



# White Paper

WP 1003HE

## Medienredundanzkonzepte

Hochverfügbarkeit im Industrial Ethernet

### 1. Einleitung

Das generelle Thema der Medienredundanz und der redundanten Pfade ist beinahe so alt wie die Anwendung von Ethernet als Lösung zur Industriellen Kommunikation selbst. Ebenso alt ist das Dilemma, dass die Ethernet Technologie per Definition aufgrund der Rundruffcharakteristik keine physikalischen Schleifenstrukturen und damit keine redundanten Kommunikationspfade zulässt. Allerdings sind die Ausfallsicherheit und damit der Einsatz von redundanten Strukturen eine wichtige, grundlegende Anforderung sehr vieler Automatisierungssysteme.

Für den Einsatz von Ethernet in der industriellen Automatisierungstechnik ist somit der Einsatz von Protokollen notwendig, die die physikalischen Schleifenstrukturen, die durch die Einführung redundanter Pfade entstehen, auflösen können.

Für redundante Kommunikationsstrukturen in der Büroumgebung hat das IEEE (Institute of Electrical and Electronics Engineers) das im Standard 802.1D-1990 veröffentlichte Spanning Tree Protocol (STP) spezifiziert. Dieses ermöglichte erstmals durch den Einsatz eines Algorithmus in allen Ethernet Switches die Verwendung vermaschter Netzstrukturen, allerdings mit Umschaltzeiten im hohen zweistelligen Sekundenbereich. Basierend auf den grundlegenden Mechanismen des STP werden weitere Protokolle entwickelt, die an die speziellen Anforderungen des industriellen Umfelds angepasst sind und insbesondere die Umschaltzeiten deutlich reduzieren.

Dieses White Paper gibt einen Überblick über den Stand der Technik und die Lösungen, sowie eine Übersicht über spezielle Anwendungsfälle.

#### Inhalt

Einleitung	1
Gründe für Medienredundanz	1
Grundsätzliche Anforderungen für den industriellen Einsatz	2
Technologien und Lösungen	2
Zusammenfassung	8
Referenzen	8
Anhang: Weitere Unterstützung	9

### 2. Gründe für Medienredundanz

Medienredundanz wird vornehmlich eingesetzt, um sog. „Single Points of Failures“ in industriellen Kommunikationsnetzwerken zu vermeiden. Wenn ein solcher Single Point of Failure existiert, so kann das Kommunikationsnetzwerk beispielsweise einer automatisierten Fertigungsstraße durch einen einzigen Fehler oder ein einziges technisches Versagen lahm gelegt werden. Dies zieht potenziell hohe Folgekosten nach sich. Werden redundante Strukturen eingesetzt, so fällt das Netzwerk bei einem einzelnen aufgetretenen Fehler lediglich in einen fehlerbehafteten Zustand zurück. Die Kommunikation über das Netzwerk ist weiterhin sichergestellt und das redundante System ermöglicht es, eine Reparatur durchzuführen um den ursprünglichen fehlerfreien Zustand wieder herzustellen. Weitergehende, detaillierte Informationen über hochverfügbare Systeme, Medienredundanz, Fehler- und Reparaturmodelle finden sich in [1].

Redundante Netzstrukturen werden für zweierlei Zwecke eingesetzt:

1. Lastverteilung: Der über einen Netzwerkpfad innerhalb einer definierten Zeitspanne übertragene Datenverkehr übersteigt die Bandbreite, die ein einzelnes Datenkabel alleine bewältigen kann. Das Hinzufügen weiterer, redundanter Verbindungen erhöht die effektive Bandbreite einer Verbindung. Ein typisches Protokoll, das zu diesem Zweck eingesetzt werden kann ist das Link Aggregation Control Protocol (LACP) des IEEE[2].
2. Ausfallsicherheit: Zusätzliche Medienverbindungen zwischen Netzwerkteilnehmern werden eingefügt, um bei Ausfall eines primären Netzwerkpfades auf einen sekundären Pfad umzuschalten.

Während Fall 2 in Fall 1 enthalten sein kann, so ist der Einsatz von Medienredundanz im industriellen Umfeld vornehmlich auf den Fall 2 beschränkt. Die Ausfallsicherheit spielt in industriellen Netzwerken eine ungleich höhere Rolle als Lastverteilung, somit sind die meisten Protokolle für dieses Einsatzgebiet auf diese Anforderung spezialisiert, um Hochverfügbarkeit zu gewährleisten.



Hochverfügbarkeit ist eine entscheidende Voraussetzung für Automatisierungssysteme, ganz egal ob in der Fabrikautomatisierung, Prozessindustrie oder in Energieversorgungsanwendungen. Der Ausfall von Komponenten, der nie völlig ausgeschlossen werden kann, muss so behandelt werden, dass der Einfluss auf das Gesamtsystem so gering wie nur möglich ist.

### 3. Grundsätzliche Anforderungen für den industriellen Einsatz

Eine grundlegende Voraussetzung für jedes Ethernet Netzwerk ist die Vermeidung von Schleifen. Zu jeder Zeit ist nur genau ein einziger Pfad zwischen Quelle und Senke der Nachrichten erlaubt. Jede Schleife hat Datenpakete zur Folge, die für immer zirkulieren, und so das Netzwerk überschwemmen. Aus diesem Grund sind bei Ethernet alternative aktive Pfade zu einem Gerät nicht erlaubt. Für die Medienredundanz jedoch werden diese alternativen Pfade benötigt. Um diesen Konflikt zu lösen wird ein Redundanz-Kontrollprotokoll benötigt. Ein solches Protokoll stellt sicher, dass es zu jedem Zeitpunkt nur einen einzigen logischen Pfad zu jedem Endgerät gibt, selbst wenn es vielfache physikalische Wege gibt. Das Protokoll sorgt nun dafür, dass jederzeit nur einer der Wege aktiv ist und Daten überträgt, während alle anderen Pfade sich im Stand-by Modus befinden.

