Georedundanz im Bahnsystem – Herausforderungen, Lösungen und mögliches Zielbild

Geo-redundancy in the rail system – challenges, solutions and a possible target picture

Dirk Schmidt | Patrick Marsch | Oliver Knapp

Eine funktionierende Bahninfrastruktur ist wichtig für Wirtschaft und Gesellschaft. Mit Blick auf zunehmende Gefährdungslagen wie Extremwetter oder vorsätzliche Zerstörung ist es darum essenziell, die Bahn hochgradig resilient zu gestalten. Hierzu gehört auch die Umsetzung angemessener Georedundanz für Leit- und Sicherungstechnik (LST), d. h. die Fähigkeit, bei Ausfall eines Systems an einem anderen Ort dessen Funktionen übernehmen zu können. In diesem Beitrag stellen wir kurz- und mittelfristige Lösungen und das InfraGO Zielbild zur LST-Georedundanz vor sowie Voraussetzungen und Handlungsbedarf im Sektor.

1 Motivation und Einführung

Die DB InfraGO und andere europäische Bahnen sind dabei, die LST zu digitalisieren. Die eigentliche Stellwerks- und Sicherungslogik wird dabei in Rechenzentren bzw. sogenannten Digitalen Technikzentralen (DTZ) zentralisiert und vom angesteuerten Gleisfeld räumlich getrennt. Diese Zentralisierung bietet viele Vorteile, wie z. B. Skalierungseffekte oder eine günstigere Betriebsführung, aber sie erhöht auch die Vulnerabilität des Bahnsystems, da der Ausfall einer DTZ, z. B. bei einer Naturkatastrophe oder bei vorsätzlicher Zerstörung, großflächige Konsequenzen hat.
Es ist daher essenziell, dass mit der Einführung der neuen digitalisierten Bahninfrastruktur auch gleich Georedundanz in der LST eingeführt wird, d. h. die Fähigkeit des Systems, dass bei Ausfall einer DTZ eine andere deren Funktionen übernehmen kann. Dies ist nicht nur geboten, um bei steigenden klimatischen und geopolitischen Risiken eine hohe Gesamtverfügbarkeit des Bahnbetriebes zu gewährleisten, sondern wird auch vom BSI (Bundesamt für Sicherheit in der Informationstechnik) im KRITIS (Kritische Infrastrukturen)-Kontext gefordert [1, 2, 3].
In diesem Beitrag möchten wir zunächst auf grundsätzliche Georedundanz-Optionen für die LST eingehen, auf den Vorteil von Virtualisierung in diesem Kontext sowie auf die Voraussetzungen, die geschaffen werden müssen, um Georedundanz zu ermöglichen. Zuletzt bieten wir eine Perspektive auf ein mögliches Georedundanz-Zielbild, welches allerdings noch Standardisierungs- und Entwicklungsaufwände erfordert.

2 Operative Szenarien und Anforderungen

Das wesentliche operative Szenario, welches den folgenden Betrachtungen zur LST-Georedundanz zugrunde liegt, ist der Gesamtausfall eines Rechenzentrums wie z. B. einer DTZ durch exter-

A functioning rail infrastructure is important for both the economy and society. In light of the increasing risks due to extreme weather or deliberate destruction, it is essential to make the railway highly resilient. This also includes the implementation of appropriate geo-redundancy for Control Command and Signalling (CCS), i.e. the ability to take over the functions of a system if it fails at another location. This article presents short and medium-term solutions and the DB InfraGO vision for CCS geo-redundancy, as well as the prerequisites and need for further action in the sector.

1 Motivation and introduction

DB InfraGO and other European railways are in the process of digitalising their CCS technology. Within this context, the actual interlocking and safety logic is centralised into data centres or so-called digital technology centres (German: Digitale Technikzentralen, DTZ) and spatially separated from the track field that it controls. This centralisation offers many advantages, such as scaling effects or more favourable operations management, but it also increases the railway system's vulnerability, as the failure of a DTZ, e.g. in the event of a natural disaster or deliberate destruction, has large-scale consequences.
It is therefore essential that the introduction of the new digitalised rail infrastructure is accompanied by the introduction of geo-redundancy for the CCS systems, i.e. the ability of the system to ensure that another DTZ can take over its functions in the event of a DTZ failure. This is not only necessary to ensure the high overall availability of railway operations in the face of increasing climatic and geopolitical risks, but it is also required by the German Federal Office for Information Security (BSI) within the context of KRITIS [1, 2, 3].
This article describes the basic geo-redundancy options for CCS, the advantages of virtualisation within this context and the prerequisites for enabling geo-redundancy. Finally, it also offers a perspective on a possible geo-redundancy target picture that, however, still requires standardisation and development.

2 The operating scenarios and requirements

The main operating scenario on which the following CCS geo-redundancy considerations are based involves the total failure of a data centre such as a DTZ due to external influences (fire, flood, destruction, etc.). At the same time, however, it is also desirable to be able to use the redundant systems established

ne Einflüsse (Feuer, Flut, Zerstörung etc.). Zugleich ist es jedoch auch wünschenswert, die zu diesem Zweck errichteten redundanten Systeme auch für reguläre Szenarien wie z. B. die Reduzierung von Ausfallzeiten durch Instandhaltungsarbeiten oder Upgrades einsetzen zu können.

Im Folgenden bezeichnen wir als **Primärinfrastruktur** bzw. -system die Infrastruktur für LST-Funktionen (z. B. Stellwerks- oder ETCS-Zentraleinheiten), die im Regelbetrieb zum Einsatz kommt, und als **Fallbackinfrastruktur** bzw. -system diejenige, die im Katastrophenfall die Funktionen der Primärinfrastruktur übernimmt.

