ComConsult Research

Der Netzwerk Insider

Februar 2006

Technologie Information für die Ausbildung zum ComConsult Certified Network Engineer

Schwerpunktthema

Gefahrenmeldetechnik und Objektüberwachung über IP-basierende Netze

von Dipl.-Ing. Hartmut Kell

Nachdem das IP-Protokoll den Bereich der Sprachkommunikation erfolgreich für sich gewinnen konnte und auch im industriellen Bereich nicht mehr aufzuhalten zu sein scheint, steht die nächste Eroberung an: Die Gefahrenmeldetechnik und Objektüberwachung. Dieses bisher durch klassische Analogtechniken dominierte Territorium wird im Sinne der Konvergenz moderner Netzwerke in Zukunft verstärkt von IP-basierenden Techniken beherrscht werden. Neben neuen Lösungsansätzen und der Verdeutlichung der heutigen technischen Grenzen ist eine sicherheitstechnische Bewertung dieser Techniken zwingend erforderlich.

Erstaunlicherweise hält dieses Thema in den Publikationen der Netzwerkspezialisten bisher nur wenig Einzug, anders dagegen geht die Gruppe der Spezialisten an das Thema heran, die für die Sicherheit eines Gebäudes verantwortlich sind. Hier wird sich bereits seit längerem in Form von Veröffentlichungen und Seminaren mit der für diese Gruppe „herannahenden“, neuen Technik beschäftigt. Ähnlich zu den bereits genannten Einführungen von IP in der Industrie und bei der Sprachkommunikation wird es also zwei Gruppen geben, die „IT-Spezialisten“ und die „Überwachungsspezialisten“. Jede Gruppe für sich verfügt über elementares, zur Nutzung der neuen Technik notwendiges Wissen und beide Gruppen müssen aufeinander zugehen.

weiter auf Seite 25

Zweitthema

RFID-Lösungen, große Architekturen für kleine Chips

von Dipl-Ing. Frank Lange-Lietz

Radio Frequency Identifikation (RFID) entwickelt sich zu einer bedeutenden Technologie bei der Verfolgung und Identifizierung von Produkten und Objekten in Supply-Chains sowohl global und weltumspannend, als auch in abgekoppelten, geschlossenen Produktionsabläufen. Immer mehr große Handelsorganisationen setzen die RFID-Technologie ein, um ihre Paletten und Container auf ihrem logistischen Weg durch Versandlager, Center und Niederlassungen zu identifizieren und zu managen. Aber nicht nur in der traditionellen Supply-Chain wird RFID-Technologie eingesetzt. Im Bereich der Instandhaltung werden RFID-Tags, wie man die Information speichernden Chips nennt, an Maschinen und Anlagen angebracht, um Wartungsvorgänge zu unterstützen und zu optimieren. In anderen Umgebungen werden RFID-Tags zum Lokalisieren von Objekten eingesetzt. Auch Zugangssysteme, in denen Plastikkarten mit eingebautem RFID-Tag Türen öffnen, sind weit verbreitet. RFID-Systeme finden wir schon seit längerem in unserer täglichen Umgebung und Analysten sind mehrheitlich optimistisch was die weitere Verbreitung und den Einsatz von RFID-Systemen betrifft.

weiter auf Seite 9

Top Veranstaltung

IT-Sicherheits-Forum 2006

auf Seite 18

Zum Geleit

Konsumenten verändern die Informationstechnik

auf Seite 2

Report des Monats

Fehlersuche in konvergenten Netzen

auf Seite 20

Zum Geleit

Konsumenten verändern die Informationstechnik

Die IT-Märkte für Unternehmen stagnieren weltweit und haben ihre Sättigung erreicht. Zwar gibt es vereinzelte Technologiebereiche mit neuen Entwicklungen wie IP-Telefonie, RFID oder Wireless, doch unter dem Strich sind die Jahre des starken globalen IT-Wachstums vorbei. So kann es nicht überraschen, dass die großen Hersteller dieser Branche, deren Aktienwert auf dem Spiel steht, immer stärker nach neuen Märkten suchen.

