1 Festlegen der Anforderungen

Dieses Dokument beschreibt, wie durch mehrfache Auslegung von Systemkomponenten die Verfügbarkeit der Videofunktionen in der Leitstelle erhöht und somit auch bei Ausfall von Komponenten ein sicherer Betrieb gewährleistet werden kann.

Die redundante Auslegung eines Systems erfordert erhebliche zusätzliche Ressourcen (Hardware, Netzwerkanbindungen, Softwarelizenzen, …) und macht das Gesamtsystem komplexer und somit anspruchsvoller zu administrieren. Je nach gegebenen Sicherheitsanforderungen muss deshalb die passende Balance zwischen maximaler Verfügbarkeit und dem dafür erforderlichen Aufwand (d.h. Kosten) gefunden werden. Zu diesem Zweck sollten zu Beginn die konkreten Anforderungen sorgfältig abgestimmt und festgelegt werden. Dabei sind folgende Aspekte zu berücksichtigen:

Für die passende Systemauslegung ist zu unterscheiden, ob die redundanten Komponenten nur im Fehlerfall aktiviert werden sollen (**Standby**) oder ob sie auch im Regelbetrieb z.B. zu einer besseren Lastverteilung (**Load balancing**) aktiv genutzt werden sollen.

Bei Standby-Lösungen ist zu unterscheiden, ob es genügt, wenn ab Auftreten des Fehlerfalls nach einer gewissen Aktivierungszeit der Ersatzkomponenten alle künftig eintreffenden Daten auf dem Ersatzsystem bearbeitet werden können (**Cold standby**), oder ob auch alle bis dahin im Regelbetrieb eingetroffenen Daten weiter verfügbar sein sollen (**Hot standby**). Letzteres erfordert einen permanenten Datenabgleich (Synchronisation) zwischen primär genutzten und redundanten Komponenten.

Soll mit der Redundanz ein **vollumfänglicher Betrieb** aufrecht erhalten werden, oder genügt ein **Notbetrieb** mit eingeschränkten Umfang? Auch dies sollte vorab klar definiert werden, um nicht unnötige Kosten zu verursachen.

Außerdem ist festzulegen, welche Umschaltzeit zwischen primärem und redundantem System akzeptabel ist, d.h. welche **Ausfallzeiten** toleriert werden können.

Entscheidend für die Verfügbarkeit ist es, auf **Single Points of Failure** zu achten: Gibt es einzelne Komponenten im System, von denen die Funktion des Gesamtsystems abhängt? Müssen auch sie redundant ausgelegt werden, oder können sie im Rahmen der **Risikoanalyse** als ausreichend sicher betrachtet werden?

Befinden sich alle Komponenten nahe beieinander, könnten sie von einem Großschadensereignis gleichzeitig betroffen sein, was wiederum zu einem Totalausfall führen würde. Deshalb wird mitunter zur weiteren Steigerung der Sicherheit die **räumliche Verteilung** der Ersatzkomponenten von den Komponenten für den Regelbetrieb gefordert, entweder in separaten Brandabschnitten, oder sogar an verschiedenen Standorten mit einer Mindestentfernung von z.B. 30 oder 50 Kilometern (**Geo-Redundanz**). Eine vollständige Redundanz zwischen mehreren Standorten erfordert dann aber auch eine sehr leistungsstarke **Netzwerkverbindung** zwischen diesen Standorten, weil alle Daten (d.h. auch alle Videobilder) permanent zwischen beiden Standorten abgeglichen werden müssen.

Homogene Redundanz bedeutet, dass gleichartige Systemkomponenten mehrfach vorgehalten werden, so dass bei Ausfall einer Komponente eine Ersatzkomponente gleicher Bauart genutzt werden kann. Systematische Fehler können allerdings auf allen diesen Komponenten gleichzeitig auftreten. Dagegen hilft nur **Diversitäre Redudanz**, also das Bereithalten von Ersatzsystemen, die auf andere Weise (andere Technologie, anderes Wirkprinzip, ...) realisiert sind.

2 Testkonzept

Die gewählten und realisierten Redundanzmaßnahmen sollten regelmäßig anhand eines definierten Prüfplans praxisnah überwacht werden. Dieser Prüfplan kann beispielsweise beinhalten

- Herausziehen von Steckern (z.B. Netzwerk)
- Abschalten von einzelnen Geräten
- Beenden von Softwarekomponenten mittels Task-Manager
- ...

