Referenzbericht

Visualisierungs- und Bediensystem für Bahnen nach SIL2 mit Typenzulassung vom BAV

Visualisierungs- und Bediensystem für Bahnen nach SIL2 mit Typenzulassung vom Bundesamt für Verkehr (BAV)

Das **V**isualisierungs- und **B**ediensystem für **Ba**hnen (VBBa) wird zum Bedienen und Visualisieren von Stellwerken und allen dazugehörigen Elementen der Sicherungsanlage wie Weichen, Barrieren, Fahrstraßen etc. bei verschiedenen Eisenbahnunternehmungen eingesetzt.

Die Aufgabe von VBBa ist die Fernsteuerung und Fernüberwachung von Stellwerken. Teilweise erfolgt die Fernsteuerung heute noch mittels konventionellen Bedienpulten. Diese werden durch VBBa abgelöst.

VBBa ist für das Ausführen von kritischen Befehlen ausgelegt. Das Bedien- und Beobachtungssystem ist gemäß den Anforderungen nach SIL2 ausgelegt, somit werden die notwendigen Sicherheitsanforderungen erfüllt. Die Sicherheit wurde in umfangreichen Tests nachgewiesen, von externen Gutachtern geprüft und vom BAV (Bundesamt für Verkehr der Schweiz) im November 2014 zertifiziert.

Mit dem vorliegenden Projekt hat LeitTec AG ein typengeprüftes, generisches System für die sichere Anzeige von Meldungen und die sichere Ausführung von Befehlen (fehlersicher) realisiert. In der Auslegung und der Größe ist das System flexibel an die Bedürfnisse der jeweiligen Bahn anpassbar. Das System ist modular aufgebaut und hat offene Schnittstellen zu anderen Leitsystemen (Zuglenkung) oder weiteren Stellwerkstypen. Zukünftige weitere Schnittstellenmodule können rückwirkungsfrei zum Grundsystem hinzugefügt werden.

Endkunde

CHEMINS DE FER DU JURA

Privatbahn mit einem Schienennetz von 85 km, 19 Bahnhöfen und 1.5 Mio Passagieren pro Jahr, welche für den öffentlichen Verkehr eines großen Teils des Schweizer Juras zuständig ist.

Systemintegrator

LeitTec AG - Prozessautomation und Bahnsicherungstechnik

LeitTec AG ist seit 2001 WinCC OA Premium Solution Partner und hat ihren Hauptsitz in Bern in der Schweiz

SIEMENS

Referenzbericht

Visualisierungs- und Bediensystem für Bahnen nach SIL2 mit Typenzulassung vom BAV

Geschäftsführer: Jörg Boltshauser
Projektleiter, Leiter Entwicklung VBBa: Peter Tschan
Applikationsentwicklung WinCC OA: Kony Meyer

Bei dem Projekt waren seitens des Systemintegrators LeitTec AG ein Projektleiter und drei weitere Mitarbeiter für Steuerung und Visualisierung (WinCC OA) beteiligt. Ein externer Gutachter, sowie ein externer Berater für Designfragen wurden zusätzlich hinzugezogen.

Realisierungszeitraum

Das Projekt startete im Juni 2012 mit der Eingabe des Gesuchs ans BAV zur Erlangung einer Typenzulassung.
VBBa ist seit Mai 2014 bei Chemins de fer du Jura (CJ) erfolgreich in Betrieb, im November 2014 erfolgte die Typenzulassung durch das BAV.

Die Erstellung der Dokumentation durch LeitTec AG und die Überprüfung der Dokumentation auf Seite der Behörde war aufwändiger als ursprünglich angenommen, deswegen kam es zu einer 6-monatigen Verzögerung des Projektes.

Projektbeschreibung

VBBa besteht im Wesentlichen aus zwei Teilsystemen – der Leitebene und den Kopfstationen.
Die Leitebene ist das eigentliche Herzstück von VBBa und beinhaltet das übergeordnete Bedien-, Visualisierungs- und Datenerfassungssystem. Hier werden das SCADA-System SIMATIC WinCC Open Architecture (WinCC OA) und Siemens SCALANCE Switches eingesetzt.