IT-Technologie wird Konsumer-Technologie, daran gibt es kaum noch einen Zweifel. Die Keynote von Bill Gates/Microsoft auf der Consumer Electronic Show CES Anfang Januar und parallel die Keynote von Steve Jobs/Apple auf der MacWorld in San Francisco haben deutlich gezeigt, wohin der Zug fährt.

Die Auswirkungen auf den Unternehmens-Markt sollten nicht unterschätzt werden. So wird Windows Vista/Vienna wohl deutlich mehr neue Funktionen beinhalten, die sich am Endverbraucher orientieren. Für die Unternehmen muss dies kein direkter Nachteil sein, doch sollten die Hoffnungen auf starke funktionale Verbesserungen für Unternehmen nicht zu hoch aufgehängt werden.

Der unglaubliche Erfolg von Apple hat im Endeffekt die ganze Branche zum Umschwenken bewegt. Microsoft auf der einen Seite, Sony auf der anderen und Google und Yahoo dazwischen, alle folgen dem von Apple gesetzten Trend. Von den 5,6 Mrd. $, die Apple im letzten Quartal umsetzte, stammen mehr als 50% aus dem iPod und iTunes Geschäft. Wurde der Verkauf von Songs im Apple-iTunes-Shop am Anfang belächelt und verhöhnt, so gilt dies nun als der zentrale Megatrend. Nach 800 Millionen verkauften Songs bei Apple spekulieren die ersten Unternehmen bereits über das Ende der CD.

Dabei geht es im Detail gar nicht um die Songs. Apple hat das geschafft, woran ganze Industrien und vor allem alle weltweit führenden Provider seit Jahren arbeiten. Und zwar wurde ein im Internet handelbarer Content geschaffen. Damit wurde der Nachweis erbracht, dass das Internet sehr wohl in der Lage ist, neue Formen von Inhalten und Diensten zu vermarkten. Für viele Unternehmen, auch

für die deutsche Telekom, ist dies schlicht eine Überlebensfrage. Der letzte Auslöser, der noch fehlte, war das Angebot von Video im Web, das Apple im Oktober 2005 auf den Markt brachte. Auch hier glaubte lange Zeit niemand, dass dies erfolgreich sein könnte. Der Durchbruch kam mit der Vermarktung von Fernsehserien für 2,99 $ (es leben die „Desperate Housewifes“). Auf einmal wurde klar, dass die Konsumenten bereit sind, diesem Weg zu folgen.

Seit Ende 2005 hat sich damit die zentrale Botschaft der Informationstechnik für die nächsten Jahre gefestigt: „Anything you want, any time, on any device“. Nahezu alle großen Anbieter bauen zur Zeit ihre Portale zum Kauf von Videos, Fernsehsendungen und Musik auf und orientieren sich dabei am Erfolgsmuster von Apple. Den Schlüssel zum Marktdurchbruch sehen die meisten Anbieter weltweit in der Vermarktung von Sportübertragungen im Internet. Jeder versucht zur Zeit, an dieser Stelle exklusive Inhalte zu schaffen. So kann der Deal der deutschen Telekom mit dem Erwerb der Rechte zur Vermarktung von Bundesligaspielen über das Internet nicht wirklich überraschen. Es kann in der Tat der geniale Schachzug sein, der die Marktanteile der Telekom sichert. Man kann erwarten, dass nur direkte Telekom DSL-Kunden in den Genuss dieser Spiele kommen werden. Je nach Preis kann die Telekom damit deutlich gegenüber den anderen Providern punkten. In den USA läuft geradezu eine Vertragsschlacht um die Übertragungsrechte für Basketball, Baseball usw.