Eine solche Prüfung erfolgt selbstverständlich jeweils erst nach Vorankündigung in und Abstimmung mit der Leitstelle und in unkritischen Betriebssituationen, damit der Wirkbetrieb nicht gestört wird. Die Prüfergebnisse werden dokumentiert; die Abstellung festgestellter Mängel wird organisiert.

3 Beteiligte Systemkomponenten

Für die Planung eines geeigneten Redundanzkonzepts ist es wichtig, die Systemarchitektur und die grundsätzliche Funktionsweise von EBÜS zu verstehen.

Diese werden im Dokument www.ebues.de/Voraussetzungen.pdf beschrieben. Dort sind die an EBÜS beteiligten Systemkomponenten sowie deren Zusammenspiel dargestellt.

Für eine redundante Auslegung einer Videoleitstelle sollten insbesondere die folgenden Systemkomponenten näher betrachtet werden:

3.1 FileServer

EBÜS nutzt das Dateisystem als zentrale Datenbasis. Alle relevanten Daten werden von den Video-Arbeitsplätzen und weiteren EBÜS-Komponenten gemeinsam genutzt und sollten daher zentral auf einem FileServer gespeichert werden.

Deshalb besteht der erste und wichtigste Schritt zur Erhöhung der Ausfallsicherheit darin, diesen FileServer hochverfügbar auszulegen. Dabei handelt es sich nicht um ein EBÜS-spezifisches Thema, sondern um eine klassische IT-Aufgabe, die mit etablierten und bewährten Verfahren umgesetzt werden kann, z. B. durch den Einsatz von Virtualisierung, Redundanzmechanismen und regelmäßigen Backups.

- **Basis für den redundanten Betrieb von EBÜS ist ein hochverfügbarer FileServer mit zuverlässiger Datensicherung (Backup)**

Welche der aktuell verfügbaren Technologien hierfür eingesetzt werden, kann von der Leitstelle bzw. der zuständigen IT-Abteilung entsprechend der betrieblichen Anforderungen und internen Vorgaben festgelegt werden.

Als FileServer kann gegebenenfalls auch eine bereits vorhandene IT-Infrastruktur genutzt werden. Ein neu eingerichteter FileServer kann zudem – abhängig vom jeweiligen Nutzungskonzept – auch für weitere IT-Dienste eingesetzt werden.

Welche Datenarten an welcher Stelle gespeichert werden (z. B. auf einem FileServer, NAS oder lokal), wird zentral in der Datei pathes.cfg festgelegt. Diese befindet sich im Startverzeichnis von EBÜS.

Eine Beschreibung der einzelnen Datenarten sowie Empfehlungen zu deren jeweiligem Speicherort finden sich in Kapitel 8.4 des Dokuments → www.ebues.de/Installation.pdf.

3.2 Netzwerk

Für optimale Ausfallsicherheit sollten auch die Netzwerkverbindungen redundant ausgelegt werden. Dies kann beispielsweise durch den Einsatz geeigneter Router, Firewalls oder VPN-Appliances erfolgen, die Verbindungen über mehrere unabhängige Übertragungswege aufbauen und automatisch zwischen diesen umschalten können.

Übliche Szenarien sind der parallele Betrieb von zwei Festnetzanschlüssen (z. B. Glasfaser und DSL) oder die Kombination eines primären Festnetzanschlusses mit einer Mobilfunkverbindung (LTE/5G) als Fallback-Lösung.

Mobilfunkrouter können dabei entweder eine separate Verbindung ins lokale Netzwerk bereitstellen oder direkt als integrierte Mobilfunkschnittstelle in der Netzwerkkomponente vorhanden sein.

Für den zuverlässigen Betrieb von EBÜS ist es wichtig, dass die beteiligten Systeme innerhalb des VPNs unabhängig vom aktuell genutzten Übertragungsweg unter konstanten, festen IP-Adressen erreichbar sind. Die Umschaltung zwischen den verfügbaren Verbindungswegen muss hierbei transparent erfolgen und darf keine Änderungen an der EBÜS-Konfiguration erforderlich machen.

- **www.ebues.de/ports zeigt die von EBÜS verwendeten Netzwerkverbindungen und Ports**

Der FileServer muss über Netzwerkfreigaben jederzeit von allen EBÜS-Software-Komponenten erreichbar sein. Dazu zählen unter anderem:

- EBÜS-VideoArbeitsplätze (VA), VideoInterface (VI)
- AlarmServer, AlarmReceiver
- Supervisor, Rundgang, Verbindungsnachweis
- PingService, Testalarmgenerator, u.v.m.