Wie bei der Topologie ersichtlich, besteht die Leitebene aus:

- Ein redundantes Serverpaar, wobei die beiden Server im Hot-Standby-Betrieb laufen und sich gegenseitig überwachen. Dabei sind der aktive Server "Master" und der Standby-Server "Slave". Bei einer Störung des Master-Servers übernimmt automatisch der Standby-Server die Funktion des Masters.
- Eine oder mehrere Bedienstationen (Clients) bestehend aus Workstation, Maus, Tastatur und mind. 2 Bildschirme. Aufgrund der Client-Server-Architektur übernehmen die Bedienstationen alle Daten von den Servern.
- Netzwerk Leitebene: Dieses Netzwerk verbindet die Server untereinander und mit den Bedienstationen
- Netzwerk Steuerung: Dieses Netzwerk verbindet die Server mit den unterlagerten Steuerungen, den Kopfstationen.

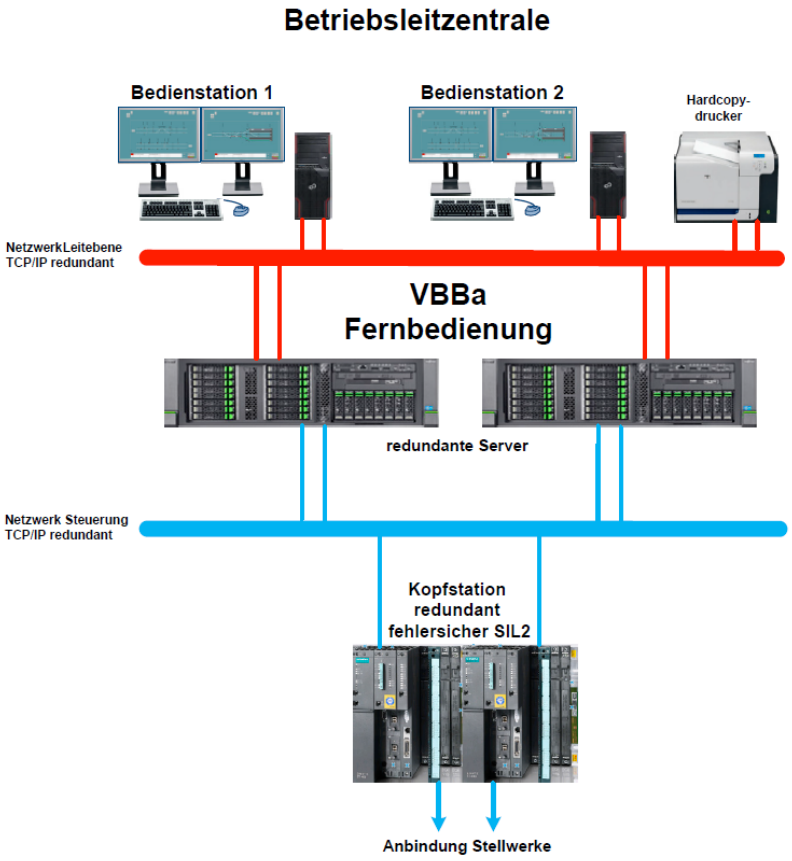
Die Kopfstation hat die Aufgabe Stellwerkinformationen vom Fernwirksystem zu übernehmen und an die Leitebene weiter zu geben.

Referenzbericht

Visualisierungs- und Bediensystem für Bahnen nach SIL2 mit Typenzulassung vom BAV

In der Gegenrichtung werden Befehle von der Leitebene übernommen und via Fernwirksystem ans Stellwerk gesendet.
Im Weiteren übernimmt die Steuerung verschiedene Prüfaufgaben, um die Konsistenz und Sicherheit der Datenübertragung zu gewährleisten.