Was bedeutet dies für die IT-Infrastrukturtechnik? Im Endeffekt brauchen Konsumenten, die diesem neuen Trend folgen wollen, zwei Kernelemente:

- Zugang zu einem sehr schnellen Internet (hier sind jetzt 50 Mbit/s HDTV-Leistung das Maß der Dinge, dies gilt für jeden Konsumentenhaushalt)
- Eine Übertragungstechnik, um die Inhalte im eigenen Haushalt an die verschiedenen Endgeräte zu bringen
- Ein entsprechend dafür optimiertes Endgerät

50 Mbit/s pro Haushalt sind kein Aprilscherz. Schon seit Jahren wird auf unseren Kongressen von Dr. Kauffels vorgerechnet, dass 100 Mbit/s-Ethernet pro Haushalt und Abschaffung der bisherigen digitalen Hierarchie bei den Providern der unter dem Strich wirtschaftlichste Weg ist.

Nun ist auf der wirtschaftlichen Seite die Art der Migration dorthin in Kombination mit den Auflagen der Regulierungsbehörde entscheidend. Doch weltweit laufen zur Zeit die Projekte an, die aus dem bestehenden Internet eine neue Infrastruktur schaffen, die bis 2010 oder 2012 eine derartige Leistung in jeden städtischen Haushalt bringen kann.

Das passt zeitlich gut zum Ende des analogen Fernsehens 2010. Im Moment sieht man jedenfalls das so genannte Triple-Play aus Internet, Telefon und Fernsehen aus einer Hand als den stärksten strategischen Schlüssel, den die Anbieter aufbauen können.

Für die Unternehmen ist aber gerade diese Entwicklung im Internet mehr als spannend. Endlich kommen wir in den Zustand, den wir seit Jahren vorhersagen. Die Grenze zwischen LAN und WAN wird schwammig, absolute Standortneutralität ist das Ergebnis. In Zukunft wird nur noch die wirtschaftliche Berechnung der Betriebskosten für einen Standort entscheidend sein. Datacenter im Web als Ablösung der bisherigen Rechenzentren und zentralisierte IP-Telefonie mit lokalen Zugangs-Gateways sind die entsprechenden Trends.

Konsumenten verändern die Informationstechnik

Die Lücke zwischen Internet und Endgerät wird für den Konsumenten durch IEEE 802.11n, den neuen Wireless-Standard, geschlossen. Er ist das perfekte Beispiel dafür, welche Rolle die Anforderungen von Unternehmen an neue Technologien spielen: schlicht gar keine mehr. 11n hat nur ein Ziel. Dies ist die Umsetzung einer stabilen und HDTV-fähigen Wireless-Technik in Kosumenten-Haushalten. Niemand hat etwas dagegen, wenn Unternehmen diesen Standard auch nutzen, aber wirklich wichtig ist es nicht. Dies wird durchaus spannend werden. Eine stabile Infrastruktur für Konsumenten, die Telefon, Fernsehen und andere Inhalte im Haushalt erst möglich macht, ist technisch durchaus sehr hochwertig. Die Aussage, Wireless-Konsumententechnik wäre minderwertig und der Enterprise-Technik weit unterlegen, stimmt schon lange nicht mehr. In Zukunft wird so noch weniger stimmen. Damit werden die Preise des Enterprise-Marktes stark unter Druck geraten. Die heutigen Wireless-Enterprise-Produkte sind mindestens 70% zu teuer bezogen auf den Listenpreis. Das wird sich ändern. Die Antwort der Wireless-Enterprise-Hersteller sind Wireless-Switches, die eine Kerneigenschaft haben. Sie sind teuer und halten den alten und schönen Enterprise-Aufpreis weiter aufrecht. Aber es ist erkennbar, dass dies nicht funktionieren wird. Auch diese Preise werden dem Druck des Konsumer-Marktes nicht standhalten.

