

Kritische Infrastrukturen (KRITIS) Anforderungen im Hinblick auf Redundanz und Sicherheit



Schutz kritischer Infrastrukturen (SKI)



Aginode Germany GmbH

Marcel Reifenberg

**Senior Product Manager & Head of Technical
Customer Support**



Was sind kritische Infrastrukturen



Kritische Infrastrukturen (KRITIS)

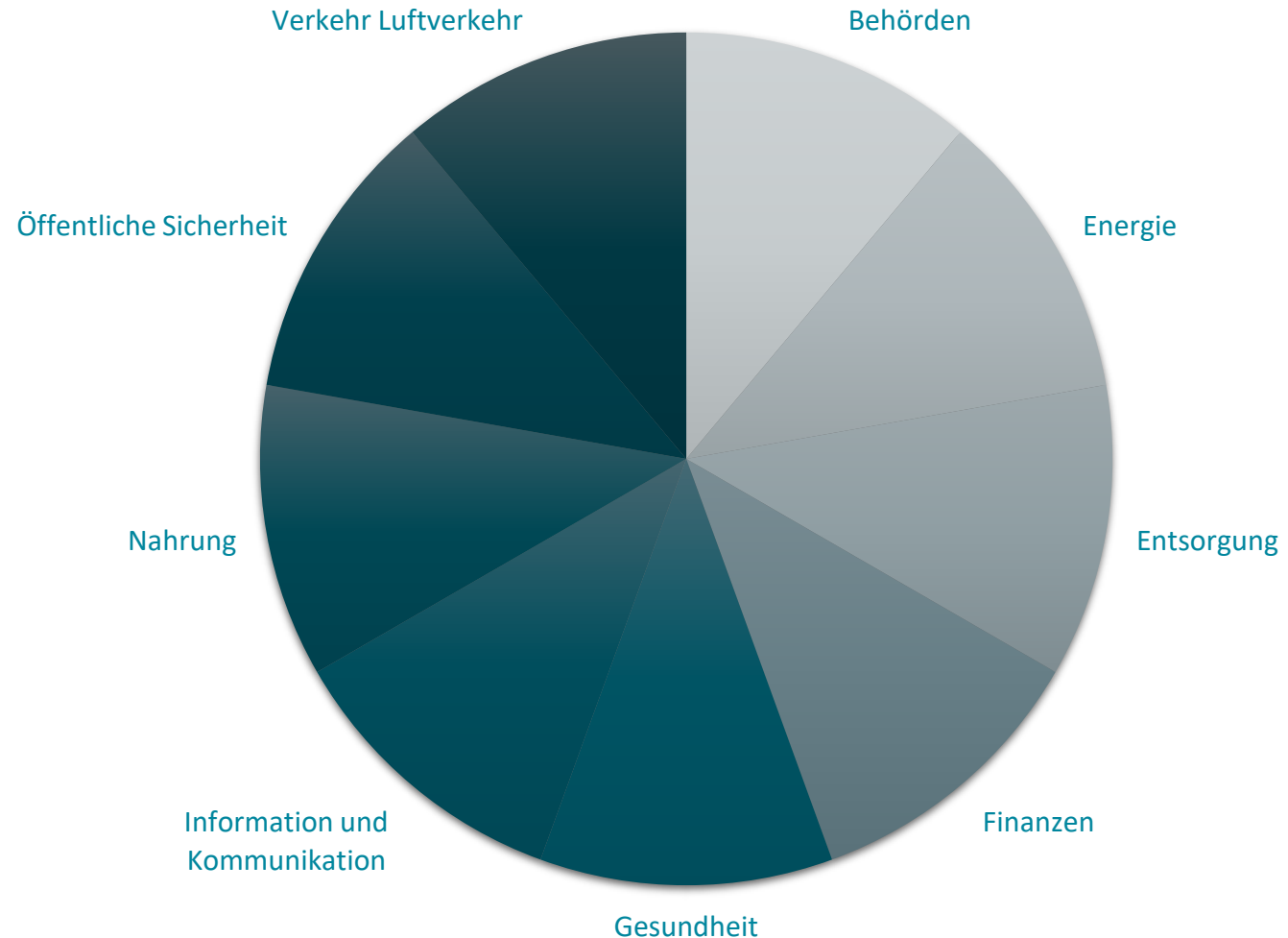
Unter kritischen Infrastrukturen werden Dienstleistungs- und Versorgungssysteme verstanden, die essenziell für die Wirtschaft bzw. die Lebensgrundlagen der Bevölkerung sind (Stromversorgung, medizinische Versorgung, Telekommunikation usw.). Dabei zählen nicht nur Bauten und Anlagen dazu, sondern sämtliche Elemente, die für die Verfügbarkeit der Güter und Dienstleistungen notwendig sind (IT-Systeme, Netzwerke etc.).

