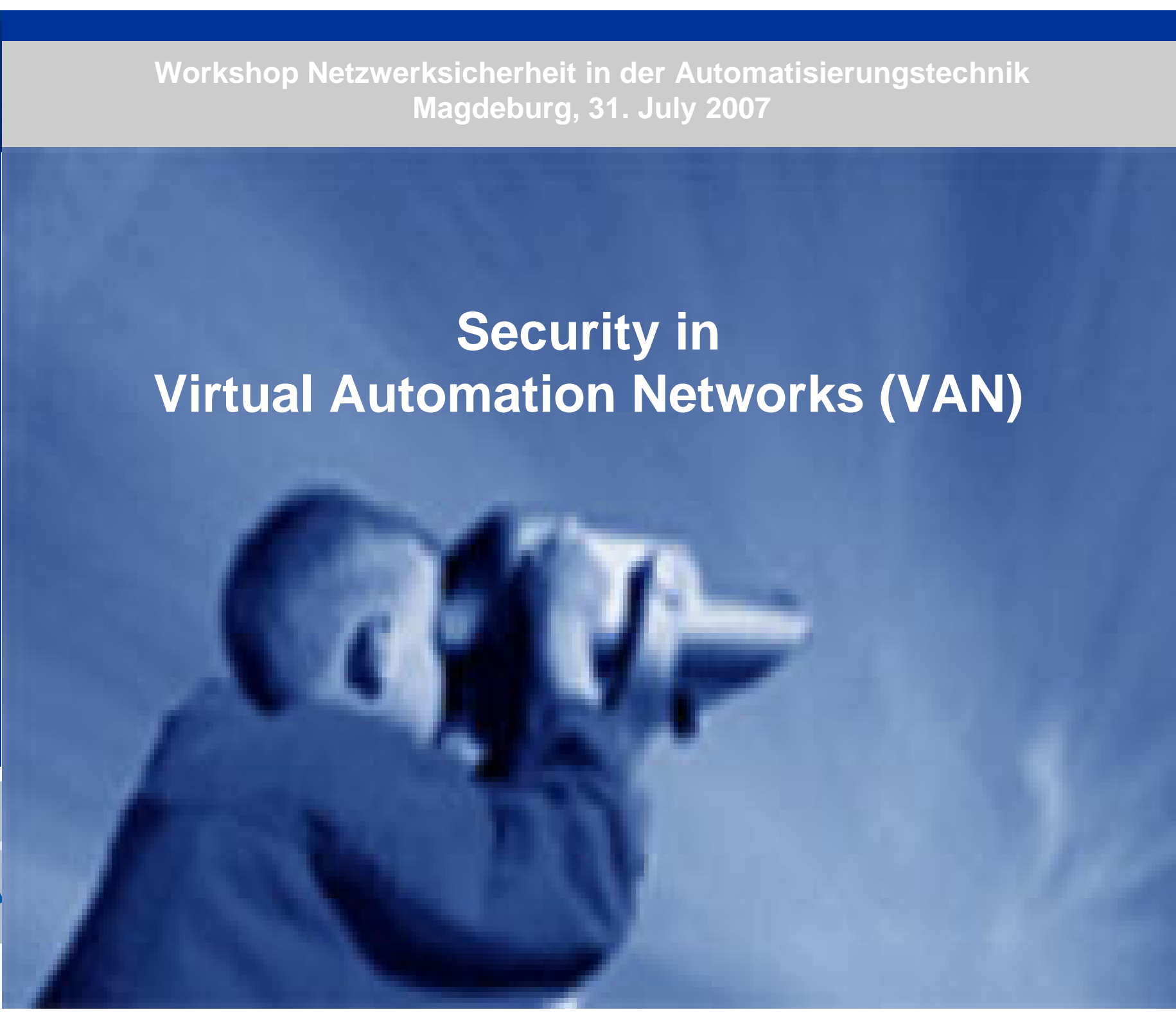




Workshop Netzwerksicherheit in der Automatisierungstechnik
Magdeburg, 31. July 2007

Security in Virtual Automation Networks (VAN)





Einstimmung

Wie lange darf Sicherheit dauern?

Wie bekommt man für neue Standards Siemens, Schneider Electric und Phoenix Contact an einen Tisch?

