Realisierungen aufgrund der Fortschreibung der Schnittstelle sowie der Hinzunahme weiterer beteiligter Hersteller komplexe Aufgabenstellungen bestehen bleiben, wo sich im Nachgang der betrieblichen Erprobung auch noch ein Lessons Learned anbieten würde. Für das konkrete Projekt befinden sich alle Beteiligten auf der Zielgeraden, wobei noch einige Arbeit speziell hinsichtlich formaler Nachweise zu leisten ist. In technischer Sicht ist durch die aktuell durchgeführten Tests nachgewiesen, dass die spezifizierte Schnittstelle funktioniert. Die Ergebnisse der betrieblichen Erprobung sind abzuwarten. Darüber wird nach Abschluss der Betriebserprobung berichtet. Des Weiteren wird zu einem späteren Zeitpunkt der Zielzustand hinsichtlich LMC-Anbindung realisiert. ■

for the manufacturer. As for the example scenarios outlined in Appendix 17, none of them really matches the described situation exactly, but scenario 4.4 comes the closest. Special attention has been given to safe integration and, in particular, to the vital procedures for display security and input security. The network operator has assigned total functional failure rates (TFFR) at the basic integrity level for the ICS manufacturer and at the Safety Integrity level (SIL) 4 for the IXL manufacturer. In accordance with Chapter 10.2.11 of EN 50126-2, specific tasks are derived for basic integrity, including the proof of non-intrusiveness. The overall system safety case should address whether the assignment of the safety integrity levels was appropriate and the operation phase includes measures to prove the effectiveness of the basic integrity functions.

4 Concluding remarks

The implementation of the SCI-CC interface in the Göttingen reference project is a complex undertaking due to the extensive requirement specifications and the distributed system architecture. A degree of modularity in the interface specification provides some advantages for project progress, especially during safe integration. A further advantageous aspect in project organisation involves the adopted cooperative approach. It looks very much as though the project's complexity will also persist in future implementations due to the additions to the requirement specifications and the involvement of other manufacturers. For this reason, a lessons-learned workshop is suggested after the operations test phase. All the participants in the Göttingen project are on the home stretch, but there is still work to be done on the formal proofs and documents. In technical matters, the tests processed so far have shown that the specified SCI-CC interface works. Finally, the results from the operations test phase remain to be seen. They will be included in a further report. The target configuration with respect to the connection to the CCMC will implemented at a later date. ■

LITERATUR | LITERATURE

[1] Fieber, F.; Wendland, M.-F.: Basiswissen Abnahmetest, dpunkt.verlag, 2021
[2] DIN EN 50126-1, Teil 1 Generischer RAMS-Prozess, 2018-10
[3] DIN EN 50126-2, Teil 2 Systembezogene Sicherheitsmethodik, 2018-10
[4] Sektorleitlinie für die Zulassungsbewertung von Signal-, Telekommunikations- und Elektrotechnischen Anlagen (Technische Vorschrift) inkl. Anlagen, Ausgabe 1.0 vom 07.07.2021
[5] Bleicher, I.; Grimm, L.; Wiedenroth, A.: Das Projekt DiB gestaltet das Bediensystem der Zukunft, SIGNAL+DRAHT, 11/2020

AUTOR | AUTHOR

Dipl.-Phys. Carsten Sattler
Systemmanager, Bereich Bahnautomatisierung /
System Manager, Railway Automation Division
Siemens Mobility GmbH
Anschrift / *Address*: Ackerstraße 22, D-38126 Braunschweig
E-Mail: carsten.sattler@siemens.com