Grundsätzlich gelten für die DB InfraGO folgende Anforderungen an die LST-Georedundanz:

- Es muss gewährleistet sein, dass zu einem Zeitpunkt immer nur die Primär- oder die Fallbackinfrastruktur einen steuernden Einfluss auf das Bahnsystem hat.
- Umschaltvorgänge und Koordinationsprozesse müssen mit den relevanten Stellen abgestimmt, Zuständigkeiten klar definiert und die Umschaltung regelmäßig geübt werden. Sind Fallbacksysteme in Verfügbarkeit und Betriebsführung gleichwertig, muss nach Ende des Störfalles nicht zwangsläufig wieder auf das Primärsystem zurückgeschaltet werden: Primär- und Fallbackinfrastruktur tauschen dann ihre Rolle.
- Es muss möglich sein, die Fallbacksysteme überwachen und steuern zu können, ohne dass ein Ausfall oder die Nichterreichbarkeit dieser die Verfügbarkeit des Primärsystems beeinflusst.
- Es sollte möglich sein, die Fallbackinfrastruktur für eine geplante Instandhaltung einzusetzen und so z. B. Sperrpausen zu verkürzen. So können die notwendigen Maßnahmen zunächst am jeweils passiven System durchgeführt und dann nach Umschaltung am vorherigen aktiven System erfolgen. Durch Bildung kleinerer logischer Einheiten, z. B. auf der Ebene von integrierten Unterzentralen (iUZ), sollte eine Umschaltung auch nur für Teile eines Standortes möglich sein.

Wie der folgende Abschnitt zeigen wird, gibt es viele Möglichkeiten, LST-Georedundanz umzusetzen. Im Dialog mit LST-Herstellern hat die DB InfraGO eine umfassende Prüfung verschiedener Optionen nach folgenden Kriterien vorgenommen:

- Benötigte Zeit für die Umschaltung / Wiederanlauf: Wie schnell kann in einem Katastrophenfall die LST-Funktionalität der Primärinfrastruktur von der Fallbackinfrastruktur übernommen werden?
- Investitions- und Betriebskosten für das Gesamtsystem aus Primär- und Fallbackinfrastruktur
- Verfügbarkeit von Spezifikationen und LST-Produkten: Ist eine Georedundanz-Lösung mit heute verfügbaren LST-Spezifikationen und -Produkten umsetzbar, oder erfordert dies in größerem Maße Änderungen an Spezifikationen oder Produktentwicklung im Sektor?
- Erforderliche Abnahmeprozesse: Welche Schritte sind bei Inbetriebnahme des Gesamtsystems sowie im Katastrophenfall erforderlich, um das Fallbacksystem in Betrieb zu nehmen?
- Benötigte personelle Ressourcen und Kompetenzen im Regelbetrieb sowie für die Umschaltung im Katastrophenfall
- Performanz- oder Verfügbarkeitsminderung der Primärinfrastruktur: Kann die Existenz einer Fallbackinfrastruktur einen negativen Einfluss auf das Primärsystem haben, oder kann dies ausgeschlossen werden?

3 Grundsätzliche Georedundanz-Optionen

Im Folgenden werden die wesentlichen grundsätzlichen Georedundanz-Optionen erläutert, wie auch in Bild 1 dargestellt.

for this purpose for regular scenarios such as the reduction of downtimes due to maintenance work or upgrades.

The following refers to the infrastructure for CCS functions (e.g. the interlocking or Radio Block Centres) that is used in regular operations as the **primary infrastructure** or system, while the **fallback infrastructure** or system takes over the primary infrastructure's functions in the event of a disaster.

DB InfraGO has defined the following basic requirements for CCS geo-redundancy:

- It is necessary to ensure that only the primary or fallback infrastructure has a controlling influence over the rail system at any one time.
- The switchover procedures and coordination processes must be agreed with the relevant parties, the responsibilities must be clearly defined and the switchover must be regularly practised. If the fallback systems are equivalent in terms of their availability and operations management, it is not necessary to switch back to the primary system again once the incident has ended: the primary and fallback infrastructure will then swap roles.
- It must be possible to monitor and control the fallback systems without a failure or any inaccessibility affecting the availability of the primary system.
- It should be possible to use the fallback infrastructure for planned maintenance and thus shorten any track closure period, for example. This means that the necessary measures can first be carried out on the passive system and then, after the switchover, on the previously active system. The creation of smaller logical units, e.g. at the level of the integrated subcentres (German: integrierte Unterzentralen – iUZ), should also make it possible to switch over only parts of a site.

As the following section will show, there are many ways to implement CCS geo-redundancy. DB InfraGO has carried out a comprehensive review of the various options in consultation with CCS manufacturers according to the following criteria:

- The time required for the switchover: how quickly can the primary infrastructure's CCS functionality be taken over by the fallback infrastructure in the event of a disaster?
- The investment and operating costs for the overall system consisting of the primary and fallback infrastructure;
- The availability of specifications and CCS products: is a geo-redundancy solution feasible with the CCS specifications and products that are available today or will this require major changes to the CCS specifications or product development in the sector?
- The required acceptance processes: which steps are required to commission the fallback system once the overall system has been commissioned, as well as in the event of a disaster?
- The required personnel resources and competences in regular operations and for the switchover in the event of a disaster;
- Performance or availability reductions on the primary infrastructure: Can the existence of a fallback infrastructure have a negative impact on the primary system or can this be ruled out?

3 General geo-redundancy options

The general geo-redundancy options are described below and also illustrated in fig. 1.

3.1 Cold Standby

The technically simplest form of geo-redundancy is a Cold Standby solution **with complete fallback infrastructure**. Here,