Ist Kommunikation deterministisch oder herrscht das Chaos?

Vertrauen Sie dem Draht?





Motivation

- Immer stärkerer Trend hin zu verteilten System in der Automatisierung
- Ethernet Technologien durchdringen immer mehr auch die Feldebene
- Immer mehr IT Standards aus der Office Welt dringen in die Industrie vor
- Komplexe Strukturen werden immer stärker in kleinere Einheiten mit mehr Intelligenz aufgesplittert
- Bedarf an höherer Flexibilität von Automatisierungssystemen
 - (Re-) Konfigurierung
 - (Neu-) Zusammenstellung
 - achieved with Plug-and-Play mechanisms and autonomous behaviour of these modules
- Nahtlose Integration aller Ebenen der Automatisierungspyramide
- Beeinflusst nicht nur einzelne Unternehmen sondern alle Partner einer Wertschöpfungskette





VAN Project – Vorstellung

- Projekt wird gefördert durch die Europäische Union

- 6. Rahmenprogramm



- Teil des Information Society Technology Programmes



- Zeitrahmen: Sept. 2005 – Aug. 2009

- Homepage: <http://www.van-eu.eu/>





VAN-Konsortium

14 Partner aus Deutschland, Italien, Tschechische Republik und Spanien

- Siemens, D (Koordinator)
- AUCOTEAM, D
- Brno University of Technology, CZ
- CARTIF, E
- Fidia, I
- HEITEC, D
- Ifak e.V., D
- M.C.M, I
- Phoenix Contact Electronics, D
- Politecnico di Milano, I
- Schneider Electric, F
- Teleport Sachsen-Anhalt GmbH, D
- Universität Magdeburg, CVS, D
- Forschungszentrum Karlsruhe, D





Generelle Ziele des Projektes

- Neue Möglichkeiten für die horizontale und vertikale Integration in der Automatisierung
- System-Integration über lokale und entfernte heterogene Netzwerke
- Dazu IT Lösungen für die Automatisierung anpassen und erweitern für:
 - Security,
 - Safety,
 - Real-Time,
 - Wireless
- Zusammenbringen von existierenden und aufkommenden IT-, Automatisierungs- und Telekommunikations-Technologien





