Digitale Transformation in kritischen Infrastrukturnetzwerken

Inhaltsverzeichnis

Kritische Infrastruktur Konzept 2
Digitale Transformation 3
Digitale Transformation – Vorteile 3
Digital Transformation – Schwachstellen 3
Cyber Security Risk Mitigation 4
Wir stellen den Advanced Industrial Router VT AIR 300 vor 6
Use Cases 8
Öffentliche und private Netzbetreiber (Abbildung 3) 8
Wind Energy Anbieter (Abbildung 4) 8
Smart City (Abbildung 5) 9
Zusammenfassung 10

Kritische Infrastruktur Konzept

Kritische Infrastrukturen (CI) sind organisatorische und physische Strukturen und Einrichtungen, die für die Gesellschaft und Wirtschaft eines Landes von so entscheidender Bedeutung sind, dass ihr Scheitern oder ihre Verschlechterung zu anhaltenden Versorgungsengpässen, erheblichen Störungen der öffentlichen Sicherheit oder anderen dramatischen Folgen führen würde.

Kritische Infrastrukturen umfassen verschiedene private und öffentliche Sektoren wie Energie, Stromnetz, Wasser, sowie Gesundheit und öffentliche Verkehrsmittel, um nur einige zu nennen. Jedes Land hat seine eigenen Definitionen dafür, welche Sektoren für seine nationale Infrastruktur von entscheidender Bedeutung sind.

Die meisten dieser kritischen Infrastrukturen stellen hohe Anforderungen an die Sicherheit digitaler Informationen und den Informationsfluss innerhalb von Netzwerken. Einige Regierungen, wie z.B. in Deutschland das BSI, stellen sogar Sicherheitsrichtlinien und -anforderungen an Systeme.

Die NATO definiert beispielsweise kritische Infrastruktursektoren wie Energie, Verkehr, Wasser, öffentliche und rechtliche Ordnung und Sicherheit, chemische und nukleare Industrie usw., wie in Abbildung 1 dargestellt.

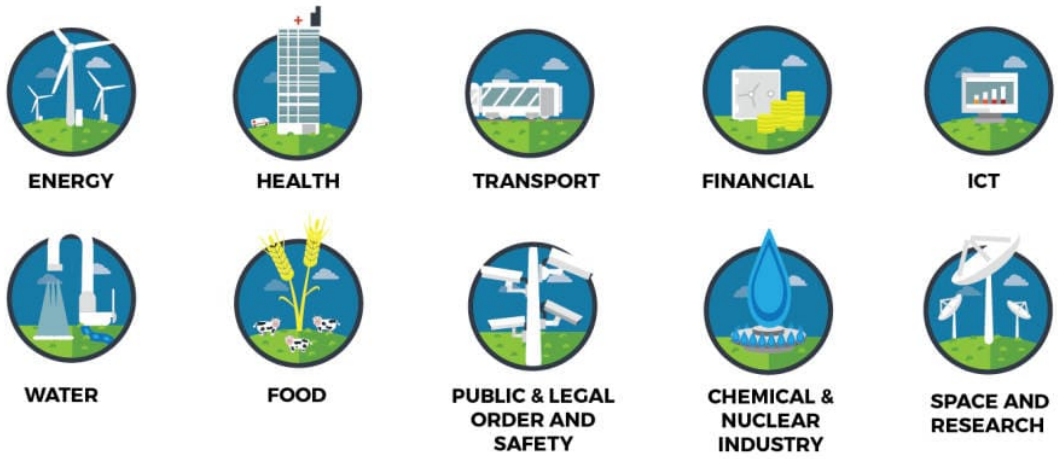


Abbildung 1: Kritische Infrastruktur Sektoren

Die Steigerung der Produktivität sowie der industriellen Praktiken bei gleichzeitiger Senkung der Kosten, der Wartung und des Betreibens von Systemen war der Hauptantrieb, der zu einem exponentiellen Wachstum bei der Einführung der neuesten intelligenten Technologien bei der digitalen Transformation kritischer Infrastrukturnetzwerke geführt hat. Diese Integration von erhöhter Automatisierung, verbesserter Kommunikation und Selbstüberwachung sowie intelligente Maschinen sind es, die die heutige digitale Transformation kennzeichnen.

Digitale Transformation

Um das Beste aus der digitalen Transformation herausholen zu können, sollte die Infrastruktur so konzipiert werden, dass sie die nachstehend beschriebenen Grundsätze unterstützt.