Definition des BABS. Quelle:
<https://www.babs.admin.ch/de/ski>



Sektoren kritischer Infrastrukturen

- **Neun Sektoren**
- **27 Teilsektoren**
- **Energie**
 - Erdgasversorgung
 - Erdölversorgung
 - Stromversorgung
 - Fern- und Prozesswärme
- **Information und Kommunikation**
 - IT-Dienstleistungen
 - Telekommunikation
 - Medien
 - Postdienste



Schutz kritischer Infrastrukturen (SKI)



- “ 2012 wurde die nationale Strategie zum Schutz kritischer Infrastrukturen eingeführt
- “ 2023 wurde diese vom Bundesrat neu verabschiedet, nachdem die bereits 2017 erneuert wurde
- “ Die SKI-Strategie ist unbefristet, jedoch prüft das Bundesamt für Bevölkerungsschutz alle vier Jahre, ob eine Aktualisierung notwendig ist



Leitfaden Schutz kritischer Infrastrukturen



- Das Bundesamt für Bevölkerungsschutz stellt einen Leitfaden Schutz kritischer Infrastrukturen zur Verfügung

Quelle:
<https://www.babs.admin.ch/de/leitfaden-schutz-kritischer-infrastrukturen>



IKT-Minimalstandard



Quelle: https://www.bwl.admin.ch/bwl/de/home/bereiche/ikt/ikt_minimalstandard.html

- Kein Gesetz, sondern eine Empfehlung für kritische Infrastrukturen
- Gliederung in drei Teile:
 - Grundlagen als Nachschlagewerk
 - Framework mit 108 Massnahmen
 - Self-Assessment zur Prüfung des Umsetzungsstand
- Defense-in-Depth-Strategie
 - Netzwerk-Architektur
 - Typische Sicherheitszonen
 - Demilitarized Zones (DMZ)
 - Virtual LANs
 - Netzwerk Perimeter Security
 - Firewalls
 - Fernzugriff & Authentifizierung
 - Jump Servers/Hosts



Was macht die EU



Quelle: @bluedesign / Fotolia.com

- **EU-Richtlinie: Netzwerk- und Informationssicherheit (NIS)**
- **2017 wurde das NIS-Richtlinien-Umsetzungsgesetz veröffentlicht**
- **NIS-2 erweitert den Anwendungsbereich und die Mindestsicherheitsanforderungen. Umsetzung bis Oktober 2024**
- **In Deutschland gibt es das IT-Sicherheitsgesetz 2.0**