Fokus und angestrebte Resultate

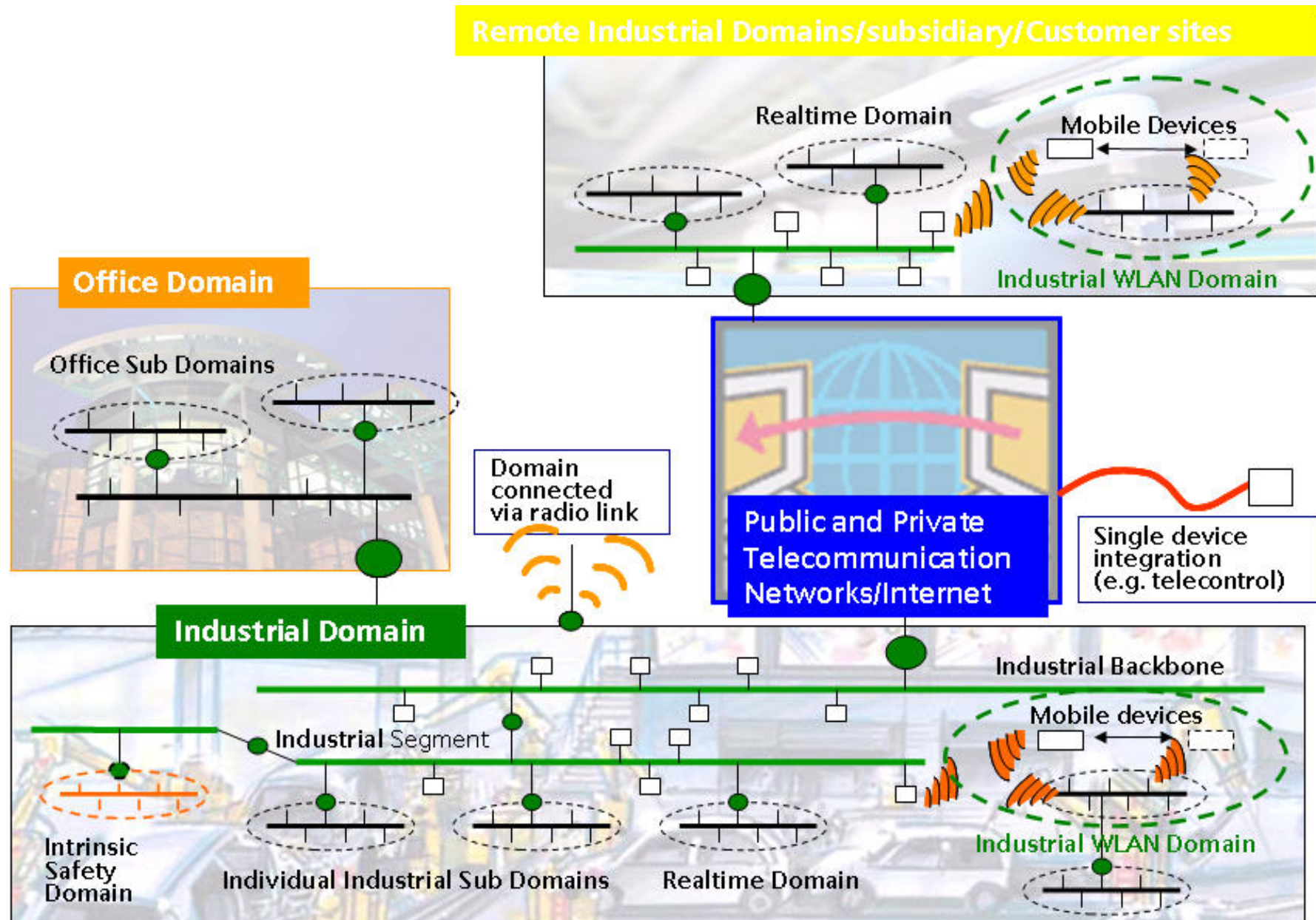


- Das VAN Projekt konzentriert sich auf einen wichtigen Teil eines flexiblen Automatisierungssystems: Das *industrielle Kommunikationsnetzwerk* zur lokalen oder entfernten Verbindung verteilter Automatisierungsfunktionen.
- Der Hauptfokus liegt auf der *Industriellen Kommunikation* mit den spezifischen Anforderungen an Realtime, Safety und Security.
- Die Lösungen sollen für *industrielle embedded Geräte* Anwendung finden
- VAN öffnet eine neue Dimension für einheitliches Networking von Produktionsprozessen