Die Lösung, die mit STP das erste Mal realisiert wurde, beruht auf der Überwachung der Nachrichtenpfade, der Detektion von Kommunikationsunterbrechungen, und einer Umschaltung auf einen alternativen Weg, sobald ein Ausfall erkannt wird. Dieses Prinzip bedingt jedoch immer eine gewisse Unterbrechungszeit in der Kommunikation, da zuerst der Ausfall entdeckt werden muss. Erst nach der Erkennung wird das Netzwerk auf den alternativen Pfad umgeschaltet, und die Kommunikation wieder aufgenommen.

Je nach Komplexität des Netzwerks ist die Unterbrechungszeit nur schwer vorzuberechnen.

Für den Einsatz im industriellen Umfeld

existieren für Medienredundanzprotokolle folgende grundlegenden Anforderungen:

1. Zeitlicher Determinismus hinsichtlich der Umschaltzeit: Die Zeitspanne, die ein Protokoll benötigt, um im Fehlerfall vom primären logischen Pfad in den sekundären, alternativen Pfad zu wechseln und die Verbindung wieder herzustellen, ist vorhersagbar.
2. Installationsvorgaben: Sind für das Einhalten der definierten Umschaltzeiten oder für den Protokolleinsatz bestimmte Installationsvorgaben wie beispielsweise die physikalische Topologie oder eine maximal nutzbare Anzahl an Netzwerkswitches notwendig, so sind diese Vorgaben klar zu definieren.
3. Das Protokoll basiert auf einem standardisierten, offen zugänglichen Verfahren. Nur so können Transparenz, Kompatibilität und somit Investitionssicherheit garantiert werden.

Insbesondere Anforderung 1 ist absolut essentiell für den Einsatz in der Automatisierungstechnik oder einer verwandten Anwendung. Ein Medienredundanzprotokoll ist nur einsetzbar, wenn verlässliche und berechenbare Zahlen verfügbar sind, die eine absolute Worst Case Obergrenze für die Umschaltzeit eines Netzwerks im Fehlerfall definieren. Nur so kann sichergestellt werden, dass die Anforderungen der Anwendung, die das Netzwerk als Übertragungsmedium nutzt, erfüllt werden: Schaltet ein Medienredundanzprotokoll schnell genug um, so dass der Protokollverkehr und die Anwendung unbeeinträchtigt weiterarbeiten können, so ist der Redundanzmechanismus für die Funktionsfähigkeit der Anwendung transparent und die zeitlichen Anforderungen sind erfüllt.

## 4. Technologien und Lösungen

### 4.1 RSTP/MSTP – Rapid/Multiple Spanning Tree Protocol

#### 4.1.1 RSTP/MSTP Überblick

Seit einigen Jahren wird das Eingang erwähnte STP größtenteils durch RSTP, das Rapid Spanning Tree Protocol ersetzt. Dieses ist eine optimierte Version von STP und wurde im Standard IEEE 802.1D-2004 [3] abschließend definiert. RSTP Implementierungen arbeiten in verschiedensten Topologien, unterstützen eine größere Anzahl von Switches, und verbessern die Umschaltzeit auf eine Größenordnung von etwa einer Sekunde. Aber auch RSTP garantiert kein deterministisches Ausfallverhalten. Die Reaktionszeiten hängen davon ab, an welcher Stelle im Netz der Ausfall geschieht, und von der Art der individuellen Implementierung. Aus diesem Grund gibt es einige Versuche, RSTP zu optimieren durch Beschränkung auf Ringtopologien und die Verwendung von festen vordefinierten Parametern. Mit diesen Optimierungen können heute Umschaltzeiten in der Größenordnung von 100 Millisekunden oder darunter demonstriert werden (siehe 4.1.2).

Das Rapid Spanning Tree Protocol, wie der Name bereits andeutet, schafft eine Baumstruktur von Verbindungen zwischen den Ethernet Switches und blockiert alle Pfade, die nicht Teil des aktiven Baumes sind. Dieses ergibt genau einen einzigen aktiven Pfad zwischen jeweils zwei Endgeräten. Das Protokoll verwendet so genannte Bridge Protocol Data Units (BPDUs), um zwischen den Switches zu kommunizieren. Eine „Root Bridge“ ist als die Wurzel des Baumes definiert, von ihr aus werden die optimalen Pfade im Netzwerk bestimmt. Im Falle einer Änderung im Netzwerk, z.B. eines Ausfalls einer physikalischen Verbindung, wird diese über so genannte Topology Change Notification BPDUs im Netz bekannt gegeben. Darauf erfolgt eine Neuberechnung des Baums, Aktivierung der entsprechenden Alternativpfade, und damit das Wiederherstellen der Kommunikation. Das MSTP [4] ist eine Weiterentwicklung

des RSTP und arbeitet nach dem gleichen Funktionsprinzip. Während RSTP allerdings unabhängig von Virtual Local Area Networks (VLANs) operiert, arbeitet ein MSTP innerhalb von VLANs und ermöglicht so flexiblere Netzwerkstrukturen, beispielsweise um Load Balancing über unterschiedliche VLANs und Netzwerkpfade zu realisieren. MSTP und RSTP sind zueinander kompatibel und können in einer Netzwerkstruktur gemeinsam eingesetzt werden.