- **Konnektivität**: Maschinen sind über öffentliche oder private Leitungen verbunden, die verschiedene Technologien wie SFP, SHDSL, VDSL, LTE und RJ45 nutzen.
- **Sicherheit**: Kritische Systeme benötigen einen hohen Sicherheitsstandard, um sich vor Angriffen wie Denial of Service (DOS) oder Distributed Denial of Service (DDOS) sowie Hackern zu schützen.
- **Wartbarkeit**: Die Systeme haben die Fähigkeit, unabhängig zu arbeiten. Das Management sollte schnell und zentralisiert sein sowie kontinuierliche Updates durchführen, um einen hohen Sicherheitsstandard zu gewährleisten.
- **Schutz**: Zum Schutz kritischer Infrastrukturen sollten verschiedene Technologien eingesetzt werden, wie DDOS-Schutz, Intrusion Detection and Protection (IDS/IPS), Firewalls und VPNs.

Digitale Transformation – Vorteile

Die Hauptvorteile sind:

- **Verbesserte Produktivität und Effizienz**: Digitale Transformation ermöglicht schnellere Reaktionszeiten, während die Ressourcenallokation kostengünstiger und effizienter wird.
- **Erhöhtes Datensharing**: Machine-to-machine und System-to-System-Kommunikation ermöglicht es, dass Daten von einer Entität (wie ein Sensor) sofort eine Verbesserung über mehrere Systeme in der Infrastruktur ohne menschliche Eingriffe erzielt.
- **Mehr Flexibilität und Agilität:** Änderungen der Infrastruktur und Sicherheitsrisiken können schneller und flexibler bewältigt werden. Wartung und Maschinenautomation können sicher und über Fernverbindungen wie Leitstellen durchgeführt werden.
- **Return on Investment (ROI)**: Die Migration zu digitalen Netzwerken in kritischen Infrastrukturen erfordert Investitionen, sodass im Voraus Kosten entstehen. Die Kosten für Wartung und Sicherheit werden jedoch durch Automatisierung, Systemintegration, Datenmanagement usw. zukünftig drastisch sinken.

Digital Transformation – Schwachstellen

Obwohl die digitale Transformation kritischer Infrastrukturnetzwerke klare geschäftliche Vorteile bietet, sind die größte Herausforderung der Implementierung dieser Techniken die Sicherheitsrisiken. Die bisher betriebenen Technologien waren relativ isoliert oder sogar nicht digital. Die Integration/Konvergenz von IT (Information Technology) und OT (Operational Technology), die für die digitale Transformation unerlässlich ist, führte unter anderem dazu, dass Maschinensysteme und Industrielle Steuerungssystemes (ICSs) der Mehrheit von Cyberangriffen ausgesetzt werden.

Industrial Control System (ICS) ist ein allgemeiner Begriff, der Überwachungssteuerungs- und Datenerfassungssysteme (SCADA), Distributed Control Systems (DCS) und andere Steuerungssystemkonfigurationen wie programmierbare Steuerungen (SPS) umfasst. ICSs finden sich in der Herstellung, Verarbeitungsanlagen und kritischen Infrastrukturen, wie Kern- und Thermalanlagen, Wasseraufbereitungsanlagen, Stromerzeugung, Schwerindustrie, intelligente Städte und Verteilungssysteme. Dies macht sie zu sehr attraktiven Zielen für Angreifer, die oft durch finanziellen Gewinn, politische oder sogar militärische Ziele motiviert sind. Angriffe können staatlich gesponsert werden oder sie könnten auch von Konkurrenten ausgeübt werden, von Insidern mit einem bösartigen Ziel und auch von Hackern. Die meisten ICS-Geräte sind aufgrund von Schwachstellen in Hardware, Betriebssystemen und ICS-Anwendungen sowie in den ICS-Netzwerken von Natur aus weniger sicher gegen fortschrittliche Angriffe.

Grundsätzlich sind jedoch alle Geräte Cyber-Bedrohungen ausgesetzt. Forscher des Cybersicherheitsunternehmens Trend Micro und Experten der Polytechnischen Universität Mailand untersuchten, wie Hacker Sicherheitslücken in IoT-Geräten ausnutzen können, um als Gateway für den Einsatz von Malware, Spionage oder sogar Sabotage in Netzwerke einzubrechen. Außerdem hat das JSOF-Forschungslabor eine Reihe von Zero-Day-Schwachstellen in einer weit verbreiteten Low-Level-TCP/IP-Softwarebibliothek entdeckt, die von Track, Inc. entwickelt wurde. Die 19 Sicherheitsanfälligkeiten mit dem Namen "Ripple20" (https://www.jsof-tech.com/ripple20/) betreffen Hunderte Millionen von Geräten (oder mehr) und umfassen mehrere Sicherheitsanfälligkeiten bei der Ausführung von Remote-Code.