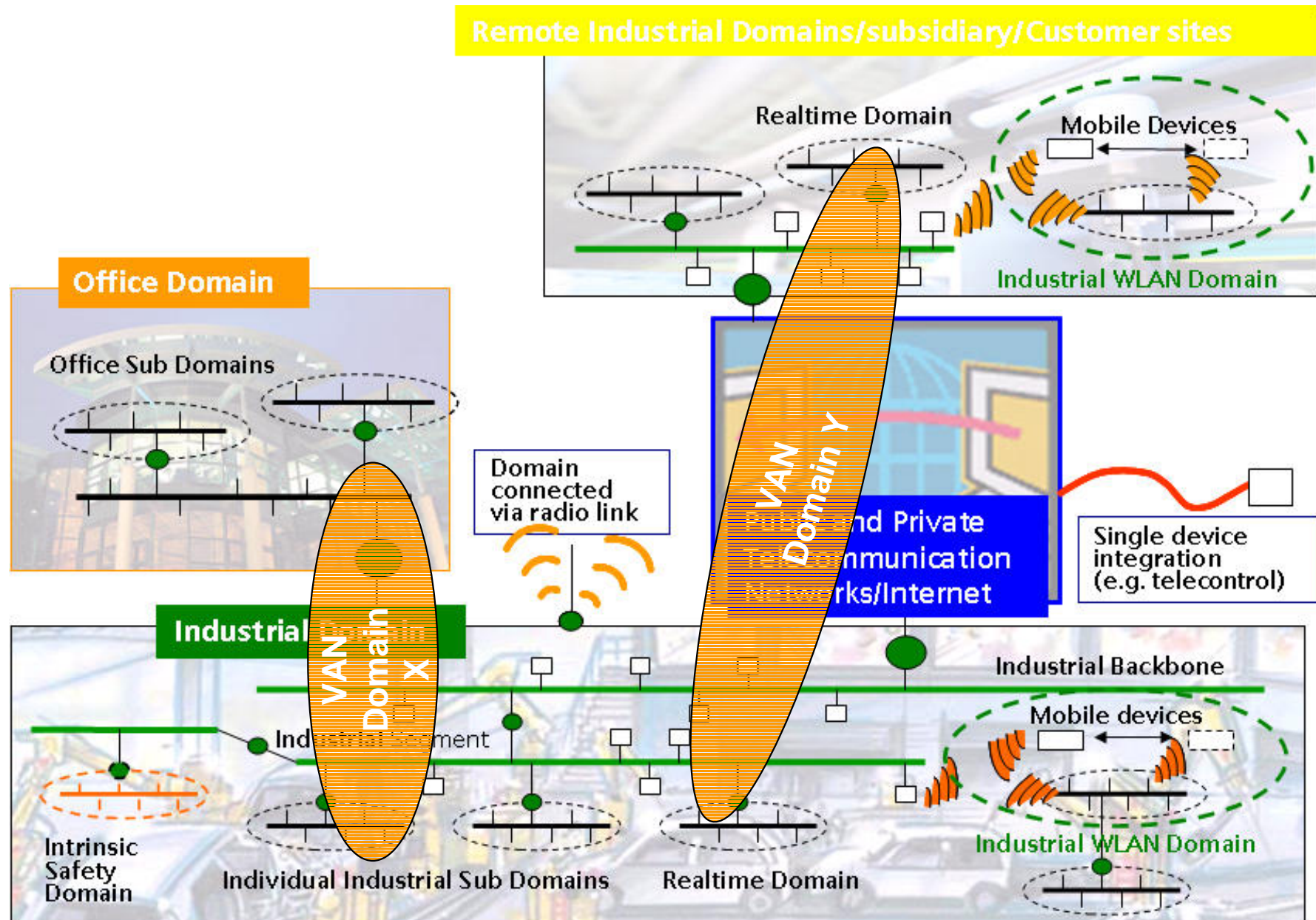


System Umgebung





Das Virtual Automation Network





VAN Security

- Security ist von Beginn an integraler Bestandteil der Arbeitsstruktur des Projektes
 - Eigenes Arbeitspaket
 - Breite Beteiligung
 - Starker Einfluss auf Architektur
- Fokus liegt auf dem Absichern der Kommunikationsverbindungen
- Interaktion mit der funktionalen Arbeit der anderen Arbeitspakete
 - Welche Anforderungen ergeben sich aus der gewünschten Funktionalität?
 - Welche Einfluss hat Security auf die angestrebten Lösungsschritte?
- VAN Security muss sich in die vorhandenen Sicherheitsstrukturen einbetten können





VAN Security Modell

- Evaluieren existierender Sicherheitstechnologien
- Identifizieren der für VAN relevanten Kommunikation und der sich daraus ableitenden zu schützenden Assets
- Bestimmung der Schutzziele für die Kommunikation
- Analyse zu den Bedrohungen und Risiken
- Identifizieren einzelner Maßnahmen für jeweiligen Szenarien
- Spezifizieren der Gesamtlösung für VAN
- Implementierung der Lösung
- Überprüfung der gefundenen Lösung



Standardprozess für Sicherheitslösungen angewendet
in der Frühphase einer Lösungsentwicklung





VAN Security Lösungen (1)

- Einsatz von SSL/TLS:
 - Verwendung bei der Kommunikation über Web Services
 - Kommunikation zum Aufbau des Virtuellen Netzwerkes, Konfiguration der Teilnehmer und den Tunnelaufbau
 - Nicht zeitkritische Metakommunikation
 - Bewährte Technologie, die bei den gegebenen Rahmenbedingungen ohne Veränderung übernommen werden kann

- Einsatz VPN:
 - Beim Übertragen von Daten zur Laufzeit des Systems
 - Soll die Verbindung über unsichere Gebiete schützen
 - Testmessungen:
 - Verschlüsselung hat wenig Einfluss auf das Gesamtverhalten
 - Verzögerung für die meisten Pakete akzeptabel, aber mitunter ist die maximal aufgetretene Latenz sehr groß