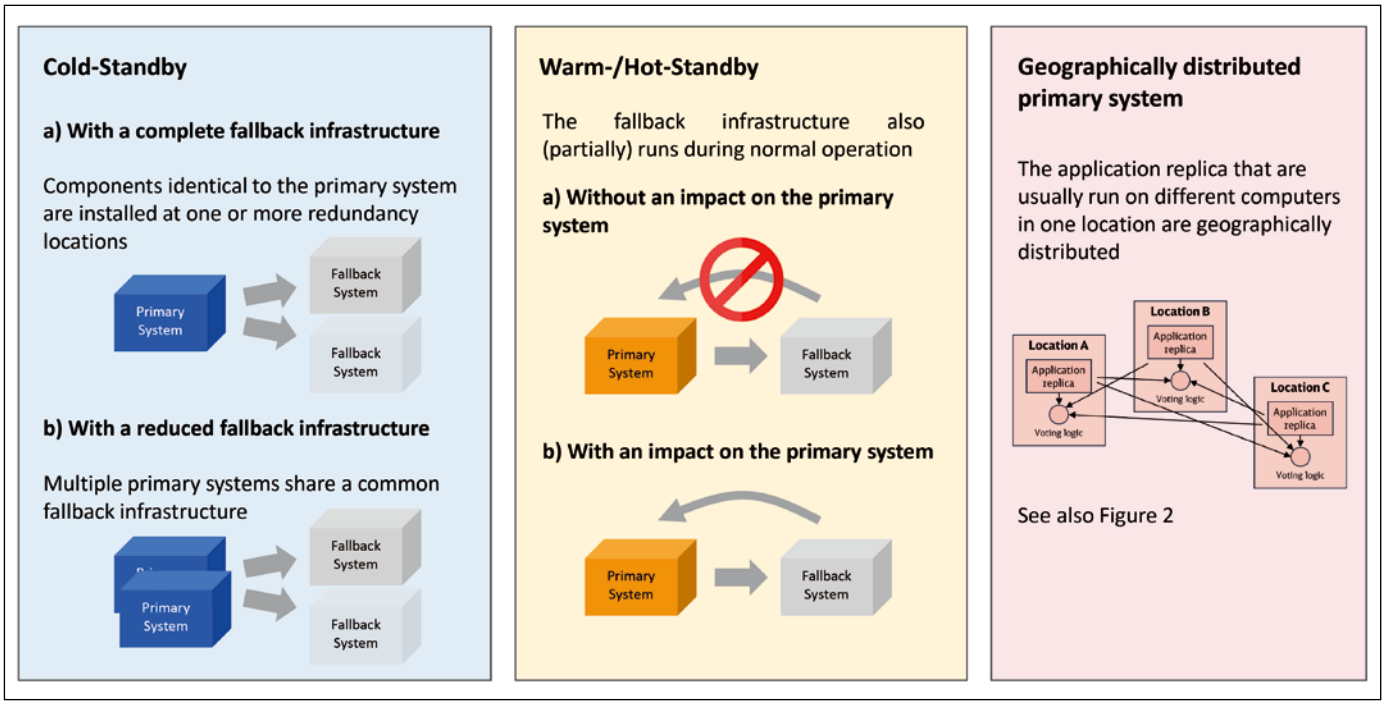


Bild 1: Grundsätzliche Georedundanzoptionen
Fig. 1: The general geo-redundancy options

3.1 Cold-Standby

Die technisch einfachste Form der Georedundanz stellt eine Cold-Standby-Lösung **mit vollständiger Fallbackausrüstung** dar. Hierbei werden zum Primärsystem identische Komponenten an einem oder mehreren Redundanzstandorten verbaut und mit den spezifischen Projektierungsdaten abgenommen, dann aber deaktiviert oder zumindest von operativen Umsystemen und dem Gleisfeld entkoppelt. Etwaige Änderungen am Primärsystem (Software-Updates, Konfigurationsänderungen etc.) werden zeitnah auch am Fallbacksystem vorgenommen, welches regelmäßig getestet wird. Da das Fallbacksystem bereits zusammen mit dem Primärsystem abgenommen wurde, ist im Katastrophenfall keine vollumfängliche Abnahme erforderlich und eine vergleichsweise schnelle Inbetriebnahme des Fallbacksystems möglich.

Ein Nachteil der Lösung sind offensichtlich hohe Investitionskosten, da das Primärsystem komplett dupliziert wird. Die Kosten lassen sich durch eine Cold-Standby-Lösung **mit reduzierter Fallbackausrüstung** senken, bei der sich mehrere Primärsysteme Fallbackstandorte teilen. Im Katastrophenfall ist dann das Einspielen spezifischer Projektierungsdaten für den ausgefallenen Standort erforderlich, ebenso wie Tests und eine Abnahme, bevor das Fallbacksystem in Betrieb genommen werden kann, was Wiederherstellungszeiten deutlich verlängert.

3.2 Warm- / Hot-Standby

Bei „Warm-Standby“ und „Hot-Standby“ läuft die Fallbackinfrastruktur auch im Regelbetrieb zumindest in Teilen mit, und der Datenstand zwischen Primär- und Fallbacksystem wird synchronisiert. Somit kann dessen Funktion im Katastrophenfall schneller als beim Cold-Standby auf das Fallbacksystem übertragen werden. Im Austausch mit LST-Herstellern wurde ersichtlich, dass es keine einheitliche Definition bzw. harte Abgrenzung von „Warm-“ und „Hot-Standby“ gibt, sondern eher ein Kontinuum an in Entwicklung befindlichen Lösungen. Ein wesentliches Differenzierungsmerkmal bei Warm-/Hot-Standby ist die Frage, ob das Fallbacksystem bzw. auch Synchronisationsmechanismen zwischen Primärcomponents identical to the primary system are installed at one or more redundancy locations and accepted together with the project-specific configuration data, but then deactivated or at least decoupled from the operating peripheral systems and the track field. Any changes to the primary system (software updates, configuration changes, etc.) are also promptly applied to the fallback system, which is regularly tested. As the fallback system has already been approved together with the primary system, full approval is not required in the event of a disaster and the fallback system can be brought into operation comparatively quickly.