#### 4.1.2 Einsatz in Ringstrukturen

Wenn die Topologie auf einen Ring beschränkt ist, können deterministische und vorher bestimmbare Umschaltzeiten bei RSTP erreicht werden, vorausgesetzt, dass das RSTP Timing der Switches bekannt ist. Im Standard IEC 62439-1 ist ein Berechnungsbeispiel gegeben, das zusätzlich weitere Einschränkungen des Protokolls fordert. So darf das RSTP beispielsweise nicht auf anderen Switchports als auf den Ringports konfiguriert sein, um Störeinflüsse von außerhalb des Rings zu vermeiden.

Da das RSTP jedoch nicht primär für Ringtopologien entwickelt wurde, weist es konzeptbedingt einige Nachteile gegenüber dem im Kapitel 4.2 vorgestellten MRP auf. Unterstützt ein Netzwerkgerät sowohl den MRP (mit dem Parametersatz von 200 ms oder besser) als auch das RSTP und schreiben beispielsweise keine Installationsvorgaben die Verwendung von bestimmten Protokollen vor, so ist dem MRP der Vorzug gegenüber dem RSTP zu geben.

Weiterhin ist zu beachten, dass das RSTP Protokoll zur Vermeidung von Überlast auf bestimmten Netzwerksegmenten durch eine hohe Anzahl von eventgesteuerten BPDUs einen eingebauten Überlastschutz besitzt. Dieser Überlastschutz kann in einer Worst Case Situation bewirken, dass die Rekonfigurationszeit aufgrund verlorener BPDUs stark bis in den Sekundenbereich hinein ansteigt. Diese Einschränkung ist in Ringstrukturen aufgrund der beschränkten Topologie nur schwach ausgeprägt, kann aber dennoch auftreten. In vermaschten Netzen kann dies jedoch häufiger auftreten, insbesondere bei komplexen Topologien

mit einer hohen Anzahl an Switchen und Medienverbindungen.

#### 4.1.3 Einsatz in vermaschten Netzen

Eine große Stärke des RSTP ist die Unterstützung beliebig vermaschter Topologien. Die damit einhergehende Flexibilität hinsichtlich der Installation ist ein klarer Vorteil gegenüber den starken Einschränkungen, die mit den Ringprotokollen wie MRP und Ringinstallationen einhergehen. Ein großer Nachteil dieser Flexibilität ist jedoch die Rekonfigurationszeit, die bei einem vermaschten Netz u. a. abhängig von der Komplexität der Netzwerktopologie ist, oder der Stelle im Netz, an der der Fehler auftritt. Weiterhin kann es, da es sich beim RSTP im Gegensatz zum MRP um ein dezentrales Protokoll handelt, bei der Etablierung neuer Kommunikationspfade und insbesondere bei der Wahl einer neuen Root Bridge zu Wettlaufsituationen kommen, die nur sehr schwer vorherbestimmbar sind. Dadurch ergeben sich Rekonfigurationszeiten im Netzwerk, die lediglich in groben Grenzen vorhersagbar sind. Dies schränkt den Einsatz von RSTP insbesondere in vermaschten Netzwerken ein.

Für vermaschte Netzwerke, die nur eine geringe Komplexität aufweisen (wie beispielsweise Ringnetzwerke mit 2-3 zusätzlichen Maschen bzw. Subringen), können jedoch nach eingehender Analyse Obergrenzen definiert werden. Diese sind aber stets individuell zu ermitteln. Im Gegensatz zu den Protokollen MRP, HSR oder PRP kann keine generelle Aussage getroffen werden.

Eine Methode zur Ermittlung der Rekonfigurationszeiten anhand konkreter Anwendungsszenarien ist beispielsweise im Rahmen der Internationalen Standardisierung durch Hirschmann/Belden für die nächste Revision des Standards IEC 62439-1 erarbeitet worden.

## 4.2 MRP – Media Redundancy Protocol

Ein Protokoll, das insbesondere industrielle Anwendungen adressiert, ist das Media Redundancy Protocol MRP. Dieses Protokoll wird im Standard IEC 62439-2, dem Industriestandard für hochverfügbare Ethernet Netzwerke, beschrieben. MRP ist exklusiv für Ringnetzwerke mit bis zu 50 Teilnehmern definiert und garantiert vollkommen deterministisches Umschaltverhalten. Je nach gewähltem Parametersatz beträgt die absolute Obergrenze der Umschaltzeit unter schlimmstmöglichen Bedingungen im Fehlerfall 500 ms, 200 ms, 30 ms oder sogar nur 10 ms. Typische Umschaltzeiten von MRP bewegen sich üblicherweise zwischen der Hälfte und einem Viertel dieser sogenannten „Worst Case Umschaltzeit“. Ein für 200 ms Worst Case konfigurierter MRP Ring benötigt so unter typischen Netzlastbedingungen zwischen 50 ms und 60 ms für die Umschaltung zwischen dem primären und dem sekundären Pfad, ein MRP Ring mit 10 ms Umschaltzeit reagiert entsprechend unter typischen Bedingungen ebenfalls schneller.