Für die Kopfstationen werden SIMATIC Steuerungen S7-41xHF eingesetzt. Diese bilden die Schnittstelle zu den Fernwirksystemen. Der Name kommt daher, weil sie gleichzeitig auch die Funktion der Kopfstation des Fernübertragungssystems FWS-S7 (Produkt der LeitTec AG, ebenfalls im Besitz einer Typenzulassung) übernehmen (gemeinsame Hardware und Betriebssystemsoftware). Die Systemgrenze verläuft innerhalb der Kopfstation.



Topologie Leitebene

Referenzbericht

Visualisierungs- und Bediensystem für Bahnen nach SIL2 mit Typenzulassung vom BAV

Projektablauf

Der Projektablauf wurde maßgeblich durch die Vorgaben des BAV und die Bahnnormen (vor allem EN50129) vorgegeben.
Es wurde von Beginn an ein Gutachter beauftragt, der das Projekt während der gesamten Laufzeit begleitete.

Um eine Typenzulassung zu erlangen, ist ein Sicherheitsnachweis zu erbringen, welcher gemäß den folgenden Vorschriften und Normen zu erstellen ist:

- AB-EBV: 2012 Ausführungsbestimmungen zur Eisenbahnverordnung AB38.1 Ziffer 1.0 - 1.4 und AB39.2 Ziffer 4.3
- SN EN 50126:1999 Bahnanwendungen - Spezifikation und Nachweis der Zuverlässigkeit, Verfügbarkeit, Instandhaltbarkeit, Sicherheit
- SN EN 50128:2011 Bahnanwendungen - Software für Eisenbahnsteuerungs- und Überwachungssystem – Dies ist eine Unternorm der IEC 61508
- SN EN 50129:2003 Bahnanwendungen - Sicherheitsrelevante elektrotechnische Systeme für Signaltechnik
- SN EN 50159: 2010 Bahnanwendungen - Sicherheitsrelevante Kommunikation in offenen Übertragungssystemen
- EN 61000-6-2:2005 EMV Störfestigkeit Industriebereich
- EN 61000-6-4:2007 EMV Störaussendung Industriebereich
- Leitfaden für die Implementierung von sicherheitskritischen Projekten (Safety Manual von ETM)

Der Aufbau der Sicherheitsnachweisdokumentation richtet sich nach der Norm EN50129. Der Sicherheitsnachweis muss folgende Dokumente beinhalten:

Teil 1: Definition des Systems

Teil 2: Qualitätsmanagementbericht

Teil 3: Sicherheitsmanagementbericht

Teil 4: Technischer Sicherheitsbericht

Teil 5: Beziehungen zu anderen Sicherheitsnachweisen

Teil 6: Zusammenfassung

Eigentlicher Projektbeginn war die **Einreichung des Gesuchs beim BAV für die Typenzulassung** von VBBa. Das Gesuch beinhaltete ein Pflichtenheft als Arbeitsgrundlage für erste Besprechungen mit dem BAV und die weitere Entwicklung des Systems, sowie einen ersten Entwurf der Grunddokumentation für eine Typenzulassung.

SIEMENS

Referenzbericht

Visualisierungs- und Bediensystem für Bahnen nach SIL2 mit Typenzulassung vom BAV

Nach Bewilligung durch das BAV wurde mit der Spezifikation der Anforderungen und der Gefährdungsanalyse begonnen. Die **Systemanforderungsspezifikation** beschreibt alle Schnittstellen von VBBa, die detaillierte Topologie, sowie alle Anforderungen, die VBBa erfüllen muss. Dieses Dokument stellt die Basis für alle weiteren Dokumente und Entwicklungen dar. Die **Gefährdungsanalyse** dient der Identifikation von Gefahren, die mit dem System verbunden sind und der Ereignisse, die diese Gefahren auslösen. In der Gefährdungsanalyse wird das mit den Gefahren verbundene Risiko bestimmt und ein Prozess für ein kontinuierliches Risikomanagement erstellt. Die Gefährdungsanalyse bedingt Fachwissen im Prozess, womit verschiedene Gefährdungsfälle und daraus resultierende (Gefahren-)situationen, aufgezeigt werden können.