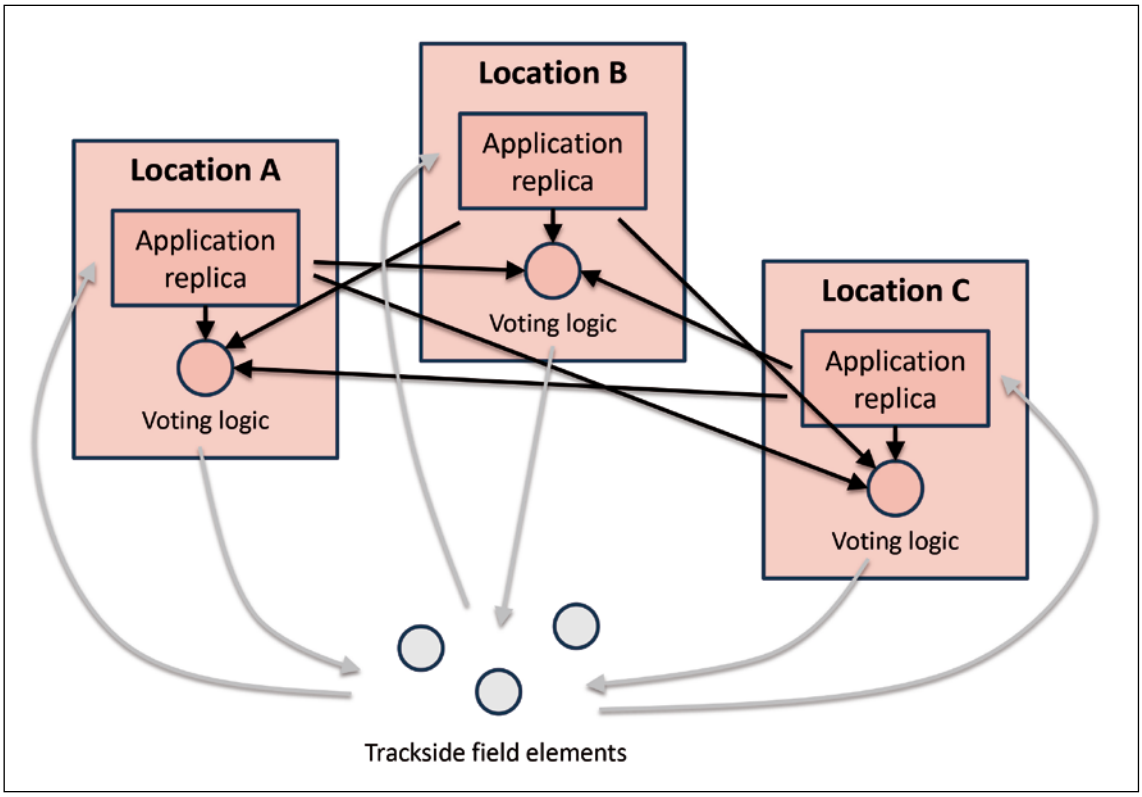
One disadvantage of the solution is obviously the high investment costs, as the primary system has been completely duplicated. The costs can be reduced by a Cold Standby solution **with a reduced fallback infrastructure**, in which several primary systems share common fallback locations. In the event of a disaster, it is then necessary to import the project-specific configuration data for the failed site and perform tests and acceptance procedures before the fallback system can be brought into operation, which significantly extends the recovery times.

3.2 Warm / Hot Standby

In “Warm Standby” and “Hot Standby” solutions, the fallback infrastructure also runs during normal operations, at least in parts, and its data is synchronised with the primary system. This means that its functions can be transferred to the fallback system in the event of a disaster more quickly than with Cold Standby.

Discussions with CCS manufacturers have made it clear that there is no standardised definition or hard demarcation between “Warm” and “Hot Standby”, but rather a continuum of solutions under development. A key differentiating feature of Warm/Hot Standby involves the question of whether the fallback system or synchronisation mechanisms between the primary and fallback systems can influence the performance and availability of the primary system.

Bild 2: Geographisch verteiltes Primärsystem
Fig. 2: A geographically distributed primary system



und Fallbacksystem die Performanz und Verfügbarkeit des Primärsystems beeinflussen können.

3.3 Geographisch verteiltes Primärsystem

Georedundanz lässt sich im Prinzip auch durch ein geographisch verteiltes Primärsystem realisieren, wie in Bild 2 dargestellt. Hierbei wird z. B. eine übliche 2-von-3-Architektur, in der eine Bahnanwendung in drei identischen Repliken auf drei Computern betrieben wird, geographisch auf drei Standorte verteilt. Eine Umschaltung von einem defekten Standort auf die anderen erfolgt dann inhärent in der 2-von-3-Logik. Diese Architektur erfordert jedoch eine hochverfügbare und latenzarme Verbindung zwischen den Standorten mit deterministischer, synchronisierter Datenverteilung.

DB InfraGO steht dieser Lösung kritisch gegenüber, da sie unweigerlich dazu führt, dass die Verfügbarkeit dieses verteilten Systems gegenüber einem klassisch an einem Ort verbauten Primärsystem abgesenkt wird, da nun immer alle räumlich getrennten Standorte an jeder Entscheidung des Systems beteiligt sind und so die Verfügbarkeit des Übertragungssystems mit einfließt. D. h., es wird zwar Georedundanz für den seltenen Totalausfall eines Rechenzentrums erreicht, allerdings zum Preis einer Absenkung der Verfügbarkeit im Regelbetrieb. Problematisch sind auch Lösungen, die Einfluss auf die Architektur der Komponenten im Gleisfeld haben, z. B. weil Objectcontroller (OC) mehr Kommunikationskanäle (Planes) als im heutigen Bahnsystem bedienen müssen oder anderweitige Abweichungen von der Eulynx-Architektur [4] implizieren.

In Bild 3 sind die beschriebenen Georedundanz-Optionen grob nach den zuvor genannten Kriterien bewertet.

3.4 DB InfraGO strebt kurz- und mittelfristig Cold-Standby-Lösungen an

Diese Lösungen sind weitestgehend mit heutigen LST-Spezifikationen sowie verfügbaren und zugelassenen LST-Produkten umsetzbar. Ein Grund hierfür ist, dass Cold-Standby so umgesetzt werden

3.3 A geographically distributed primary system

In principle, geo-redundancy can also be realised using a geographically distributed primary system, as shown in fig. 2. Here, for example, a standard 2-out-of-3 architecture, in which a railway application is operated in three identical replicas on three computers, is geographically distributed across three locations. The switchover from one defective site to the others then takes place inherently in the 2-out-of-3 logic. However, this architecture requires a high-availability, low-latency connection between the sites with deterministic, synchronised data distribution.

DB InfraGO is critical of this solution, as it inevitably leads to a reduction of availability for this distributed system compared to a primary system installed classically in one location, as all the spatially separated locations are now always involved in all the system's decisions and thus the availability of the transmission system plays a major role. This means that geo-redundancy is achieved for the rare total failure of a data centre, but at the price of a reduction in availability during regular operations. Solutions that influence the architecture of the components in the track field are also problematic, e.g. because object controllers have to operate more communication channels than in today's rail system, or imply other deviations from the Eulynx architecture [4].

Fig. 3 roughly evaluates the described geo-redundancy options according to the aforementioned criteria.

