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. 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
- 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

Folgende Systemkomponenten sollten für die redundante Auslegung einer Videoleitstelle näher betrachtet werden:

1. Video-Arbeitsplätze

Alle EBÜS Arbeitsplätze sind gleichberechtigt (Peer-to-peer) und können sich gegenseitig ersetzen. Fällt ein Arbeitsplatz aus, können alle Funktionen ersatzweise von einem anderen Arbeitsplatz aus erledigt werden. Ab einer 5-Platz-Lizenz können weitere EBÜS-Videoarbeitsplätze in einer Leitstelle ohne Aufpreis betrieben werden. Damit ist auf dieser Seite mit linear skalierendem Aufwand eine beliebig hohe Ausfallsicherheit erreichbar.

2. FileServer

. für Konfigurationsdaten
. als Bildspeicher

Synchronisation z.B. mittels Microsoft DFS oder FreeFileSync
Realisierung auf virtuellen verteilten Plattformen

3. Netzwerkverbindungen

Redundanz mittels VPN-Router, der Verbindungen über mehrere Wege aufbauen kann
Es können zwei LAN/WAN Lines verwendet werden zur Redundanz im VPN Router.
Ein UMTS Router müsste eine UMTS Verbindung ins LAN stellen oder hat eine UMTS Schnittstelle bereits an Board. Die Geräte innerhalb des VPN sollen immer über die selbe IP-Adresse erreichbar sein, egal welche Route der VPN Router gerade nutzt.

4. Alarmübertragung

- An der Quelle: Bildquelle sendet Alarme auf mehreren Wegen
  So eine Lösung ist nur mit entsprechend geeigneten Bildquellentypen möglich
- 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.

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 + UMTS)

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: 07.03.2016, Dipl.-Ing. Hardo Naumann

Accellence Technologies GmbH • Garbsener Landstr. 10 • D-30419 Hannover
Tel. 0511 - 277.2400 • Fax 0511 - 277.2499 • E-Mail: info@accellence.de • Website: www.accellence.de