Die Risiken, die mit dieser Situation verbunden sind, sind hoch. Nur ein paar Beispiele: Daten könnten aus einem Drucker gestohlen werden, das Verhalten einer Infusionspumpe geändert oder industrielle Steuergeräte könnten zu Fehlfunktionen gebracht werden. Ein Angreifer könnte bösartigen Code jahrelang in eingebetteten Geräten verstecken. Eine der Sicherheitsanfälligkeiten könnte den Einstieg von außen in die Netzwerkgrenzen ermöglichen. und dies ist nur ein kleiner Vorgeschmack auf die potenziellen Risiken. Solche Erkenntnisse sind zu einem der Hauptgründe geworden, die die digitale Transformation in kritischen Infrastrukturen zurückhalten.

Cyber Security Risk Mitigation

Die Backend-Systeme von Kritischen Infrastrukturnetzwerken sind für das Routing verschiedener Datentypen zwischen Geräten und Anwendungen verantwortlich. Eine Möglichkeit, das Risiko von Cyber-Angriffen zu mindern, die erheblichen Schaden anrichten können, besteht darin, eine einfache, intelligente und erweiterbare Netzwerkinfrastruktur zu entwerfen. Ein typisches Netzwerk funktioniert dezentral und verteilt. Es besteht aus separaten Backend-Netzwerken, die mit dem öffentlichen Internet verbunden sind. Jedes Backend-Netzwerk erfordert Gateways, um zwischen bestimmten Drahtlosprotokollen und drahtgebundenen Protokollen und dem Internet zu kommunizieren.

Diese Gateways müssen Pakete an das Internet weiterleiten sowie Routing und Verarbeitung durchführen, bevor Daten an eine Anwendung übermittelt werden können. Darüber hinaus sollten Router der nächsten Generation als Gateways verwendet werden. Diese Router eignen sich für industrielle Umgebungen und bieten sowohl eine hohe Flexibilität im Netzwerkdesign durch verschiedene Schnittstellentypen als auch Schutz vor Cyber-Angriffen

durch integrierte Firewall-Software. Da Netzwerke der kritischen Infrastruktur normalerweise nicht von Kommunikationsexperten oder IT-Teams betrieben werden, sollten die Router einfach zu konfigurieren und einfach zu bedienen und zu warten sein.

Wir stellen den Advanced Industrial Router VT AIR 300 vor

Die Voleatech GmbH aus Deutschland, ein führender Anbieter fortschrittlicher Netzwerktechnologie (https://www.voleatech.de/), hat im Oktober 2019 den VT AIR 300 (https://www.voleatech.de/en/product/vtair300/) auf den Markt gebracht – einen innovativen, kompakten, robusten und flexiblen Industrierouter der nächsten Generation, der in Abbildung 2 dargestellt ist.

Abbildung 2: VT AIR 300

Der VT AIR 300 wurde speziell für ein anspruchsvolles industrielles Umfeld und seine Anforderungen entwickelt. Aufgrund seiner modernen Technologie (SHDSL, VDSL, LTE, SFP, RJ45) und seiner zahlreichen innovativen Lösungen ist der VT AIR 300 die nächste Generation von Industrieroutern, die auf der fortschrittlichsten ClearFog GT-8K-Familie von SolidRun Ltd. (https://www.solidrun.com/), einem weltweit führenden Entwickler von IIoT- und Netzwerk-Embedded-Systemen und der funktionsreichen, hochmodernen Firewall-Software VT AIR von Voleatech basieren.

Der VT AIR 300 ist maßgeschneidert für kritische Infrastrukturen und komplexe Industrieumgebungen, die durch den digitalen Wandel erneuert oder sogar komplett neu positioniert werden müssen. In der Netzwerktechnik markiert der intelligente Router den logischen Schritt ins digitale Zeitalter kritischer Infrastrukturen und 5G-Technologie – damit den Beginn moderner Netzwerktechnik.