3.4 DB InfraGO is aiming for Cold Standby solutions in the short and medium term

These solutions can be implemented to a large extent using today's CCS specifications and the available and approved CCS products. One reason for this is that Cold Standby can be implemented in such a way that the peripheral systems can only see one active system at a time (i.e. the primary system or the fall-

	Cold-Standby		Warm-/Hot-Standby		A geographically distributed primary system
	a) With a complete fallback infrastructure	b) With a reduced fallback infrastructure	a) Without an impact on the primary system	b) With an impact on the primary system	
Time required for switchover *					
Investment and operating costs *					
Availability of specifications and CCS products			(depends on CCS vendor)	(depends on CCS vendor)	(in development)
Required acceptance processes					
Required personnel resources and competences					
Reduction in performance or availability of the primary infrastructure					

* Switchover times and cost substantially reduced when using virtualisation, see Section 4

Comparatively less favourable

Comparatively average

Comparatively favourable

Bild 3: Bewertung der grundsätzlichen Georedundanz-Optionen
Fig, 3: An evaluation of the general geo-redundancy options

kann, dass Umsysteme jeweils nur ein aktives System sehen (d. h. das Primärsystem oder das Fallbacksystem) – und hiermit Spezifikationsänderungen in Umsystemen vermieden werden können.
Ob eine vollumfängliche oder reduzierte Fallbackinfrastruktur angemessen ist, hängt von der Kritikalität einzelner LST-Funktionen ab, also den verkehrlichen und (volks-) wirtschaftlichen Konsequenzen eines Ausfalls. Diese werden über dedizierte Business Continuity und Risikobetrachtungen ermittelt.
Die DB InfraGO geht davon aus, dass Fallbacksysteme für möglicherweise ausfallende DTZ auch in DTZ verortet sind. Wenn aber z. B. noch keine geeignete Fallback-DTZ verfügbar ist, sind grundsätzlich aber z. B. auch containerbasierte, mobile Fallbackinfrastrukturen denkbar.
Grundsätzlich sollte, aufgrund schnellerer Wiederherstellungszeiten im Katastrophenfall, der Trend in Richtung von Warm- oder Hot-Standby-Lösungen gehen. Allerdings sind diese nach dem Verständnis der DB InfraGO nicht kurzfristig umsetzbar, da sie größere Änderungen an LST-Spezifikationen erfordern, insbesondere weil hier Primär- und Fallbackinfrastruktur gleichzeitig aktiv und für Umsysteme sichtbar sind. Die DB InfraGO würde zudem grundsätzlich nur Warm- und Hot-Standby-Lösungen in Betracht ziehen, bei denen nachweisbar ist, dass sie keinen negativen Einfluss auf Performanz und Verfügbarkeit des Primärsystems haben.
Geographisch verteilte Primärsysteme verfolgt DB InfraGO nicht, da hier nach aktuellem Kenntnisstand ein Absenken der Systemverfügbarkeit im Regelbetrieb nicht vermeidbar ist und dies nicht akzeptabel wäre.

4 Perspektivisch: Effiziente Georedundanz durch Virtualisierung

Wenn zuvor genannte Georedundanz-Lösungen mit heutigen LST-Produkten – mit üblicherweise herstellerspezifischer Hardware – umgesetzt werden, besteht grundsätzlich das Problem, dass sehr viel Hardware mit viel Platz- und möglicherweise auch

back system), meaning that any specification changes in the peripheral systems can thus be avoided.
Whether a full or reduced fallback infrastructure is appropriate depends on the criticality of the individual CCS functions, i.e. the consequences of a failure in terms of rail operations and (macro)economic impact. These are determined through dedicated business continuity and risk assessments.
DB InfraGO assumes that the fallback systems for any potentially failing DTZ will also be located in DTZ. However, if, for example, no suitable fallback DTZ are yet available, container-based, mobile fallback infrastructures are also viable.
In principle, the trend should be towards Warm or Hot Standby solutions due to the faster recovery times in the event of a disaster. However, DB InfraGO believes that these cannot be implemented in the short term, as they require major changes to the CCS specifications, especially because the primary and fallback infrastructure are active at the same time and visible to the peripheral systems. DB InfraGO would also only consider Warm and Hot Standby solutions if it can be proven that they have no negative impact on the performance and availability of the primary system.
DB InfraGO is not pursuing geographically distributed primary systems as, according to current state of knowledge, a reduction in system availability during regular operations is unavoidable and would be unacceptable.

4 Perspective: efficient geo-redundancy through virtualisation

If the aforementioned geo-redundancy solutions are implemented with today's CCS products – usually with manufacturer-specific hardware – there will be a fundamental problem involving the fact that a lot of hardware with high space and possibly also energy requirements will have to be maintained and operated for years to cope with, hopefully, rare disasters.