Darüber hinaus müssen alle EBÜS-Software-Komponenten untereinander stabile IP-Verbindungen über den dafür konfigurierten TCP/IP-Port (Standard: 23) aufbauen können.

Von jedem EBÜS-VideoInterface (VI) aus müssen IP-Verbindungen zu allen angebundenen Bildquellen möglich sein. Üblicherweise dient jeder EBÜS-VA auch als VI. Bei besonderen Anforderungen an Kompatibilität und Netzwerksicherheit können VA und VI aber auch getrennt betrieben werden → www.ebues.de/VideoInterface.pdf

Alarmdaten müssen – je nach Redundanzkonzept – über mehrere unabhängige Übertragungswege zu den EBÜS-AlarmReceivern gesendet werden können, um auch bei Teilstörungen eine zuverlässige Alarmverarbeitung sicherzustellen.

Eine redundante Auslegung der Netzwerkverbindungen (z. B. durch doppelte Switches, getrennte Netzpfade oder redundante Anbindungen) wird dringend empfohlen, um Single Points of Failure zu vermeiden.

3.3 Video-Arbeitsplätze

Alle EBÜS-Arbeitsplätze sind gleichberechtigt im Peer-to-Peer-Verbund organisiert und können sich gegenseitig vollständig ersetzen.

Fällt ein Arbeitsplatz aus, lassen sich sämtliche Funktionen ohne Einschränkungen von einem anderen Arbeitsplatz aus weiterführen.

Ab einer 5-Platz-Lizenz können in einer Leitstelle zusätzliche EBÜS-Videoarbeitsplätze ohne Lizenz-Mehrkosten betrieben werden. Dadurch lässt sich die Ausfallsicherheit mit linear steigendem Aufwand flexibel erhöhen und an die jeweiligen Anforderungen anpassen.

3.4 Alarmübertragung

Um die Übertragung der Alarmmeldungen und -Bilder zur Leitstelle auch bei Teilausfällen des Netzwerks zu gewährleisten, kann an verschiedenen Stellen angesetzt werden:

- An der Quelle: Bildquelle sendet Alarme auf mehreren Wegen
  So eine Lösung erfordert Bildquellentypen, die dies unterstützen
- Auf dem Weg: Umrouten von Alarmen durch den Provider
  Mit Provider klären, welche Dienste er dafür bietet
- In der Leitstelle: Umrouten von Alarmen durch den Leitstellenbetreiber
  Achtung: Single point of failure, insbesondere bei Totalausfall der Leitstelle oder der Netzwerkverbindung zur Leitstelle

EBÜS unterstützt den Parallelbetrieb mehrerer AlarmServer (incl. FTP-Server etc.).
Dabei ist aber dafür Sorge zu tragen, dass jeder Alarm nur auf einem Weg gemeldet wird.

Die Zuverlässigkeit der Alarmübertragung sollte mittels Routinemeldungen und Testalarmgenerator kontinuierlich überwacht werden, damit eventuelle Ausfälle zeitnah erkannt und behoben werden können.

4 Möglichkeiten für Redundanz

Redundanz kann auf verschiedene Weise erreicht werden:

- Homogene Redundanz: Zusätzliche EBÜS-Arbeitsplätze; der Ausfall einzelner Arbeitsplätze ist dann unkritisch; zusätzliche Software-Lizenzen sind ab dem 5. Arbeitsplatz kostenlos.
- Diversitäre Redundanz: Original-Software der integrierten Video-Hersteller als Fallback-Ebene; wird im Unterverzeichnis „..\EBÜS\Bildquellen\“ bereitgestellt
- Mehrfaches Speichern von Konfigurationsdaten durch EBÜS
- Mehrfaches Speichern von Videobildern durch EBÜS
- Redundanz durch IT-Umgebung (z.B. RAID, Virtualisierung, Cloud-Dienste)
- Umschaltbares Routing beim Provider
- Mehrere Übertragungswege Bildquelle ↔ Leitstelle (z.B. DSL + LTE/5G)
- Geo-Redundanz durch Verteilung von EBÜS auf mehrere Standorte

Wo immer möglich sollten vorzugsweise Standard-Lösungen auf der Ebene der IT-Infrastruktur genutzt werden; proprietäre Ansätze auf Anwendungsebene kommen nur in Frage, wenn für die gegebene Aufgabenstellung und unter den gegebenen Randbedingungen keine geeigneten Standard-Lösungen verfügbar sind.

Stand: 12.04.2026, Dipl.-Ing. Hardo Naumann