Der VT AIR 300 bietet folgende wesentliche Vorteile:

- **Modulare Hardware**: Verschiedene Arten von optionalen physischen Schnittstellen und Funktionen, um das Gerät an die genauen Bedürfnisse des Kunden und der Implementierungen anzupassen. Der modulare Aufbau ermöglicht auch, die Gerätekonfiguration nach der Bereitstellung zu ändern.
- **Sicherheit immer auf dem neuesten Stand der Technik**: Dank modularer Softwarestruktur können verschiedene Komponenten des Systems individuell modifiziert und Sicherheitslücken sofort upgedatet werden! Tools wie Firewall, DDOS Protection und Deep Package Inspection IDS/IPS können bereitgestellt werden, um die Infrastruktur zu sichern. VPNs können zur Verschlüsselung des Datenverkehrs auf öffentlichen Leitungen (IPSec, OpenVPN, Wireguard) bereitgestellt werden.
- **VT AIR Software**: Ein funktionsreiches Firewall-Linux-basiertes System, das eine moderne, benutzerfreundliche, leicht verständliche und dynamische Web-Oberfläche in mehreren Sprachen bereitstellt, die es Benutzern ermöglicht, alle Einstellungen

einfach und bequem auszuführen. Ein zentrales Verwaltungssystem kann verwendet werden, um eine große Anzahl von VT AIR-Geräten einfach zu konfigurieren.

Der VT AIR 300 wird bereits erfolgreich von Energieunternehmen in Deutschland eingesetzt, um hochkritische Netzwerkinfrastrukturen zu sichern und zu verwalten.

Anwendungsfälle

Die folgenden Unterabschnitte enthalten Beschreibungen einiger Anwendungsfälle.

Öffentliche und private Netzbetreiber (Abbildung 3)

VT AIR – DSL und VPN für schnelle und sichere Netze
Kritische Infrastrukturen benötigen ebenso moderne wie innovative Netzwerktechnologien, um sich im Rahmen des digitalen Wandels zielgerichtet zu erneuern und den steigenden Sicherheitsanforderungen gerecht zu werden. Der VT AIR 300 bietet nicht nur SHDSL, VDSL, SFP und LTE, das System überzeugt auch dank seiner hohen Verschlüsselungstechnologie. Die innovative Firewall-Technologie ist zudem jederzeit nachrüstbar und dank Over-The-Air Updates immer auf dem neuesten Stand der Sicherheit.

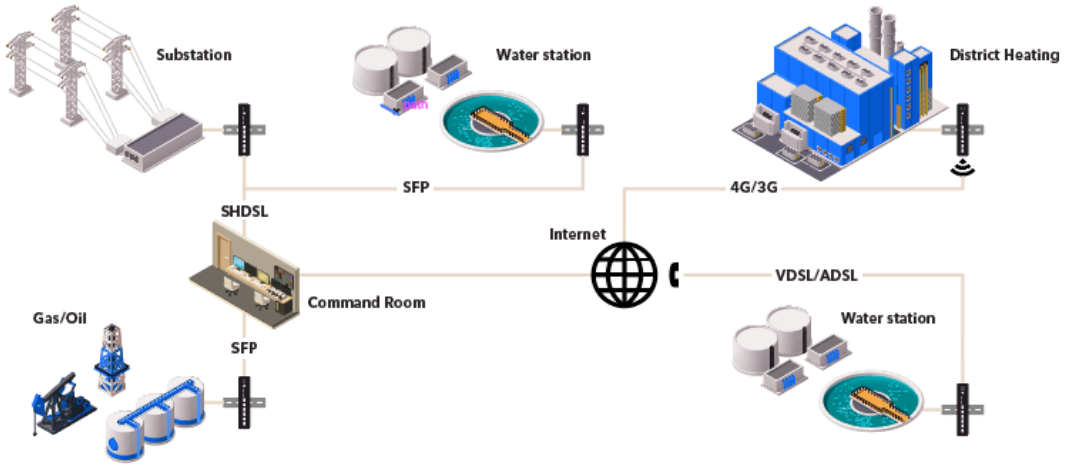


Abbildung 3: Netzbetreiber- and Energieversorgerimplementierung

Windenergieanbieter (Abbildung 4)

VT AIR – modular und nachrüstbar für höchste Anforderungen
Windenergie ist ein fester Bestandteil der Energiewende, die stetig und schnell vorantreibt. Gerade in einem solchen Umfeld ist es wichtig, innovative Netzwerktechnologie einzusetzen, die nicht nur höchsten Sicherheitsanforderungen genügt, sondern auch modular aufgebaut und jederzeit nachrüstbar ist. Das ist mit dem VT AIR 300 garantiert. Durch die modulare Softwarestruktur können einzelne Komponenten upgedatet und eventuelle Sicherheitslücken sofort geschlossen werden. Dank der Docker-Applikationen können eigene Anwendungen und Steuerungssoftware genutzt werden.