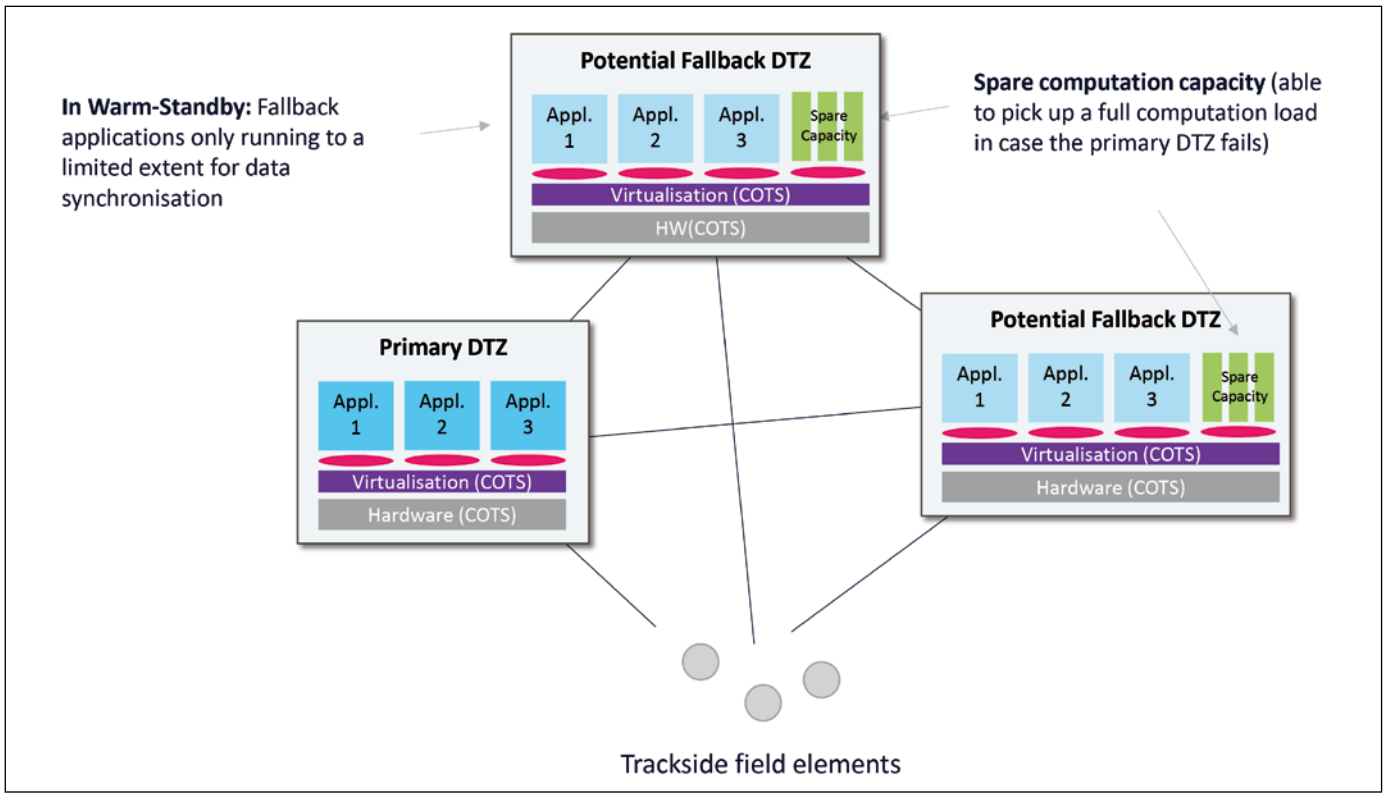


Bild 4: Virtualisierung als Grundlage effizienter Georedundanz
Fig. 4: Virtualisation as the basis for efficient geo-redundancy

Energiebedarf jahrelang für seltene Katastrophenfälle vorgehalten bzw. betrieben werden muss.

Wesentlich kosteneffizienter kann LST-Georedundanz umgesetzt werden, wenn LST-Funktionen virtualisiert und auf herstellerunabhängiger Hardware in einer On-Premises-Cloud betrieben werden, wie im Cloud-Zielbild der DB InfraGO vorgesehen [5]. Hierzu besteht bereits eine in Europe's Rail vereinbarte Architektur mit standardisierter Trennung von LST-Anwendungen bis SIL4 und der darunterliegenden IT-Plattform [6], welche gerade im Projekt Cloud4Rail [7, 8] implementiert wird.

Konkret ist dann die in Bild 4 dargestellte Architektur denkbar, mit der gleichermaßen Cold-, Warm- und Hot-Standby umgesetzt werden kann:

- LST-Funktionen laufen virtualisiert an einem Primärstandort
- Zugleich werden diese Funktionen aber auch an einem oder mehreren weiteren Standorten mit gleicher Konfiguration virtualisiert initiiert. Wie mit diesen Instanzen im Regelbetrieb umgegangen wird, hängt dann von der konkreten Georedundanz-Variante ab:
  - Bei Cold-Standby würden virtuelle Fallbackinstanzen vollständig deaktiviert, d. h. sie würden im Regelbetrieb keine CPU-Ressourcen beanspruchen (allenfalls zu gelegentlichen Testzwecken).
  - Bei Warm-Standby würden virtuelle Fallbackinstanzen mit stark reduziertem Ressourcenbedarf laufen und z. B. lediglich dynamische Zustandsdaten aus dem laufenden Bahnbetrieb synchronisieren, um diese im Katastrophenfall vorliegen zu haben.
  - Bei Hot-Standby würden Fallbackinstanzen genauso laufen wie die Instanzen der Primärsysteme, d. h. mit dem gleichen Ressourcenbedarf.
- Für etwaige Konfigurationsänderungen am Primärsystem werden zugleich auch die Fallbackinstanzen aktualisiert.
- Im Katastrophenfall werden nun geeignete Fallbackinstanzen der betroffenen LST-Funktionen vollständig aktiviert und der Betrieb auf diese umgeschaltet.

CCS geo-redundancy can be implemented much more cost-effectively if the CCS functions are virtualised and operated on manufacturer-independent hardware in an on-premises cloud, as envisaged in DB InfraGO's cloud vision [5]. An architecture with the standardised separation of the CCS applications up to SIL4 and the underlying IT platform [6], which is currently being implemented in the Cloud4Rail project [7, 8], has already been agreed upon in Europe's Rail.

Specifically, the architecture shown in fig. 4 is then conceivable, with which Cold Standby, Warm Standby or Hot Standby can be implemented in the following way:

- The CCS functions run in a virtualised form at a primary location
- At the same time, however, these functions have also been initiated in a virtualised form at one or more other locations with the same configuration. How these instances are handled in regular operations will then depend on the specific geo-redundancy variant:
  - with Cold Standby, virtual fallback instances would be completely deactivated, i.e. they would not use any CPU resources during regular operations (at most for occasional testing purposes)
  - in Warm Standby, virtual fallback instances would run with greatly reduced resource requirements and, for example, only synchronise dynamic status data from ongoing railway operations in order to have this available in the event of a disaster
  - in Hot Standby, fallback instances would run in exactly the same way as the instances of the primary systems, i.e. with the same resource requirements
- The fallback instances are also updated at the same time for any configuration changes to the primary system

Es ist anzunehmen, dass auch bei Umsetzung von Georedundanz über Virtualisierung ein manuelles Umschalten zum Fallbacksystem erfolgt – nicht, weil es nicht möglich wäre, automatisiert umzuschalten, sondern weil diese gravierende Entscheidung vermutlich immer von einem Menschen und in einem erprobten Verfahren getroffen werden sollte. Hiernach sollte es allerdings möglich sein, die betroffene LST innerhalb von Sekunden oder wenigen Minuten wieder in Betrieb zu nehmen.
Eine auf Virtualisierung basierte Architektur unterstützt offensichtlich auch den zuvor genannten Anwendungsfall einer geplanten Instandhaltung: So kann auch im Regelbetrieb der Bahnbetrieb auf das Fallbacksystem umgeschaltet werden, um Instandhaltung oder Konfigurationsänderungen im Primärsystem zu ermöglichen.