Jeder MRP Knoten benötigt einen Switch mit zwei an den Ring angeschlossenen Ringports. Bei MRP hat einer der Knoten die Funktion eines Medienredundanz-Managers (MRM). Der MRM überwacht und kontrolliert die Ringtopologie, um auf Netzwerkfehler zu reagieren. Der MRM sendet dazu Ethernet Redundancy Test Frames auf den einen Ringport, und empfängt diese auf dem anderen Port, und umgekehrt.

Im fehlerfreien Zustand blockiert der MRM auf einem seiner Ringports den Netzwerkverkehr, mit Ausnahme des MRP Protokollverkehrs. Damit wird die physikalische Ringstruktur auf der logischen Ebene für den normalen Netzwerkverkehr wieder in eine Linienstruktur umgewandelt und Schleifen werden vermieden. Erkennt der MRM aufgrund des Ausbleibens der Test Frames, dass im Ring ein Übertragungsfehler vorliegt, beispielsweise durch ein ausgefallenes Gerät oder eine defekte Medienverbindung, so öffnet er den bislang blockierten, stand-by Ringport für den normalen Protokollverkehr. Somit sind weiterhin alle Geräte über den sekundären Netzwerkpfad erreichbar.

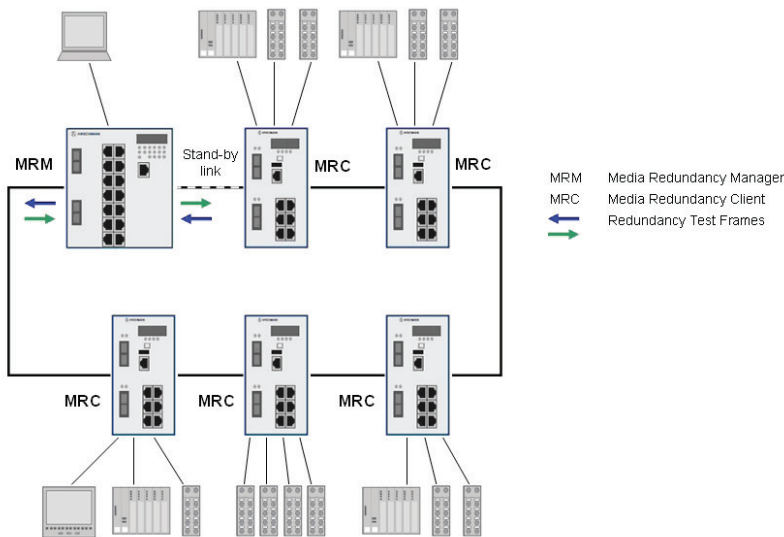


Abbildung 1- MRP Ring

Alle anderen Knoten im Ring haben die Rolle von Medienredundanz-Clients (MRC). Ein MRC leitet die vom MRM in den Ring eingespeisten Redundancy Test Frames von einem Ringport an den anderen weiter. Weiterhin reagiert er ebenfalls auf erhaltene Rekonfigurationsframes (Topology Change) des MRM, detektiert Zustandsänderungen seiner Ports und meldet diese an den MRM. Treffen diese Zustandsänderungen früher beim MRM ein, als dieser einen Fehler im Ring über das Ausbleiben von Test Frames erkennen kann, so nutzt der MRM diese Information des MRC zur Fehlererkennung auf dem Ring. Somit ist sichergestellt, dass das Umschalten vom primären auf den sekundären Netzwerkpfad im MRM stets mit einer möglichst kurzen Umschaltzeit erfolgt. Aufgrund der Flexibilität hinsichtlich Umschaltzeit und der Unterscheidung zwischen einem dedizierten Manager (MRM) und einem ressourcenschonenden Client (MRC), deckt der MRP Ring eine große Anzahl an praktischen Anforderungen ab und kann in der Implementierung optimal auf diese angepasst werden.

#### 4.3 PRP – Parallel Redundancy Protocol

Obwohl mit einem schnellen MRP Ring mittlerweile eine große Anzahl an Anforderungen abgedeckt wird, existieren dennoch Anwendungen, die keinerlei Umschaltzeit tolerieren können. Für diese Anforderungen wird ein völlig neuer Ansatz gewählt, um Hochverfügbarkeit sicherzustellen. Dieser völlig andere Ansatz der Netzwerkredundanz basiert auf zwei unabhängigen aktiven Pfaden zwischen zwei Geräten. Der Sender verwendet zwei unabhängige Netzwerkschnittstellen, die beide gleichzeitig dieselben Daten aussenden. Hier stellt das Redundanz-Kontrollprotokoll sicher, dass der Empfänger nur das erste Datenpaket verwendet, und das zweite verwirft. Wenn nur ein Paket empfangen wird, weiß der Empfänger, dass auf dem anderen Pfad ein Ausfall aufgetreten ist. Dieses Prinzip wird von dem Parallel Redundancy Protocol (PRP) verwendet. Das PRP ist im Standard IEC 62439-3 beschrieben. PRP verwendet zwei unabhängige Netzwerke beliebiger Topologie und ist nicht auf Ringnetzwerke beschränkt. In den beiden voneinander unabhängigen parallelen Netzwerken werden jeweils MRP Ringe, RSTP Netze oder auch Netzwerke ohne

jegliche Redundanz verwendet. Der große Vorteil von PRP ist die unterbrechungsfreie Umschaltung, die jegliche Umschaltzeit im Fehlerfall vermeidet und so die höchstmögliche Verfügbarkeit bietet. Dies gilt natürlich nur wenn nicht beide Netzwerke gleichzeitig Ausfälle zeigen.