Inhalt der Gefährdungsanalyse war die Bestimmung des Sicherheitsintegritätslevels (SIL-Level) für jede erfasste Gefährdung. Aus dieser Gefährdungsanalyse ergab sich, dass VBBa als Gesamtsystem für kritische Befehle (Befehle, welche das Umgehen von Sicherheitseinrichtungen im Stellwerk ermöglichen) SIL2 erreichen muss. Dasselbe gilt auch für die Anzeige der Stellwerkrückmeldungen.

Resultierend aus der Gefährdungsanalyse wurde die Grunddokumentation (bestehend aus Systemdefinition, dem Qualitätsmanagement-, Sicherheitsmanagement- und technischen Sicherheitsbericht, sowie dem Bericht über die Beziehungen zu anderen Sicherheitsnachweisen) überarbeitet.

Der Zweck des **Qualitätsmanagementberichts** ist es, die Häufigkeit menschlichen Versagens in jeder Stufe des Lebenszyklus zu minimieren und damit das Risiko von systematischen Fehlern in dem System, Teilsystem oder der Einrichtung zu reduzieren. Das Dokument beschreibt die Organisationsstruktur zur Entwicklung von VBBa, das Qualitätsmanagement von LeitTec AG bei der Entwicklung von VBBa, die Organisation der Verifikationen und Reviews, sowie die benötigte Dokumentation für den gesamten Lebenszyklus von VBBa.

Die Aufgabe des **Sicherheitsmanagementberichts** besteht darin, die Sicherheit durch einen wirkungsvollen Sicherheitsmanagementprozess, der mit dem Managementprozess für Verlässlichkeit für RAMS aus der EN 50126 übereinstimmen muss, zu gewährleisten.

Inhalte des Dokuments:

- Beschreibung aller Prozesse und Dokumente, die während den verschiedenen Phasen des Lebenszyklus von VBBa benötigt werden (Systementwicklung und Validierung, Projektierung und Inbetriebnahme, Betrieb und Unterhalt, Entsorgung)
- Beschreibung der Sicherheitsorganisation (abhängig vom SIL-Level)
- Beschreibung des Sicherheitsplans (Wann wird was gemacht, wann wird reviewt, was haben die Reviews für Auswirkungen)

Referenzbericht

Visualisierungs- und Bediensystem für Bahnen nach SIL2 mit Typenzulassung vom BAV

- Beschreibung der benötigten Dokumentation für den gesamten Lebenszyklus von VBBa

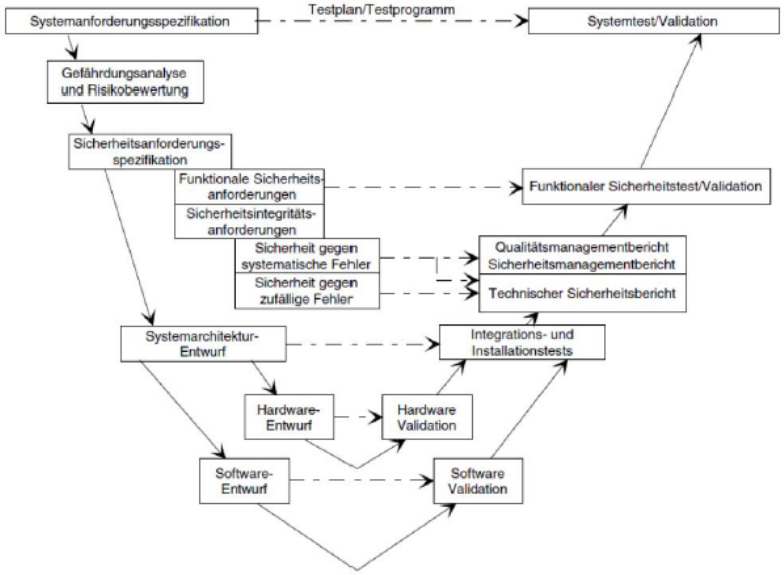


Abbildung aus der Norm EN50129 – Beispiel der Entwurfs- und Validationsteile eines Systemlebenszyklus

Der **technische Sicherheitsbericht** hat die Aufgabe den Nachweis der funktionalen und technischen Sicherheit von VBBa zu erbringen.
Er beinhaltet:

- den Nachweis zur Erfüllung der Anforderungen aus der Norm EN50128
- den Nachweis zur Erfüllung der einzelnen Anforderungen aus der Anforderungsspezifikation
- den Nachweis zur Erfüllung der Anforderungen laut Rahmen- und Betriebsbedingungen des Safety Manuals von WinCC OA
- den Nachweis zur Erfüllung der Anforderungen der Normen EN50128 und EN50159

Das Dokument für die **Beziehungen zu anderen Sicherheitsnachweisen** beinhaltet die Auflistung aller Nachweise, die für den Sicherheitsnachweis von VBBa zugezogen wurden (z.B. SIL Zertifikat WinCC OA, SIL-Zertifikat SIMATIC S71xx F).

SIEMENS

Referenzbericht

Visualisierungs- und Bediensystem für Bahnen nach SIL2 mit Typenzulassung vom BAV

Im nächsten Schritt wurde die **Systemspezifikation** für die Hard- und Software erstellt. Dies beinhaltete

- die Beschreibung der Topologie,
- die Beschreibung aller Hardware- und Software- Komponenten,
- die Beschreibung der einzelnen Funktionen in VBBa
- die Zuordnung der einzelnen Anforderungen auf die einzelnen Funktionen in VBBa.

Anhand dieser Spezifikation wurde die Leitebene installiert, die dann entsprechend dokumentiert und validiert wurde. Anschließend wurden die Grundfunktionalitäten der Leitebene spezifiziert und validiert. Ein essentieller Punkt bei diesem Projekt war die Sicherstellung der korrekten Übertragung der Meldungen und Befehle. Dafür wurden spezielle Funktionsbausteine und Objekte für die Kommunikation entwickelt. Diese Kommunikation wird mit einem Watchdog überwacht.

Für das Erstprojekt bei CJ (Stellwerk Tavannes), wurden weitere projektspezifische Funktionen und Objekte (z.B. Signal, Block, Weiche, Gleis und Fahrstraße) implementiert.

Danach starteten die grundlegenden Integrations- und Installationstests.
Nach erfolgreichem Abschluss der Tests wurde die erste VBBa Applikation – das Stellwerk Tavannes – detailliert spezifiziert. Dazu wurden ein Pflichtenheft, die Steuerung, die Leitebene, sowie eine Simulatorapplikation für das Stellwerk Tavannes erstellt. Im nächsten Schritt wurde ein funktionaler Sicherheitstest durchgeführt, um die bisherigen Funktionen zu validieren.

Zusätzlich wurde ein Gutachten von einem unabhängigen Gutachter zu Handen des BAV erstellt. Dieses dient der Begutachtung des Sicherheitsnachweises von VBBa und beinhaltet eine Bewertung des Sicherheitsnachweises aus Sicht des unabhängigen Gutachters (Erfüllung aller Normen, die Einhaltung des Vorgehens, Vollständigkeit des Nachweises etc.), einen Bericht über die Begutachtung, eine Auflistung der Mängel und Empfehlungen, sowie eine Empfehlung für die Typenzulassung.

Mit dem Erreichen dieses Meilensteines konnte ein erstes Sicherheitsgutachten vom externen Gutachter erstellt werden.

Danach galt es die Grunddokumentation weiter auszubauen. Es wurden Projekthandbücher, eine Bedienungsanleitung sowie diverse Schulungsunterlagen für den Bediener, den Systemverantwortlichen für VBBa, für den elektrischen Unterhalt und für das Vorgehen bei der Entsorgung erstellt.
Weiter war es notwendig, Spezifikationen für das Vorgehen bei Anlagenerweiterungen, für die Entwicklung und Anwendung von zusätzlichen

SIEMENS

Referenzbericht

Visualisierungs- und Bediensystem für Bahnen nach SIL2 mit Typenzulassung vom BAV

Funktionsbausteinen und für periodische Unterhalts- und Wartungsarbeiten, sowie ein Logistikkonzept zu erstellen.