Die Endgeräte-Technologie ist parallel auf dem Weg zum Konsumer. Der Ausblick auf Windows Vista/Vianna, den Bill Gates in seiner Keynote gegeben hat (kann über die Microsoft-Site abgespielt werden), belegt dies. Auch hier ist Apple der Wegbereiter. Mit OS X in Kombination mit iLife hat Apple eine Endgeräte-Technologie geschaffen, die es jedem Konsumenten ermöglicht, bisher für unmöglich gehaltene Dinge an seinem PC zu tun. Mit iLife Version 6 hat Apple nun erneut einen Standard gesetzt. Das seit 2 Wochen in Auslieferung befindliche Softwarepaket ermöglicht den perfekten Umgang mit Musik, Videos, Fotos bis hin zur eigenen Website-Gestaltung auf Konsumenten-Ebene. Für professionelle Anwendungen ist die Funktionalität allerdings nicht in jedem Fall ausreichend (komischerweise haben gerade iPhoto und iTunes hier Mängel, da sie eine zentrale Verwaltung von Content nur wirklich eingeschränkt unterstützen).

Leider ist diese schöne neue Content-Welt nicht so heil wie sie aussieht. Der Markt zerstückelt sich zur Zeit. Jeder Content-Besitzer schließt Exklusiv-Verträge mit Content-Providern. Im Ergebnis kann der Konsument seinen Bedarf nur über eine Menge von Providern decken. Die Übersicht ist im Moment sehr gering. Und hier kommt nun Google ins Spiel. Wenn man nicht weiß, wo man was finden kann, benutzt man eine Suchmaschine. So ist Google auf dem Weg zur weltweit führenden TV, Video und Musik-Programmzeitschrift.

Konsumenten verändern die IT-Technik. Wie weit wird das gehen? Welche Auswirkungen hat das für die Unternehmen? Wie investitionssicher sind einzelne Technologiebereiche noch? Dies wird der Inhalt der diesjährigen Keynote zum Netzwerk-Redesign Forum sein. Ich würde mich freuen, Sie dort zur Keynote begrüßen zu können.

Ihr
Dr. Jürgen Suppan

Top-Kongress

Netzwerk-Redesign Forum 2006

Die ComConsult Akademie veranstaltet vom 27. - 30. März das Netzwerk-Redesign Forum 2006.

Mit den wachsenden Anforderungen an Netzwerke hat sich das Design moderner Netzwerke immer weiter gewandelt. Im Wesentlichen basiert dieser Wandel auf 5 Kernfaktoren:

- Erhöhte Leistung in Kombination mit erhöhter Verfügbarkeit
- Vorbereitung auf IP-Telefonie (Voice-ready) und weitere neue IP-basierte Dienste
- Architektonische Integration von WLANs
- Sicherheit in mehreren Stufen auf Netzwerk-Ebene
- Vorbereitung auf Service-Management für ausgewählte Services

Nachdem Netzwerk-Produkte in den letzten Jahren im Kern immer ähnlicher wurden, laufen sie angesichts dieser Bedarfssituation wieder deutlich auseinander. Die Hersteller wählen zum Teil stark voneinander abweichende Lösungs- und Design-Ansätze.

Unsere Top-Veranstaltung des Jahres 2006 analysiert die aktuellsten Entwicklungen der Netzwerk-Technologien und bewertet Marktrends, Hersteller-Strategien und Produktentwicklungen. Wir blicken für Sie hinter die Kulissen, geben Erfahrungsberichte aus Top-aktuellen Projekten und bewerten die Praxis-Relevanz der neuesten Trends.

Am 4. Tag bieten wir den Teilnehmern Ein-Tages-Intensiv-Trainings zu ausgesuchten Top-Themen. Dabei werden der Stand der Technik und der optimale Betrieb wichtiger Themen über den ganzen Tag intensiv evaluiert. Sie können zwischen folgenden Intensiv-Trainings wählen:

- SIP in der Analyse: auf dem Wege zur offenen IP-Telefonie?
- Wireless LAN in Produktion und Logistik
- Quality of Service

Fax-Antwort an ComConsult 02408/955-399

Anmeldung

Netzwerk-Redesign Forum 2006

Ich buche den Kongress
Netzwerk-Redesign-Forum 2006
vom 27.03. - 30.03.06 in Königswinter

mit „Ein-Tages-Intensiv-Training“
☐ SIP in der Analyse: auf dem Wege zur offenen IP-Telefonie?
☐ Wireless LAN in Produktion und Logistik
☐ Quality of Service
zum Preis von € 2.190,- zzgl. MwSt.