5 Voraussetzungen und Herausforderungen im Kontext von Georedundanz

Die im Folgenden genannten Voraussetzungen und Herausforderungen gelten für die meisten zuvor genannten Georedundanz-Optionen, mit oder ohne Virtualisierung.

5.1 Anbindung des Gleisfeldes an Primär- und Fallbacksysteme

Mit der Implementierung geografisch verteilter Redundanzen wird es erforderlich, die zugrundeliegende Netzwerktopologie, insb. bezogen auf die Anbindung des Gleisfeldes an zentrale LST-Funktionen, weg von einer Festlegung genau definierter Netzwerkrouten hin zu einer größeren Vermaschung von Netzwerkknoten und der Einführung von dynamischem Routing weiterzuentwickeln.

5.2 Entkopplung des jeweils inaktiven Systems

Bei Umsetzung von Cold-Standby ist es erforderlich, die nicht aktiven Systeme sicher isolieren und im Einsatzfall geregelt aktivieren zu können. Diese Isolierung sollte sinnvollerweise auf einer kleineren, logischen Einheit als der des gesamten Standortes erfolgen. Die Isolierung muss auch im Katastrophenfall von außen geregelt möglich sein und mit einer sehr hohen Sicherheit erfolgen, damit es zu keinen unerwünschten Nebeneffekten kommt. Hierfür sind geeignete Mechanismen zur Aktivierung bzw. Umschaltung der Verbindungen zu entwickeln.

5.3 Monitoring und Wartung der Fallbacksysteme

Mit der Notwendigkeit der Isolierung der nicht aktiven Systeme ergibt sich bei Cold-Standby gleichzeitig die Schwierigkeit, diese überwachen zu können. Hierfür müssen Lösungen entwickelt werden. Für Wartung und Funktionstest der Fallbacksysteme muss ebenfalls eine Lösung entwickelt werden, da ohne das (vom Fallbacksystem notwendigerweise entkoppelte) Gleisfeld kein kompletter Ende-zu-Ende-Test möglich ist.

5.4 Anlagenverantwortung und Instandhaltung

Für Anlagenverantwortung und Instandhaltung ergeben sich neue Herausforderungen. Primär- und Fallbacksystem liegen räumlich weit voneinander entfernt, sodass die Anlagen vermutlich von unterschiedlichen Personen bzw. Teams verantwortet werden müssen und eine enge Koordination bei Test, Update der Systeme und Umschaltung notwendig ist. So muss z. B. sichergestellt werden, dass beide Systeme den gleichen Versionstand aufweisen.

6 Zielbild und nächste Schritte im Sektor

Für die DB InfraGO stellt ein Warm-Standby basierend auf Virtualisierung ein langfristiges Zielbild für LST-Georedundanz dar. Dies kombiniert eine schnelle Wiederherstellungszeit der LST-Funktionen im Ka-

- In the event of a disaster, suitable fallback instances of the affected CCS functions are fully activated and operations are switched over to them

It can be assumed that a manual switchover to the fallback system will also take place when implementing geo-redundancy via virtualisation, not because it is not possible to switch over automatically, but because this serious decision should probably always be made by a human and in a tried and tested procedure. However, it should then be possible to return the affected CCS to operation within seconds or a few minutes.
An architecture based on virtualisation obviously also supports the aforementioned use case of planned maintenance: this means that rail operations can also be switched to the fallback system during normal operations to enable maintenance or configuration changes to the primary system.

5 The prerequisites and challenges within the context of geo-redundancy

The prerequisites and challenges listed below apply to most of the geo-redundancy options mentioned above, with or without virtualisation.

5.1 Connecting the track field to the primary and fallback systems

The implementation of geographically distributed redundancies will necessitate the further development of the underlying network topology, in particular with regard to the connection of the central CCS functions to the track field, away from the specification of any precisely defined network routes towards a greater meshing of network nodes and the introduction of dynamic routing.

5.2 Decoupling the inactive system

When implementing a Cold Standby, it is necessary to be able to safely isolate the inactive systems and only activate them in a controlled manner in the event of an emergency. This isolation should ideally take place on a smaller logical unit than that of the entire site. Isolation must also be possible from the outside in a controlled manner in the event of a disaster and must be carried out with a very high level of safety so that there are no undesirable side effects. Suitable mechanisms for activating or switching the connections must be developed for this purpose.

5.3 The monitoring and maintenance of the fallback systems

The need to isolate the non-active systems in Cold Standby also makes it difficult to monitor them. Solutions must be developed for this. Additionally, a solution must be developed for the maintenance and functional testing of the fallback systems, as a complete end-to-end test is not possible without the track field (being consequentially decoupled from the fallback system).

5.4 System responsibility and maintenance

New challenges arise for system responsibility and maintenance. The primary and fallback systems are located far away from each other, which means that different people or teams will likely be responsible for the systems and close coordination is required for testing, updating the systems and switching. For example, it is necessary to ensure that both systems have the same version status.

6 The target picture and the next steps in the sector

A Warm Standby approach based on virtualisation represents a long-term CCS geo-redundancy target picture for DB InfraGO.

tastrophenfall mit hoher Kosten- und Energieeffizienz, da im Regelbetrieb nur wenig CPU-Ressourcen für Redundanz aufgebracht werden müssen.

Auf dem Weg zu diesem Zielbild müssen allerdings noch diverse Schritte vollzogen werden, u. a.

- muss der Einsatz von Virtualisierung in der LST umgesetzt und zur Zulassung gebracht werden, und
- wie in Abschnitt 3 genannt, erfordert ein Warm-Standby grundsätzliche Änderungen an den LST-Spezifikationen, u. a. weil für Umsysteme dann sowohl die Primär- als auch Fallbackinfrastruktur sichtbar sind.

Auf dem Weg zum Zielbild wird daher zunächst Cold-Standby als kurzfristig verfügbare Option umgesetzt – perspektivisch dann basierend auf Virtualisierung. In einem nächsten Schritt wäre dann der Übergang zu Warm-Standby in Angriff zu nehmen.