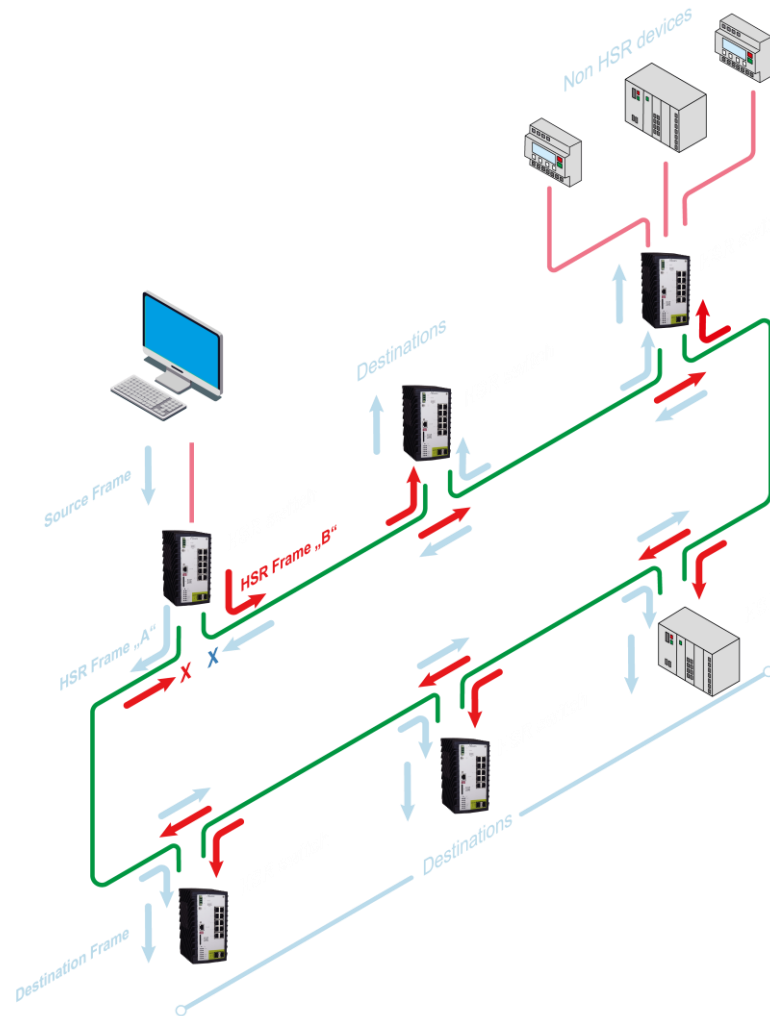
Redundanz in KRITIS Netzwerken



- **Hardware-Redundanz:** Servern, Switches, und Routern sollten im Falle eines Defektes schnell ersetzt werden können
- **Weg-Redundanz:** Wichtige Netzwerkknoten sollten redundant angebunden werden
- **Protokoll-Redundanz:** Die Verwendung von Redundanz Protokollen ermöglicht alternative Pfade
- **Redundante Stromversorgung:** Unterbrechungsfreie Stromversorgung