☐ **ohne „Ein-Tages-Intensiv-Training“**
zum Preis von € 1.790,- zzgl. MwSt.

☐ **mit Report**
„Netzwerkdesign-Wettbewerb 2005“
zum Preis von nur € 210,- zzgl. MwSt.

☐ **mit Report**
„Sicherheit in Enterprise-Netzen durch den Einsatz von 802.1X“
zum Preis von nur € 338,- zzgl. MwSt.

☐ **ohne Report**

☐ Bitte reservieren Sie für mich ein Hotelzimmer
vom_____bis_____06

Buchen Sie über unsere Web-Seite
www.comconsult-akademie.com

Vorname _____ Nachname _____

Firma _____ Abteilung _____

Telefon _____ Fax _____

Straße _____ PLZ,Ort _____

eMail _____ Unterschrift _____

Programmübersicht: Netzwerk-Redesign Forum 2006

Montag, den 27.03.2006

9:30 bis 12:30 Uhr

Top-Analyse unseres internationalen Labors: Internationale IT-Trends und Auswirkungen auf Netzwerke und Infrastrukturen

- Neue IT-Architekturen und ihre Anforderungen
- Der Konsumer-Markt und seine Auswirkungen auf Client, Betriebssystem, Software
- Globalisierung und die Konsequenzen für Kommunikations-Architekturen
- Strategien ausgewählter Hersteller: Cisco, IBM, Microsoft, Siemens
- Moderne Technologien in der Trend-Analyse:
  - Speicher • Server/Datacenter
  - Intelligent Networks / Virtualisierung von Ressourcen im Netzwerk
  - IP-Telefonie • Kollaboration: Teamwork im Netzwerk
  - RFID, Architekturen und die Integrations-Aufgabe
  - Logistik-Anwendungen im Netzwerk
  - Aktuelle Netzwerk-Technologien und der Trend
  - Sicherheits-Architekturen für vernetzte Systeme
- Ausblick auf die internationale Entwicklung und die Konsequenzen für den deutschen Markt

Dr. Jürgen Suppan, ComConsult Research

14:00 bis 15:30 Uhr

Wireless-Technologien - wohin geht der Weg? Investitionssicherheit im Wettstreit von IEEE 802.11n und WiMax

- Aktuelle Wireless-Standards und ihre Vor- und Nachteile
- Konsumer- kontra Enterprise-Markt: wer bestimmt die Produkte
- IEEE 802.11n in der Analyse: Leistung + Grenzen eines neuen Standards
- WiMax: Vorteile der Wireless-Megatechnik
- IEEE 802.11n kontra WiMax: wohin geht der Weg
- Investitionssicherheit mit Wireless-Technologien: was ist zu tun?
- Wireless-Architekturen der Zukunft: die neue Wireless-Hierarchie
- Konsequenzen für die Zukunft: wie Netzwerke in 5 Jahren aussehen können
  - Campus-Design
  - Integration von Servern und Speicher
  - Distribution
  - Desktop-Bereich
- Fazit: Handlungsempfehlungen

Dr. Franz-Joachim Kauffels, Unternehmensberater

16:00 bis 17:30 Uhr

Netzwerk-Redesign 2006: Alternativen, Aufwand, Wirtschaftlichkeit

- Gründe für ein Redesign
- Bewertung bestehender Netzwerke und Designs
- Neue Technologien und ihr Einfluss auf Design-Entscheidungen
- Optimierung von Konvergenz-Zeiten
- Leistungsspektrum moderner Switch-Produkte
- Grundsätzliche Design-Alternativen
- Campus-/Backbone-Design im Umfeld konvergenter Netzwerke
- Design-Konzepte im Vergleich: der neue Cisco Campus-Guide in der Nutzbarkeits-Analyse
- Fallbeispiele und Empfehlungen