Grundsätzlich ist es wichtig, verkehrliche und betriebliche Aufgabenstellungen, vorhandene betriebliche Redundanzen, Korridorplanungen, Bildung von Stellbereichen und die Bedeutung der Anlagen im Netz zu berücksichtigen, um fallspezifisch die optimale Georedundanz-Ausprägung (d. h. Cold-Standby mit dedizierter oder reduzierter Fallbackinfrastruktur, oder Warm-Standby) sowie geeignete Fallbackstandorte zu ermitteln. Die Implementierung der genannten Konzepte erhöht nicht nur die Resilienz des Gesamtsystems bei externen Einflüssen, sondern auch die Verfügbarkeit laufender Systeme z. B. durch Unterstützung geplanter Instandhaltungsmaßnahmen.

Neben einer konsequenten Fortsetzung der Arbeiten zur Einführung von Virtualisierung in der LST [6, 7, 8] hält die DB InfraGO es für sinnvoll, einen standardisierten Ansatz für LST-Georedundanz im europäischen Bahnsektor zu etablieren. Dieser sollte beinhalten:

- standardisierte Netzwerkprotokolle und Synchronisationsmechanismen im Kontext von Warm- und Hot-Standby
- standardisierte Mechanismen, um Fallbacksysteme zu managen und geregelt auf diese umschalten zu können, insbesondere im Hinblick auf die Verbindungen zwischen Gleisfeldelementen und LST-Innenanlage. ■

This combines a fast CCS function recovery time in the event of a disaster with high costs and energy efficiency, as only a small amount of CPU resources is required for redundancy during regular operations.

However, various steps still need to be taken on the way to achieving this vision, including

- the use of virtualisation in the CCS must be implemented and approved, and
- as mentioned in section 3, a Warm Standby requires fundamental changes to the CCS specifications, partly because both the primary and fallback infrastructure are then visible to the peripheral systems.

Cold Standby will therefore initially be implemented as a short-term option on the way to the target picture, while this may also be based on virtualisation in the future. The next step would then be to tackle the transition to Warm Standby.

In principle, it is important to consider the traffic and operations tasks, the existing operating redundancies, the corridor planning, the formation of control areas and the importance of the systems in the network in order to determine the optimum geo-redundancy configuration (i.e. Cold Standby with a dedicated or reduced fallback infrastructure or Warm Standby) and suitable fallback locations on a case-by-case basis. The implementation of the aforementioned concepts will not only increase the resilience of the overall system to external influences, but also the availability of the running systems, e.g. by supporting any planned maintenance measures.

In addition to consistently continuing work on the introduction of virtualisation in CCS [6, 7, 8], DB InfraGO also believes it makes sense to establish a standardised approach to CCS geo-redundancy in the European rail sector. This should include

- standardised network protocols and synchronisation mechanisms within the context of Warm and Hot Standby
- standardised mechanisms for managing fallback systems and the ability to switch to them in a controlled manner, particularly with regard to the connections between the trackside elements and the centralised CCS systems. ■

LITERATUR | LITERATURE

[1] BSI, „Gesetz über das Bundesamt für Sicherheit in der Informationstechnik und über die Sicherheit in der Informationstechnik von Einrichtungen (BSI-Gesetz)", Paragraph § 8a, Dezember 2025, https://www.gesetze-im-internet.de/bsig_2025/BJNR12D0B0025.html

[2] BSI, „Konkretisierung der KRITIS-Anforderungen (§ 8a Absatz 1 und Absatz 1a BSIG)", Version 1.2, September 2024, https://www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/KRITIS/Konkretisierung_Anforderungen_Massnahmen_KRITIS.html

[3] BSI, „Kriterien für die Standortauswahl von Rechenzentren", Version 2.1, Dezember 2024, https://www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/RZ-Sicherheit/Standort-Kriterien_Rechenzentren.pdf?__blob=publicationFile&v=1

[4] Eulynx, „Eulynx System Definition", Version 4.2, Juni 2025, https://eulynx.eu/storage/simple-file-list/General-Documents/Baseline-set-4-Release-4/20250619-EULYNX-System-Definition-Eu_Doc_7-v4_2-4_A.pdf

[5] Heine, A.; Marsch, P.; Rebstadt, J.: „Die Migration der Leit- und Sicherungstechnik in ein modernes IT- und Cloud-System", SIGNAL+DRAHT 11/2025

[6] Fox, M. et al.: „D26.3 – Final Modular Platform requirements, architecture and specification", ERJU FP2 R2DATO, September 2025, https://rail-research.europa.eu/rail-projects/outputs/d26-3-final-modular-platform-requirements-architecture-and-specification/

[7] Heine, A.; Marsch, P.; Albert, W.: „Nächste Station Cloud: Wie Cloud4Rail den Plattform-Markt für Europas Bahnen mobilisiert", Eisenbahntechnische Rundschau 11/2024, https://digitale-schiene-deutschland.de/Downloads/2024-11-15_ETR_Naechste_Station_Cloud.pdf

[8] IPCEI-CIS (Important Projects of Common European Interest Next Generation Cloud Infrastructure and Services) Projekt Cloud4Rail, https://www.bundeswirtschaftsministerium.de/Redaktion/DE/Artikel/Industrie/ipcei-cis.html

AUTOREN | AUTHORS

Dipl.-Inform. Dirk Schmidt
Senior Experte Digitalisierung Bahnbetrieb /
Senior Expert in Digitalisation of Railway Operations
DB InfraGO AG
Anschrift / *Address*: EUREF-Campus 17, D-10829 Berlin
E-Mail: dirk.s.schmidt@deutschebahn.com

Dr.-Ing. Patrick Marsch
Leiter Technische Gesamtsystemarchitektur, Technologiegrundsätze und IT-Plattformen /
Head of Overall Technical System Architecture, Technology Foundations and IT Platforms
DB InfraGO AG
Anschrift / *Address*: EUREF-Campus 17, D-10829 Berlin
E-Mail: patrick.marsch@deutschebahn.com

Oliver Knapp, M.Sc.
Senior Experte Informationssicherheit / *Senior Information Security Expert*
Domain Lead Railways der EU-Rail Security Domain
DB InfraGO AG
Anschrift / *Address*: Adam-Riese-Straße 11-13, D-60327 Frankfurt am Main
E-Mail: oliver.knapp@deutschebahn.com