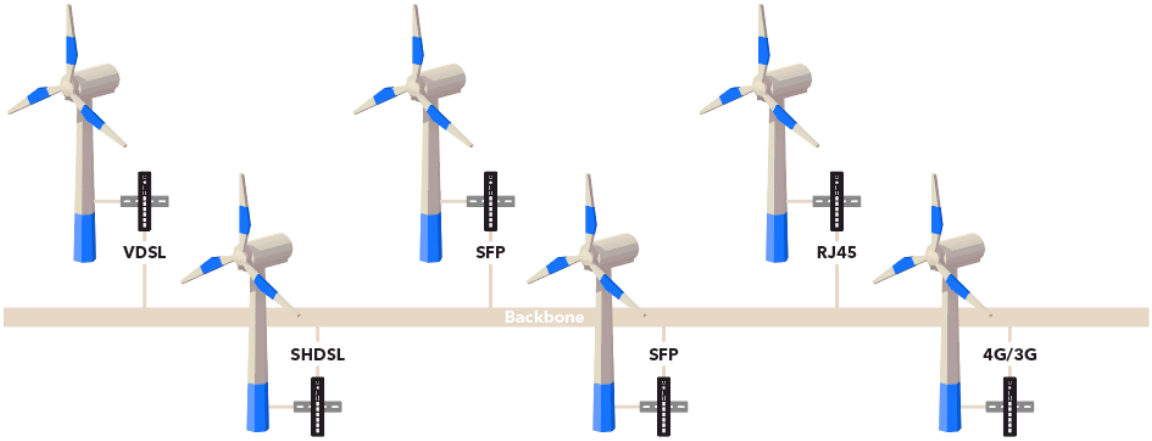
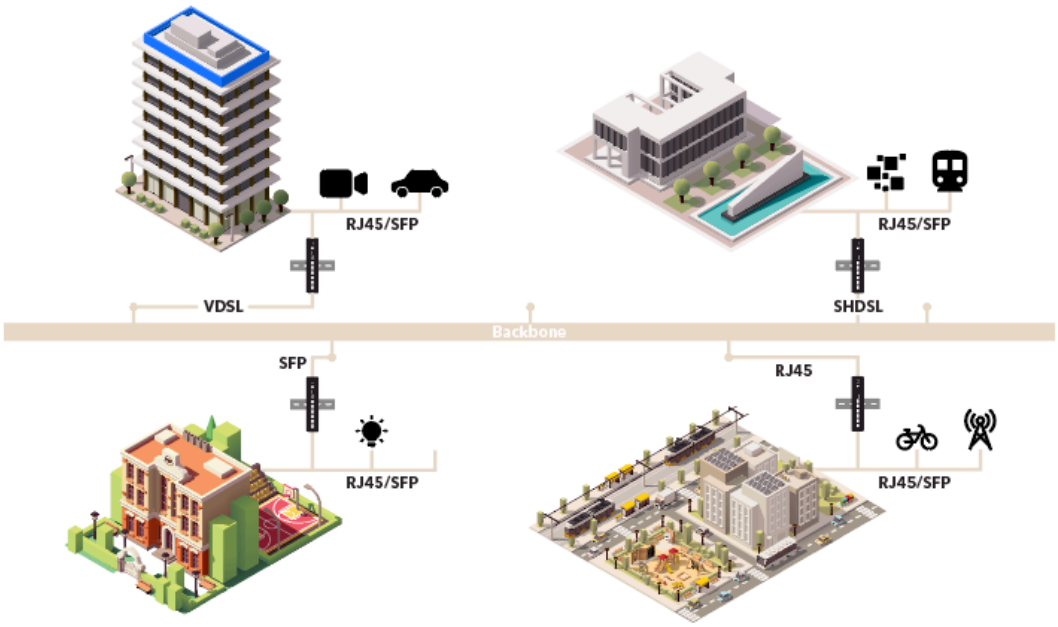