Parallel zum Erstellen der Dokumentation wurde die Standardapplikation von VBBa entwickelt und das erste Projekt bei CJ, das Stellwerk Tavannes, realisiert. Die Leitebene, der Steuerungsteil und der VBBa-Simulator wurden geliefert und installiert. Nach der Einschulung des Personals bei CJ war VBBa bereit zur Inbetriebnahme. Um Tavannes in Betrieb nehmen zu können, benötigte LeitTec AG allerdings die Bewilligung zur Betriebserprobung vom BAV. Um diese Bewilligung zu erhalten, musste im Vorfeld der gesamte Sicherheitsnachweis erbracht und begutachtet werden.
LeitTec AG erstellte ein Konzept für die Betriebserprobung des Stellwerks Tavannes, welches durch den externen Gutachter begutachtet wurde. Nach einer Prüfung durch das BAV wurde schließlich im April 2014 die Freigabe zur Betriebserprobung erteilt. Die Begutachtung durch das BAV dauerte etwas länger als geplant, da es für alle Beteiligten das erste Mal war, dass ein so komplexes System wie VBBa gemäß den neuen Normen zugelassen wurde. Anschließend stellte der Bahnbetreiber ein Gesuch für eine Änderung seiner Sicherungsanlage (PGV). Nach der Bewilligung durch das BAV stand einer Inbetriebnahme von VBBa mit der Steuerung des Stellwerks Tavannes nichts mehr im Wege.
Nach einer zweimonatigen Betriebserprobung wurde diese ausgewertet und durch das BAV geprüft.

Damit waren alle Auflagen für eine Typenzulassung für VBBa erfüllt und die Erteilung der Typenzulassung wurde im November 2014 offiziell durch das BAV erteilt.

SIEMENS

Referenzbericht

Visualisierungs- und Bediensystem für Bahnen nach SIL2 mit Typenzulassung vom BAV

Technische Daten

Pro Stellwerk werden ca. 350 Objekte mit insgesamt 1.200 Variablen verarbeitet (ca. 300 Schnittstellensignale mit dem Stellwerk). Maximal werden 50 Stellwerke angebunden.

Eingesetzte Standard Sicherheitskomponenten:

- SIMATIC S741x HF (bis SIL 3)
- SIMATIC WinCC Open Architecture (bis SIL 3)
- KERBEROS
- VPN mit IPSEC Protokoll für Fernzugriff
- CRC (TCP/IP)

Vorteile / Nutzen

Die SIL 3 Zertifizierung von WinCC OA, mit den dazugehörigen Dokumenten, hat maßgeblich dazu beigetragen, dass VBBa auf diese Art und Weise realisiert werden konnte. Ohne das SIL-Zertifikat wäre der Aufwand mindestens doppelt so hoch gewesen, da wesentliche Sicherheitsaspekte zusätzlich durch LeitTec AG nachgewiesen hätten werden müssen.

Die Skalierbarkeit sowie das Redundanzkonzept von WinCC OA waren zusammen mit der hohen Verfügbarkeit von WinCC OA für die Realisierung von erheblichem Nutzen. Die langjährige WinCC OA Partnerschaft von LeitTec AG war bei dieser Aufgabenstellung extrem von Vorteil, da bereits viele Erfahrungen mit WinCC OA gesammelt werden konnten und viele Funktionalitäten von WinCC OA bereits bekannt waren.

Mit ETM stand ein Partner zur Verfügung der im Bedarfsfall einen sehr guten Support bieten konnte, bei Problemen jeweils schnell reagierte und bereit war, mittels Workshops spezifische Fragestellungen zu den SIL3-Konzepten und zur Realisierung zu diskutieren.

Der Endkunde CJ ist überaus zufrieden mit dem System VBBa. Seit der Inbetriebnahme, Anfang Mai 2014, läuft das System zuverlässig. CJ war während der Projektlaufzeit sehr zufrieden mit der Flexibilität und der unkomplizierten Abwicklung durch LeitTec AG.

Mit "Regionalverkehr Bern – Solothurn" (RBS) konnte bereits eine weitere namhafte Bahn überzeugt werden, die Fernsteuerung für das gesamte Bahnnetz mittels VBBa zu realisieren.