Dipl.-Inform. Petra Borowka, Unternehmensberatung Netzwerke UBN

10:30 - 11:00 Uhr Kaffeepause
12:30 - 14:00 Uhr Mittagspause
15:30 - 16:00 Uhr Kaffeepause
ab 18:00 Uhr Happy Hour

Dienstag, den 28.03.2006

9:00 bis 10:00 Uhr

Configuration Management Data Base CMDB: Optimierung des Konfigurations-Managements von Netzwerken

- CMDB als Basis zentralisierter Konfigurations-, Sicherheits- und Management-Architekturen
- ITIL und CMDB: vom Leitfaden zur Lösung
- Praktische Anforderungen
- Alternativen zur Umsetzung
- Automatisierung als logische Folge:
  - Spezialthema Automatisierung: Generierung aus einer CMDB
  - Spezialthema Sicherheit: Zugangspflege der Netzwerk-Plattform automatisiert mit Hilfe der CMDB
  - Spezialthema Management: Konfigurationspflege der Management-Plattform auf Basis der CMDB
- Kosten und Betrieb
- Bewertung und Ausblick

Dipl.-Kfm. Martin Woyke, ComConsult Kommunikationstechnik GmbH

10:00 bis 10:30 Uhr

Standardisierung und Technologie-Entwicklung:

- Was passiert aktuell bei IEEE, was ist neu, wie relevant ist es?
- Positionen der Hersteller
- Aktuelle Standardisierungs-Arbeiten
  - 802.3an 10GBASE-T • 802.3aq 10GBASE-LRM
  - 802.3as Frame Extension • 802.3at Power oE Plus
  - 802.3ap Backpanel Ethernet
  - 802.3ar Congestion Management • Residential Ethernet
- Einschätzungen und Empfehlungen

Dipl.-Ing. Thomas Schramm, Hirschmann GmbH

11:00 bis 11:45 Uhr

Anforderungen an die Netzwerk-Infrastruktur für 10 Gig-Ethernet und für zukünftige Anwendungen

- Stand der Normierung
- Problematik bei der Umsetzung
- Empfehlungen

Stefan Ries, Reichle & De-Massari AG

11:45 bis 12:30 Uhr

WAN-Planung und Optimierung

- Neue WAN-Verfahren und ihre Bedeutung
- MPLS: Projekterfahrungen
- Applikationen und Datacenter im WAN
- Trends und Ausblick

Dr.-Ing. Behrooz Moayeri, ComConsult Beratung und Planung GmbH

14:00 bis 15:30 Uhr

Neue Wireless LAN-Technologien in der Analyse: Projekterfahrungen

- Controller-basierte Architekturen kontra traditionelles Access-Point-Design
- Herausforderung: zentralisierte Konfiguration
- Konsequenzen für das Distributions-System und die WLAN-Sicherheits-Infrastruktur
- Markt- und Produktsituation Wireless-Switching
- Mobilität und Sicherheit: wie aufwendig ist IEEE 802.11i
- Empfehlungen für erfolgreiche und investitionssichere Wireless-Projekte

Dr. Simon Hoff, ComConsult Beratung und Planung GmbH

16:00 bis 17:00 Uhr

Sicherheit im Netzwerk: Zugriffsschutz auf Benutzerebene

- Bedrohungsanalyse
- Zugriffsschutz im Netzwerk: alternative Lösungsansätze
- Bestehende Standards und ihre Nutzbarkeit
- Potenziale und Grenzen gruppenbezogener Zugriffsrechte
- Praktische Umsetzung und Einsatzszenarien
- Behandlung von Problem-Geräten
- Prüfung der Patch-Level von Clients: Hersteller-Konzepte in der Bewertung
- Ausblick und Empfehlungen