Abbildung 4: Windenergieanbieter

Smart City (Abbildung 5)

VT AIR – moderne Verschlüsselungsalgorithmen für mehr Sicherheit

Städte verändern ihren Charakter. Viele Metropolen werden sich in den kommenden Jahren zu Smart Citys wandeln und damit komplett vernetzt sein. Die Betreiber sind somit auf modernste Netzwerktechnologie angewiesen, wollen sie den damit einhergehenden und vermutlich stark anwachsenden Datentransfer absichern. VT AIR steht für hohe Verschlüsselung, Sicherheit und bietet zudem eine Hardware, die auch in komplexen Umfeldern mit hohen Temperaturen einsetzbar ist und somit das Backend der Metropole der Zukunft bildet.



Abbbildung 5: Smart City Implementierung

Zusammenfassung

Kritische Infrastrukturen wie Energie, Verkehr, Wasser, öffentliche und rechtliche Ordnung und Sicherheit, chemische und nukleare Industrie usw. sind von entscheidender Bedeutung für Gesellschaft und Wirtschaft. Ihr Versagen oder ihre Verschlechterung würde zu anhaltenden Versorgungsengpässen, erheblichen Störungen der öffentlichen Sicherheit oder anderen dramatischen Folgen führen. Die Steigerung der Produktivität bei gleichzeitiger Senkung der Kosten für Wartung und Betrieb sowie industrieller Praktiken haben zu einem exponentiellen Wachstum bei der Einführung der neuesten intelligenten Technologien bei der digitalen Transformation kritischer Infrastrukturnetzwerke geführt. Neben den klaren geschäftlichen Vorteilen ist die Herausforderung bei der Implementierung dieser Techniken das Sicherheitsrisiko aufgrund der IT- und OT-Integration in die industriellen Steuerungssysteme. Infolgedessen sind die kritischen Infrastrukturen, einschließlich aller "intelligenten" Geräte, Cyberangriffen ausgesetzt.

Das Risiko von Cyber-Angriffen kann durch einfache, intelligente und erweiterbare Netzwerkinfrastrukturen auf Basis von Routing-Gateways der nächsten Generation gemindert werden, da diese für industrielle Umgebungen geeignet sind und sowohl eine hohe Flexibilität im Netzwerkdesign (aufgrund verschiedener Schnittstellentypen) als auch Schutz vor Cyber-Angriffen durch integrierte Firewall-Software bieten. Der von Voleatech kürzlich eingeführte **VT AIR 300** Advanced Industrial Router basiert auf SolidRuns fortschrittlichster ClearFog GT8K-Familie und ist maßgeschneidert für kritische Infrastrukturen und komplexe Industrieumgebungen. Seine modulare Hardware und die funktionsreiche Firewall-Software machen ihn zum idealen Baustein in öffentlichen und privaten Energieversorgungsunternehmen, die DSL und VPN für schnelle und sichere Netzwerke benötigen. Darunter sind auch Windenergieanbieter, die modulare und nachrüstbare Systeme benötigen und intelligente Städte, die moderne Verschlüsselungsalgorithmen für mehr Sicherheit benötigen.

Über Voleatech GmbH

Voleatech hat sich von einem klassischen Startup zu einem führenden Anbieter fortschrittlicher Netzwerktechnologien entwickelt. Die Philosophie der Entwickler ist klar definiert: Für die Ingenieure der Voleatech GmbH liegt der Fokus auf den Kunden. Dies drückt sich in zwei Prinzipien aus: Einerseits muss Technologie innovativ sein, andererseits muss sie intelligent und intuitiv sein – nur dann hat der Kunde den größtmöglichen Nutzen. Voleatech investiert daher gezielt in innovative Zukunftstechnologien.

https://www.voleatech.de/

Über SolidRun Ltd.

SolidRun ist ein weltweit führender Entwickler von Embedded-Systemen und Netzwerk-lösungen, der eine breite Palette energie-effizienter, leistungsstarker und flexibler Produkte anbietet. Wir bieten einen Onestop-Shop für Entwickler und OEMs, -einschließlich kompletter Service von der Hardwareanpassung bis hin zu Software-Support, Produktbranding und Gehäusedesign. Unsere Mission ist es, die Anwendungsentwicklung zu vereinfachen und gleichzeitig Die Bereitstellungs-herausforderungen zu bewältigen und dadurch eine schnellere Markteinführung und geringere Kosten zu bieten.

https://www.solid-run.com/