SIEMENS

Referenzbericht

Visualisierungs- und Bediensystem für Bahnen nach SIL2 mit Typenzulassung vom BAV

Anlagenbilder

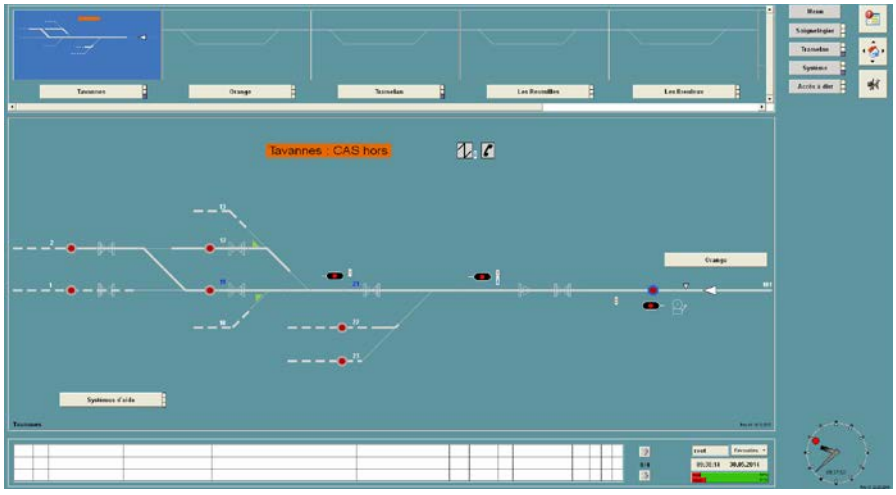
siemens.de/wincc-open-architecture

SIEMENS

Referenzbericht

Visualisierungs- und Bediensystem für Bahnen nach SIL2 mit Typenzulassung vom BAV

Bildschirmdarstellungen



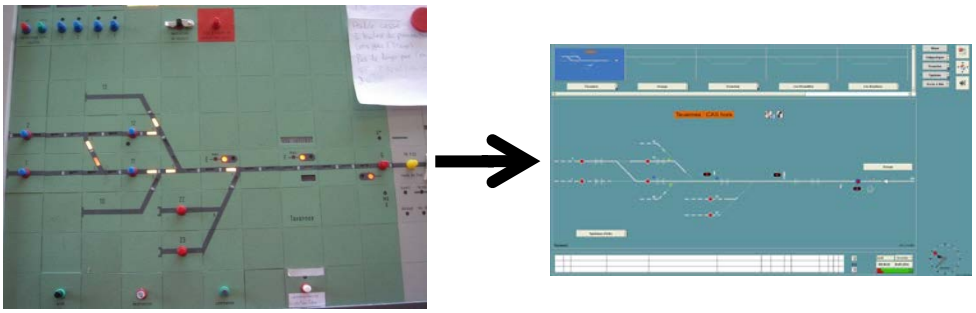
siemens.de/wincc-open-architecture

SIEMENS

Referenzbericht

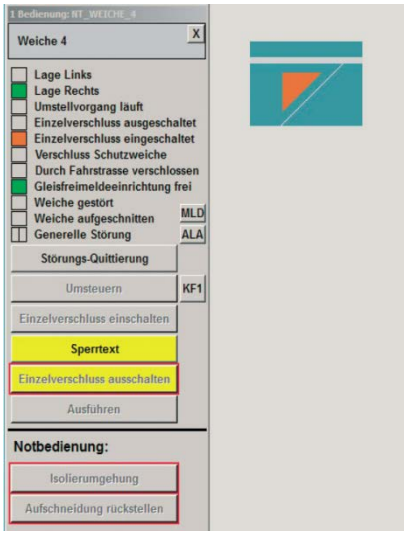
Visualisierungs- und Bediensystem für Bahnen nach SIL2 mit Typenzulassung vom BAV

Vom Pult zum Lupenbild:



Bedienung:

Weiche:



Streckenblock