Das PRP Protokoll ist in den Endgeräten implementiert, während die Switches in den Netzwerken Standard Switches sind, und nichts von PRP wissen. Ein Endgerät mit PRP Funktionalität wird Double Attached Node for PRP (DAN P) genannt und hat je eine Verbindung zu jedem der zwei unabhängigen Netzwerke. Diese beiden Netzwerke können entweder identische Strukturen haben, oder sie können sich in der Topologie oder Leistung unterscheiden.

Ein Standardgerät mit einer einzelnen Netzwerkschnittstelle (Single Attached Node, SAN) kann an eines der beiden Netze direkt angeschlossen werden. In diesem Fall hat das Gerät natürlich keinen redundanten Pfad im Falle eines Ausfalls verfügbar. Oder ein SAN kann an eine so genannte Redundancy-Box (RedBox) angeschlossen werden, welche ein oder mehrere SANs an beide Netzwerke anschließt. SANs brauchen nichts von PRP zu wissen, sie können Standardgeräte sein. In vielen Anwendungen brauchen nur kritische Geräte eine doppelte Netzwerkschnittstelle, während weniger kritische Geräte als SAN, mit oder ohne den Gebrauch einer Redundancy-Box, angeschlossen werden.

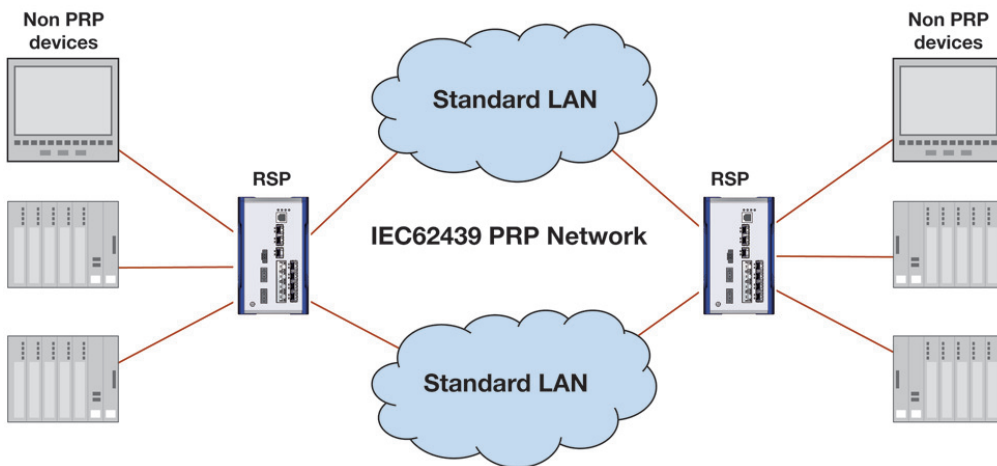


Abbildung 2 – Identische Datenpakete werden in beide Netzwerke gleichzeitig gesendet

Eine DAN P Implementierung steuert die Redundanz und behandelt Duplikate. Wenn ein zu sendendes Paket von den oberen Schichten erhalten wird, sendet die PRP Einheit diesen Frame gleichzeitig über beide Ports auf das Netzwerk. Die beiden Frames durchlaufen die zwei unabhängigen Netzwerke normalerweise mit verschiedenen Verzögerungen bis zum Empfänger. Am Bestimmungsort leitet die PRP Einheit das erste ankommende Paket an die oberen Schichten, also die Anwendung weiter, und verwirft das zweite Paket. Die Schnittstelle zur Anwendung ist damit völlig identisch wie jede andere Ethernet Netzwerk Schnittstelle auch.

Die Redundancy-Box implementiert das PRP Protokoll für alle angeschlossenen SANs und arbeitet damit als eine Art von Redundanz Proxy für jede Art von Standard Geräten.

Die Erkennung von Duplikaten erfolgt mit Hilfe eines durch eine PRP Anschaltung oder RedBox in jedes Frame eingefügten Redundancy Control Trailers (RCT). Dieses 32 Bit lange Identifikationsfeld beinhaltet neben einer Kennung für das Netzwerk (LAN A oder B) und einer Information über die Länge der Nutzlast des Frames auch eine Sequenznummer. Diese wird für jedes Frame, das ein Knoten versendet, inkrementiert. Anhand der somit eindeutigen Merkmale in jedem Frame (Physikalische MAC-Quelladresse und Sequenznummer) kann eine RedBox oder DAN P Anschaltung Duplikate erkennen und, wenn notwendig, verwerfen.

Da der RCT am Ende des Frames eingefügt wird (siehe Abbildung 3), bleibt sämtlicher Protokollverkehr für SANs vollständig lesbar. Ein SAN interpretiert den RCT lediglich als zusätzlich eingefügte Füllbits („Padding“) ohne Bedeutung. Eine direkt ohne RedBox angeschlossene SAN kann somit in einem PRP Netzwerk mit allen DAN Ps und mit SANs des gleichen Netzwerks (entweder A oder B) kommunizieren. Lediglich zu den Knoten des jeweils anderen Netzwerks hat eine SAN keine Verbindung, da ein DAN P Frames eines LAN nicht an das andere weitergeben. Das PRP erfüllt höchste Ansprüche an Umschaltzeit, ist sehr flexibel im Netzaufbau und in den möglichen Topologien, benötigt allerdings stets eine doppelt installierte Infrastruktur aus Switchen und anderen Netzkomponenten.