VAN Security Lösungen (2)

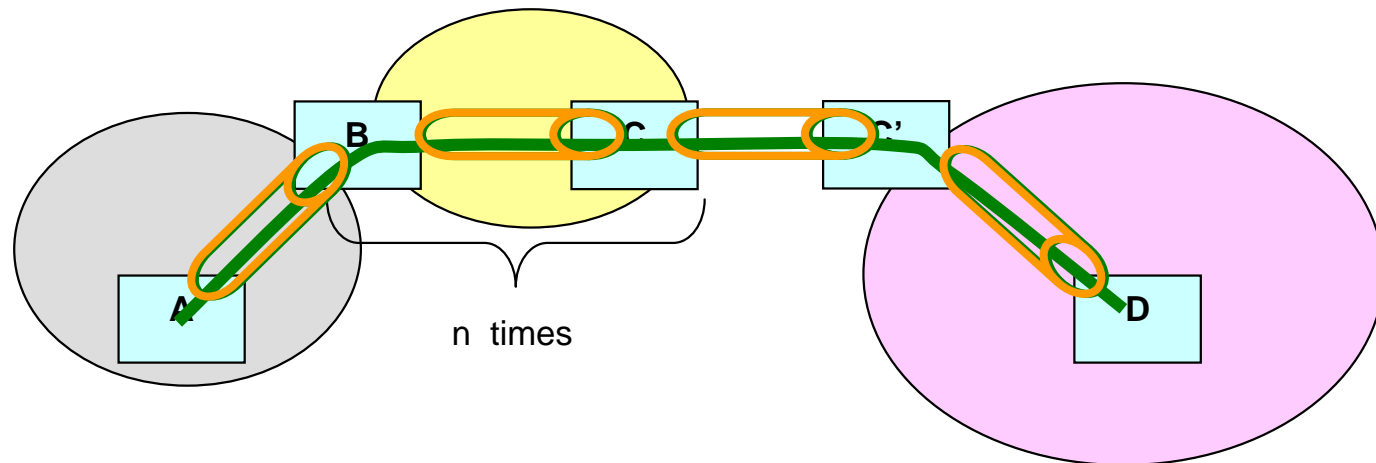
- Einsatz von Firewalls:
 - Bei Nicht-zeitkritischer Kommunikation – kein Problem
 - Firewalls zur Abgrenzung einer Zelle gegenüber dem Rest des Automatisierungsnetzwerkes – Zeitkritische Kommunikation
 - Testmessungen:
 - Der Durchsatz verringert sich nur unwesentlich bei einer geringen Zahl von Regeln, ab 200 Regeln eine merkliche Verringerung
 - Latenzzeit der meisten Pakete in akzeptabler Zeit, aber die maximale Verzögerung bei einem Teil der Daten ist sehr groß.
- Einsatz von ACL
 - Kontrolliert den Zugang zu Funktionen im VAN Gerät
 - Eine unumgängliche Schicht in der Gerätearchitektur
 - Jede Anfrage an ein Gerät wird kontrolliert, ob sie verarbeitet wird oder nicht.
(Quell-/Zielhost, aufgerufene Methode, angesprochenes Objekt, Zertifikat)





Was will das Security Arbeitspaket erreichen?:

- Absicherung der Web Services Kommunikation
- Erreichen der Routbarkeit von Feldbuskommunikation über öffentliche Netzwerke mit Hilfe der aufgebauten Tunnel



- Absichern der Laufzeittunnel über Authentifizierung und Verschlüsselung der Daten
- Spezifizieren einer geeigneten Sicherheitskonfiguration aller VAN Security Maßnahmen
- Entwicklung eines Security Layers für die VAN Geräte zur Kontrolle des Zugriffs
- Erste Ansätze zur Umsetzung von Security Maßnahmen als reine Hardwarelösungen