Markus Schaub, ComConsult Technologie Information GmbH

10:30 - 11:00 Uhr Kaffeepause
12:30 - 14:00 Uhr Mittagspause
15:30 - 16:00 Uhr Kaffeepause

Programmübersicht: Netzwerk-Redesign Forum 2006

Mittwoch, den 29.03.2006

9:00 bis 10:00 Uhr
Projekterfahrungen zur IP-Telefonie
- Vorgehensweise bei Ausschreibungen
- Applikationen und Sonderanwendungen in einer VoIP-Umgebung
- Voice-Tauglichkeit bestehender Netzwerke
- QoS-Konzeptionierung
- Welche QoS-Architektur ist zu empfehlen
- Integration und Trennung von Sprache und Daten im Netzwerk
- Ergebnisse aktueller Ausschreibungen

Dr.-Ing. Behrooz Moayeri, ComConsult Beratung und Planung GmbH

10:00 bis 11:00 Uhr
Business-Case IP-Telefonie
- Typischer Projektablauf: was gehört zum typischen Voice-Projekt, wo liegen Stolpersteine, welcher Zeitablauf ist realistisch
- Traditionelle TK kontra IP-Telefonie: was zeigen aktuelle Projekterfahrungen
- Wirtschaftlichkeit: Ergebnisse aktueller TCO-Berechnungen, typische Amortisationszeiten
- Hosted IP-Telefonie: eine Alternative?
- Markt-Analyse: wo stehen wichtige Hersteller, welche Strategien verfolgen sie, wer ist für die nächsten Jahre am besten aufgestellt
- Sind offene, standardisierte Lösungen realisierbar?
- Zeitlicher Ausblick: was dominiert die nächsten 3 Jahre
- Empfehlungen für die erfolgreiche Projektdurchführung

Dipl.-Inform. Petra Borowka, Unternehmensberatung Netzwerke UBN

11:30 bis 12:30 Uhr
Mobile Kommunikation
- Anwendungsszenario mobile Kommunikation
- Aktuelle Standards: was sie leisten, was sie nicht leisten
- Herausforderung: zentrales Management der mobilen Endgeräte
- Integration in bestehende Strukturen (Active Directory, Exchange)
- Spezifische Sicherheitsanforderungen an mobile Endgeräte
- Sicherheit versus Nutzungskomfort
- Marktanalyse: welche Softwarelösungen gibt es und was sie leisten
- Welche Leistungsmerkmale sind unverzichtbar
- Trends und Ausblick

Dr. Frank Imhoff, ComConsult Beratung und Planung GmbH

14:00 bis 14:45 Uhr
Integration von Gefahren- und Meldetechnik in IP-Netzwerke
- Das universelle Gefahrenmeldenetz, baldige Realität oder bleiben es zwei Welten
- Videoüberwachung im Netzwerk: Motivation, Trends und Produkte
- Anforderungen an das Netz zur Einführung von Videoüberwachung
- Aufbau von „Video-Netzwerken“
- Video over Wireless
- Gefahrenmeldetechnik im LAN: Probleme und Lösungen
- Anforderungen der Sicherheitstechnik und Anforderungen an die Verfügbarkeit
- Trends und Ausblick

Dipl.-Ing. Hartmut Kell, ComConsult Beratung und Planung GmbH

15:15 bis 16:00 Uhr
IPS und Firewalls: Ergänzung oder Konkurrenz
- Funktionsweise eines Intrusion Prevention Systems (IPS)
- Techniken zur Erkennung von Angriffsmustern
- Netzbasierte und Host-basierte Systeme
- Abgrenzung zu Firewall-Systemen
- Einsatzvarianten und Architekturen
- Produktsituation

Dr. Simon Hoff, ComConsult Beratung und Planung GmbH

11:00 - 11:30 Uhr Kaffeepause
12:30 - 14:00 Uhr Mittagspause
14:45 - 15:15 Uhr Kaffeepause

Donnerstag, den 30.03.2006 - Ein-Tages-Intensiv-Trainings/Workshops

BITTE EIN GEWÜNSCHTES THEMA ANKREUZEN!!