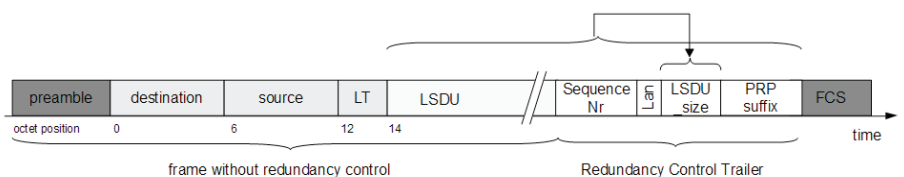


Abbildung 3- PRP Frame Format ohne VLAN Tag (Auszug aus IEC 62439-3)

#### 4.4 HSR – High Availability Seamless Redundancy

Eine Weiterentwicklung des PRP Gedankens ist die High Availability Seamless Redundancy (HSR). HSR ist allerdings in der Ausprägung ein Protokoll zur Herstellung von Medienredundanz. PRP ist, wie im vorherigen Kapitel beschrieben, ein Protokoll zur Herstellung von Netzwerkredundanz. HSR ist ebenso wie PRP im Standard IEC 62439-3 beschrieben.

HSR ist, im Gegensatz zu PRP, primär für den Einsatz in (redundant gekoppelten) Ringtopologien ausgelegt. Hierbei wird, ebenso wie bei PRP, mit zwei Netzwerkports gearbeitet. Im Gegensatz zu PRP werden in einer HSR Anschaltung, einem DAN H (Double Attached Node for HSR), die beiden Schnittstellen allerdings zu einem Ring verschaltet (siehe Abbildung 4).

Ein Frame von der Anwendung wird durch die HSR Anschaltung mit einem HSR Tag versehen. Dieser beinhaltet, analog zum PRP RCT, die Länge der Nutzlast, den Sendeport und die Sequenznummer des Frames. Im Gegensatz zu PRP wird der HSR Header allerdings dazu genutzt, das Ethernet Frame zu kapseln. (siehe Abbildung 5) Dies hat den Vorteil, dass die Duplikaterkennung für jedes einzelne Frame in jedem Gerät unmittelbar nach Empfang des HSR Headers erfolgt. Das Warten mit der Duplikaterkennung, bis das Frame inklusive RCT empfangen ist, entfällt. So wird in den einzelnen HSR Anschaltungen und RedBoxen, ähnlich wie bei Cutthrough Switching, bereits mit der Weiterleitung des Frames am zweiten Ringport begonnen, sobald der HSR Header komplett empfangen und die Duplikaterkennung durchgeführt ist.

Jeder HSR Knoten nimmt Frames die nur an ihn selbst adressiert sind vom Netz und leitet sie an die Anwendung weiter. Multicast oder Broadcast Nachrichten werden von jedem Knoten auf dem Ring weitergeleitet und zusätzlich an die Anwendung weitergegeben. Um ein permanentes Kreisen von Multicast/Broadcast Frames zu vermeiden, verwirft der Knoten, der das Multicast/Broadcast Frame ursprünglich auf den Ring gelegt hat, dieses nach einem Ringumlauf (siehe HSR data flow in Abbildung 4).

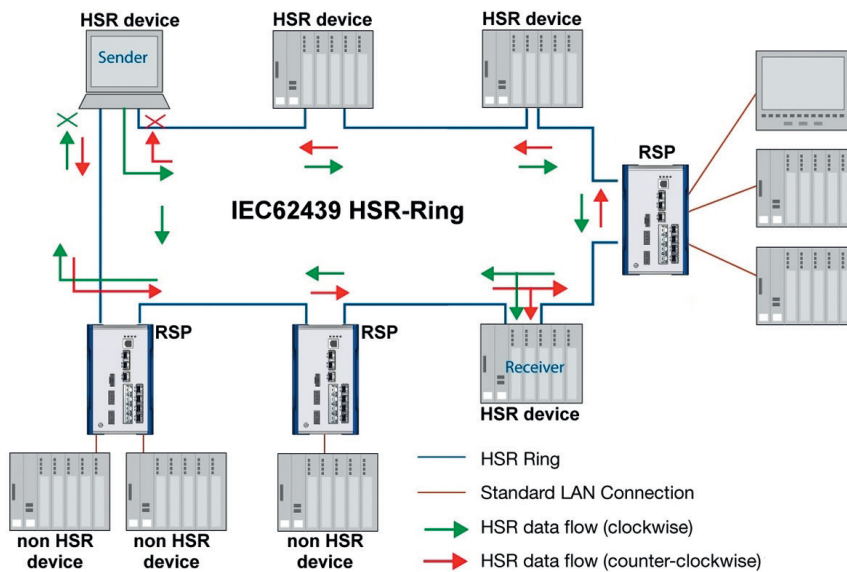


Abbildung 4 – Duplizierte Datenpakete werden gleichzeitig in beide Richtungen gesendet