Bisherige Erkenntnisse

- Einsatz von vorhandener IT Security Technologie auch für viele Bereiche der industriellen Kommunikation möglich
 - Es hängt viel von der geeigneten Implementierung und Konfigurierung ab
 - Definierte Use Cases zeigen vielfältige Anwendungsszenarien
- Netzwerkverhalten der Betriebssystemelemente hat größeren Einfluss auf das Kommunikationsverhalten als zusätzliche Sicherungsmaßnahmen
- Es muss mit dem statistischen Verhalten umgegangen werden
- Sicherheit ist immer die Gesamtlösung des unternehmensweiten Security Konzeptes





investigation

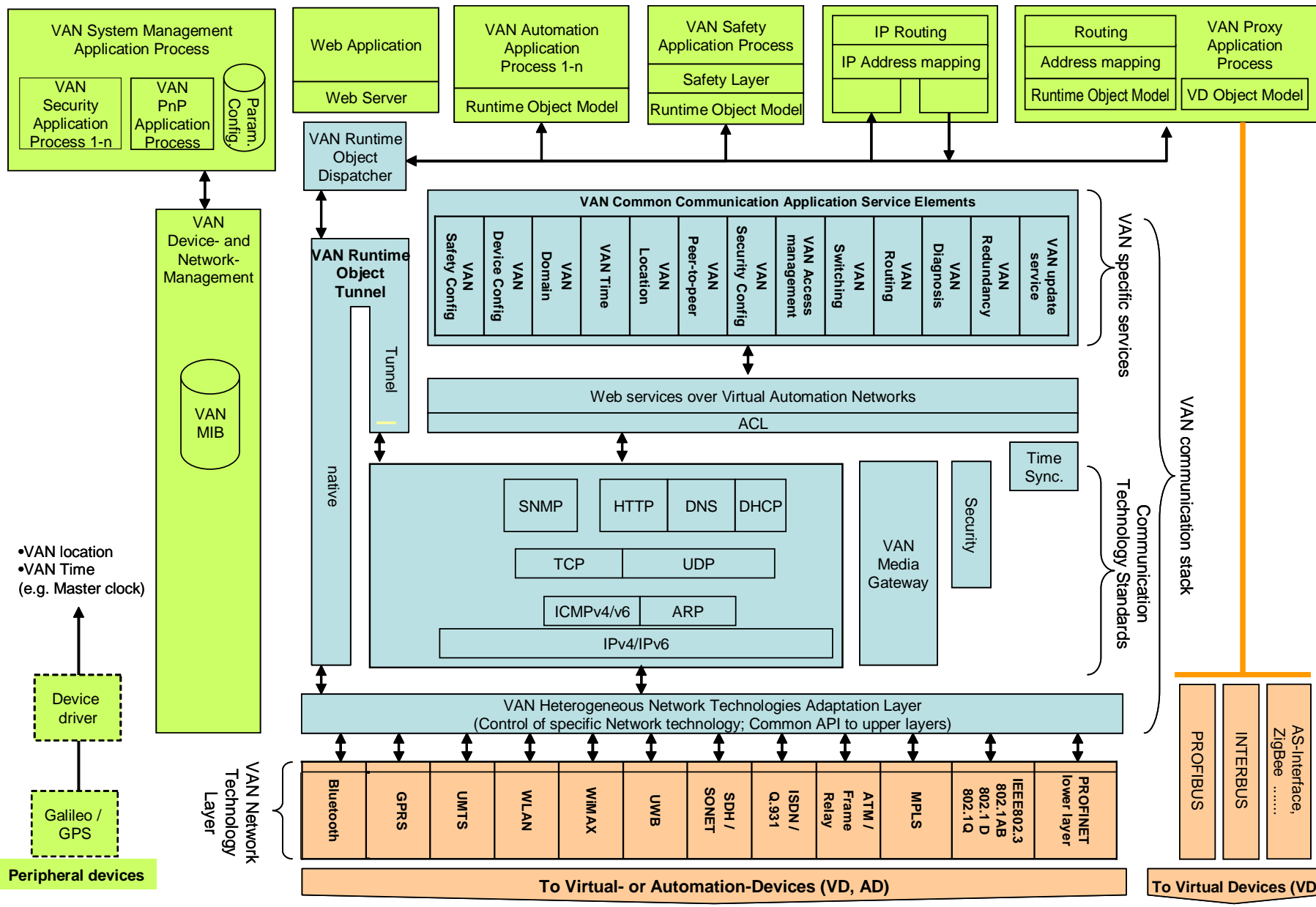
for future communication

**Vielen Dank für das
Interesse !**





VAN Device Architecture





Performance-Erfahrungen