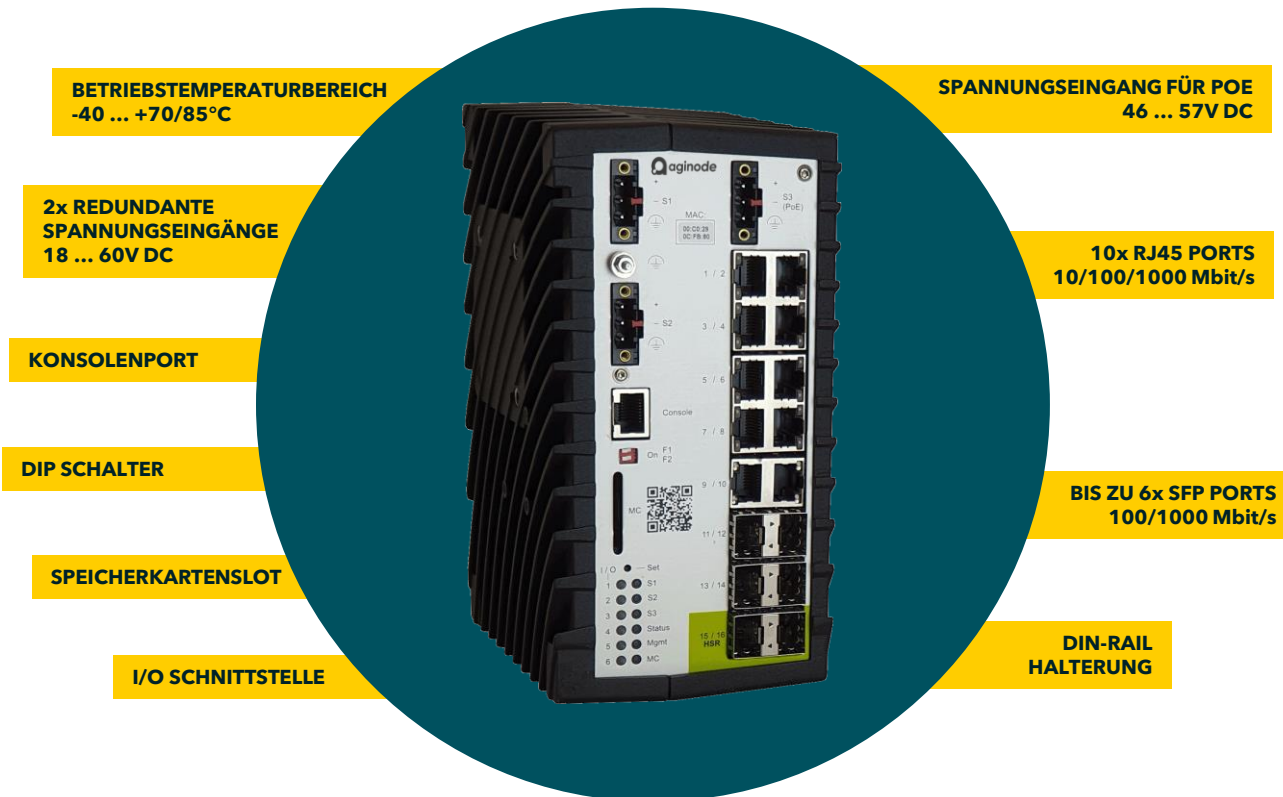
Zero Loss Redundanz in Ringtopologien



- High Availability Seamless Redundancy (HSR)
- Beschrieben im Standard IEC 62439-3
- Für Anwendungen mit höchsten Anforderungen an die Verfügbarkeit und Datenübertragung in Ring-Topologien
- Redundante Übertragung aller Datenpakete über beide Wege zum Ziel
- Keine Wiederherstellungszeit des Netzwerks im Fehlerfall
- Kein Paketverluste im Fehlerfall
- Optimierte Switch-Hardware mit HSR- Funktionalität



iGigaSwitch HSR Familie



- **16 und 12 Port industrielle Ethernet-Switche mit HSR-Redundanz:**
 - 2x oder 6x SFP-Ports (100/1000 Mbit/s) je nach Switch-Modell
 - 2x HSR/PRP-Ports
- **Bis zu 8x PoE+-Ports (IEEE802.3at)**
- **Smart Grid: IEC 61850-Konformität**
- **Optionale I/O-Schnittstellen:**
 - 4x Eingangs- + 2x Ausgangsports
- **AC oder DC-Eingangsspannung**
- **Betriebstemperaturbereich:**
 - -40...+70/85°C



Sicherheit in KRITIS Netzwerken



- **Zugriffskontrolle:** Erfolgreiche und nicht erfolgreiche Zugriffe protokollieren
- **Verschlüsselung:** Konfiguration, sowie Nutzdaten sollten verschlüsselt versendet werden
- **Firewalls:** Unerwünschte Zugriffe blockieren
- **Sicherheitsaudits und Updates:** Identifizieren von Sicherheitslücken. Firmware auf dem neusten Stand halten
- **Physische Sicherheit:** Vermeidung unbefugter Manipulation oder Diebstahl
- **Support:** Gültige Support Verträge abschließen
- **Hardware:** Keine abgekündigte Hardware verwenden




Regelmäßige Sicherheitsaudits und Updates



- **Test der kryptographischen Verfahren:** Verfahren nach Vorgabe des BSI implementieren
- **PSIRT:** Einrichtung eines Security Incident Response and Product Security Portal
- **Granulare Zugriffskontrolle :** Es müssen unterschiedliche Benutzerrollen zur Verfügung gestellt werden
- **Logging:** Sämtliche Konfigurationsänderungen müssen nachverfolgbar sein
- **Deaktivierung unsicherer Schnittstellen:** Kommunikationsschnittstellen ohne Verschlüsselung deaktivieren
- **Betriebssystem:** Das verwendete Betriebssystem sollte den neusten Stand aufweisen
- ...



Was können wir als Hersteller anbieten ?



Management von Aginode Switches
Empfehlung für sichere Einstellungen

mit Firmware V7.06 oder höher

KD975D14

INHALT

1. Empfehlung für die sichere Einstellung	2
1.1. Gegenüberstellung des Default- und Secure-Betriebsmodus	2
1.2. Einzelkonfiguration der sicherheitsrelevanten Parameter	2
1.3. Aktivierung einer sicheren Access Policy per Konfiguration	3
1.4. Aktivierung einer sicheren Access Policy per DIP Schalter	4
1.5. Weitere sicherheitsrelevante Einstellungen	4
2. Liste der verwendeten Ports beim Secure Mode	7
2.1. Port 22 TCP (SSH - Secure Shell)	7
2.2. Port 50271 TCP (SCP - Secure Copy)	8
2.3. Port 443 TCP (HTTPS)	10
2.4. Port 123 UDP (SNTP)	13
2.5. Port 161 UDP (SNMPv3)	14
2.6. Port 514 UDP (Remote SYSLOG) und Local Logging	16
2.7. Port 50266/50268 UDP (Switch Manager NexManV3)	17

Aginode Germany GmbH
1860
Bonnensbröcher Straße 2-14
41238 Mönchengladbach

support.lanactive@aginode.net
T + 49 2166 255 2017

- **Support:** Mit der Connect Com AG haben wir einen zuverlässigen lokalen Partner in der Schweiz
- **Schulungen:** Ein sicherer Umgang mit der eingesetzten Hardware ist der erste richtige Schritt
- **Der Leitfaden Empfehlung für sichere Einstellungen** unterstützt Kunden, Systeme mit einer sicheren Konfiguration auszustatten





aginode