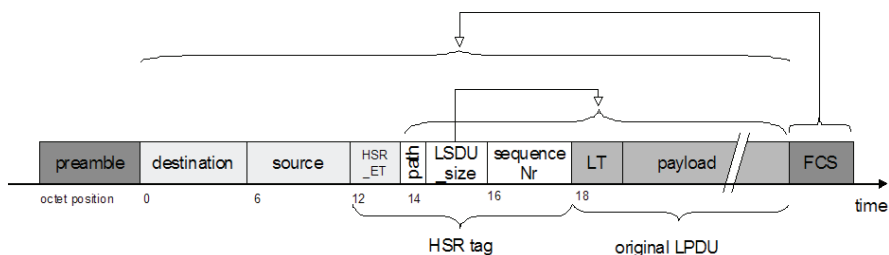


Abbildung 5 – HSR Frame Format ohne VLAN Tag (Auszug aus IEC 62439-3)

Im Gegensatz zu PRP ist die direkte Integration von SAN Knoten in ein HSR Netzwerk unmöglich, ohne den Ring aufzubrechen. Zum Schließen des Rings fehlt einem SAN die zweite Netzwerkschnittstelle. Dies ist ein Grund, warum SANs in HSR Netzwerken nur über Redundancy Boxes angebunden werden können. Der zweite Grund ist die Kapselung des Netzwerkverkehrs auf dem Ring mit dem HSR Header. Dies verhindert eine direkte Teilnahme normaler Netzwerkknoten am HSR Verkehr, im Gegensatz zu PRP. Während der PRP RCT von einem SAN Knoten als Padding interpretiert wird, ist dies beim HSR Tag unmöglich: Der HSR Tag wird aufgrund seiner Position im Frame stets als gültige Layer 2 Frameinformation interpretiert, und ein korrektes Auslesen der Nutzlast des Frames durch den SAN Knoten wird verhindert.

Da manche HSR Geräte möglicherweise zu Konfigurations- und Diagnosezwecken mit einer Management Station oder einem Notebook kommunizieren, akzeptieren HSR Anschaltungen Geräte, die Standard Ethernet Frames versenden temporär auch an den Ringports. In diesem Fall kommunizieren die HSR Anschaltungen ohne die HSR Header Kapselung. Allerdings wird dieser Verkehr nicht an das HSR Netzwerk weitergereicht, es findet lediglich eine bidirektionale Kommunikation zwischen der konfigurierenden Managementstation an einem HSR Port und dem HSR Gerät statt. Die normale HSR Kommunikation wird

erst wieder aufgenommen, wenn der Ring wieder geschlossen wurde. Eine Kopplung zwischen zwei HSR Ringen wird mittels zweier Ringkopplungselemente, den sog. QuadBoxes realisiert. Diese ermöglichen eine Kopplung zwischen zwei HSR Ringen ohne Single Point of Failure (siehe Abbildung 6)

Die HSR weist hinsichtlich der Umschaltzeit das gleiche Verhalten auf wie PRP: Durch den doppelten Versand der Frames von beiden Ports einer HSR Anschaltung wird bei einem aufgetretenen Fehler weiterhin ein Frame über den noch intakten Netzwerkpfad übertragen. Die Redundanz arbeitet somit ebenfalls ohne Umschaltzeit und im Gegensatz zu PRP werden keine zwei parallelen Netzwerke benötigt.

Allerdings ist ein HSR Netzwerk stets als Ring oder als Struktur mehrerer gekoppelter Ringe ausgeprägt und bietet bei der Installation weniger Flexibilität als PRP. Weiterhin steht auf dem Ring durch den doppelten Versand der Frames in beide Richtungen lediglich effektiv 50% der Bandbreite des Netzwerks für den Datenverkehr zur Verfügung.

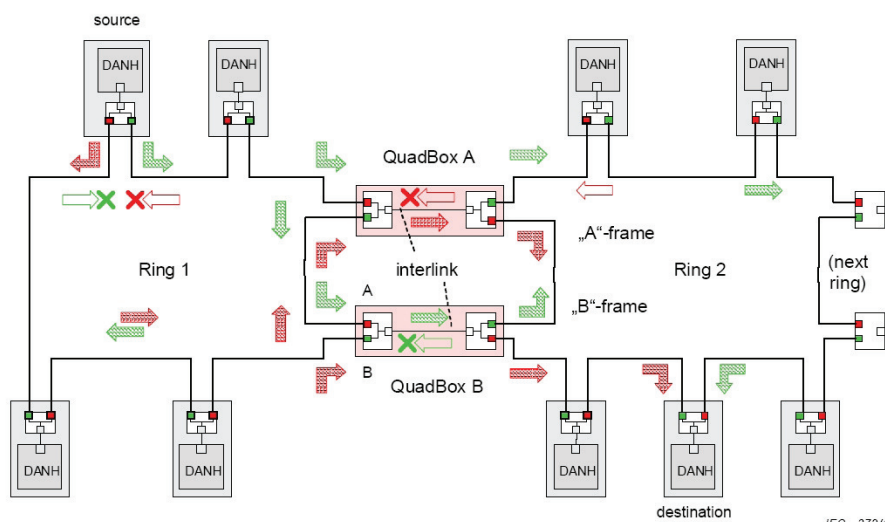


Abbildung 6 – Gekoppelte HSR Ringe (Auszug aus IEC 62439-3)

IEC 372/10



## 5. Zusammenfassung

In der Praxis existiert weder die perfekte Netzwerktopologie, noch das perfekte Medienredundanzprotokoll, das alle Anwendungsgebiete und Anforderungen exakt abdeckt.

Die richtige Wahl von Topologie und Protokoll hängt immer von zusätzlichen Faktoren ab wie beispielsweise physikalische Installationsvorgaben und/oder die Anforderungen der Anwendung an die Umschaltzeit.

Zur Übersicht der in diesem White Paper abgedeckten Redundanztechnologien sind die Protokolle und die zugehörigen wichtigsten Parameter in der folgenden Tabelle nochmals zusammengefasst

Ethernet nach dem neuesten technischen Stand ist in der Lage, auch die Anforderungen anspruchsvollster Anwendungen zu erfüllen.

Wird bereits in der Planungsphase eines Kommunikationsnetzwerks die korrekte Technologie identifiziert, so können Projektrisiken bereits früh minimiert werden. Dieses White Paper ist ein erster Schritt zur Identifikation der geeigneten Technologie. Für weiterführende Gespräche, Service und Beratung steht das Consultingteam im HICOM Center von Belden mit Rat und Tat zur Seite, um für Sie die individuell passende Lösung zu erarbeiten[5].

Protokoll	Topologie	Max. Geräte	Worst Case Rekonfigurationszeit	Normal Case Rekonfigurationszeit
RSTP (IEEE 802.1D-2004)	Ring	40	>2s bei mehrfachem BPDU Verlust	Abhängig von der RSTP Implementierung und Anzahl der Switche im Ring. Typischerweise zwischen 100ms und 200ms bei 40 Geräten
RSTP (IEEE 802.1D-2004)	Beliebig	Beliebig	>2s bei mehrfachem BPDU Verlust	Nur schwer abschätzbar, erfordert eingehende individuelle Analyse eines Netzwerks.
MRP (IEC 62439-2)	Ring	50	500ms, 200ms, 30ms, 10ms (Je nach unterstütztem Parametersatz)	Ca. 200ms, 60ms, 15ms, <10ms (Je nach unterstütztem Parametersatz)
PRP (IEC 62439-3)	Doppelt, Beliebig	Beliebig	0ms	0ms
HSR (IEC 62439-3)	(gekoppelte) Ringe	512	0ms	0ms

## 6. Referenzen

- [1] Hubert Kirrmann – Fault tolerant computing in industrial automation ([http://lamspeople.epfl.ch/kirrmann/Pubs/FT\\_Tutorial\\_HK\\_050418.pdf](http://lamspeople.epfl.ch/kirrmann/Pubs/FT_Tutorial_HK_050418.pdf))
- [2] IEEE 802.1AX-2008 (<http://standards.ieee.org/getieee802/download/802.1AX-2008.pdf>)
- [3] IEEE 802.1D-2004 (<http://standards.ieee.org/getieee802/download/802.1D-2004.pdf>)
- [4] IEEE 802.1Q-2005/cor1-2008 ([http://standards.ieee.org/getieee802/download/802.1Q-2005\\_Cor1-2008.pdf](http://standards.ieee.org/getieee802/download/802.1Q-2005_Cor1-2008.pdf))
- [5] Hirschmann Service und Support(<http://www.beldensolutions.com/de/Service/index.phtml>)



## Anhang: Weitere Unterstützung

### Technische Fragen und Schulungsangebote

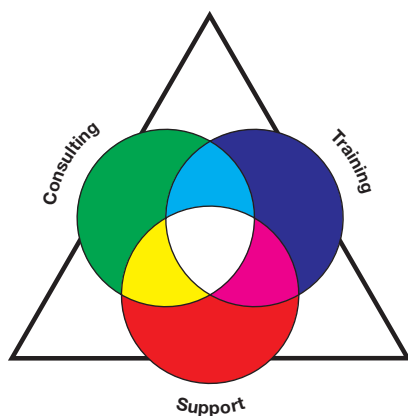
Bei technischen Fragen wenden Sie sich bitte an den Hirschmann™-Vertragspartner in Ihrer Nähe oder direkt an Hirschmann™. Die Adressen unserer Vertragspartner finden Sie im Internet unter [www.hirschmann.com](http://www.hirschmann.com)

Darüber hinaus steht Ihnen unsere Hotline zur Verfügung:

Tel. +49 (0)1805 14-1538

Fax +49 (0)7127 14-1551

Das aktuelle Schulungsangebot zu Technologie und Produkten finden Sie unter <http://www.hicomcenter.com>.



### Belden Competence Center

Langfristig garantieren hervorragende Produkte allein keine erfolgreiche Kundenbeziehung. Erst der umfassende Service macht weltweit den Unterschied. In dieser globalen Konkurrenz hat das Belden Competence Center mit dem kompletten Spektrum innovativer Dienstleistungen vor den Wettbewerbern gleich dreifach die Nase vorn:

- Das Consulting umfasst die gesamte technische Beratung von der Systembewertung über die Netzplanung bis hin zur Projektierung.
- Das Training bietet Grundlagenvermittlung, Produkteinweisung und Anwenderschulung mit Zertifizierung.
- Der Support reicht von der Inbetriebnahme über den Bereitschaftsservice bis zu den Wartungskonzepten.

Mit dem Belden Competence Center entscheiden Sie sich in jedem Fall gegen jeden Kompromiss. Das kundenindividuelle Angebot lässt Ihnen die Wahl, welche Servicekomponenten Sie in Anspruch nehmen.

Weitere Informationen finden Sie im Internet unter: <http://www.hicomcenter.com>.