☐ **Intensiv-Training 1:**
SIP in der Analyse:
auf dem Wege zur offenen IP-Telefonie?
- Was leistet SIP, wie arbeitet es
- Welche Komponenten werden benötigt
- Wie sehen typische Produkte aus
- Ein Alltags-Szenario und seine Umsetzung mit SIP
- Variante 1: die offene Lösung
- Variante 2: SIP und die traditionellen Hersteller
- Ausblick

Markus Schaub, ComConsult Technologie Information GmbH

☐ **Intensiv-Training 2:**
Wireless LAN in Produktion und Logistik
- Anforderungen
- Wireless-Technologien und ihre Nutzbarkeit
- Roaming-/Handover
- Handhabung mobiler Teilnehmer
- Umsetzung hoher Verfügbarkeit und Redundanz
- Koexistenz und Integration unsicherer Teilnehmer und Teilnehmer alter Standards
- Beispiele und Projekterfahrungen
- Ausblick und Empfehlungen

Dr. Simon Hoff, ComConsult Beratung und Planung GmbH

Die Intensiv-Trainings starten alle parallel um 9:00 Uhr.
Bitte wählen Sie vorab einen der Intensiv-Trainings aus,
damit wir die weitere Organisation planen können. DANKE!

☐ **Intensiv-Training 3:**
Quality of Service
- QoS-Ziele
- QoS-Anforderungen in Lokalen Netzwerken
- QoS-Mechanismen
  - Auf Ethernet-Ebene
  - Auf IP-Ebene
  - Über IP-Ebene
- Konzepte für den LAN-Ausbau im Hinblick auf QoS
  - Access-Bereich • Core-Bereich • Back-End-Bereich
- Sonderfall: QoS und IP-Telefonie
- Messungen in produktiven Netzwerken
  - Aufbau • Ergebnisse
- QoS im WAN
  - Architektur
  - Flankierende Maßnahmen
  - IP-Telefonie im WAN
- QoS im Wireless LAN
  - Einfluss der WLAN-Technologie
  - Kanalzugriff und Handover
  - IP-Telefonie
- Fazit und Empfehlungen

Dr.-Ing. Behrooz Moayeri, ComConsult Beratung und Planung GmbH

10:30 - 11:00 Uhr Kaffeepause
13:00 - 14:00 Uhr Mittagspause
15:30 Ende der Veranstaltung

Der Veranstalter behält sich Änderungen im Programm vor!

Aktueller Kongress

Gefahrenmeldetechnik und Objektüberwachung im Netz 2006

Die ComConsult Akademie veranstaltet vom 15. - 16. Mai den Kongress „Gefahrenmeldetechnik und Objektüberwachung im Netz 2006“ in Bad Neuenahr.

Der Ruf nach konvergenten Netzen macht vor dem Bereich der Gefahren- und Meldetechnik nicht halt, die Nachfrage nach einer Nutzungsmöglichkeit von IP-basierenden Netzen für Videoüberwachung, Einbruchmeldetechniken, Brandmelder, Zutrittskontrollen und ähnlichem nimmt rapide zu.

Sowohl auf der Seite der klassischen Gebäudeüberwachungstechnik als auch bei den IT-Spezialisten herrscht Unsicherheit darüber, welche dieser klassischen Techniken bereits heute durch IP abgedeckt werden können.

Das ComConsult-Forum „Gefahrenmeldetechnik und Objektüberwachung im Netz 2006“ führt die bereits 2005 im gleichnamigen Forum begonnene Analyse der Technologie-, Markt- und rechtlichen Situation fort, und gibt wesentliche Empfehlungen zur Einführung dieser neuen Techniken.

Neben der Überarbeitung der Themen des Forums von 2005 werden vollkommen neue Themen Gegenstand der Veranstaltung sein.

Für Teilnehmer am gleichnamigen Forum vom Oktober 2005 bieten wir die Teilnahme am diesjährigen Kongress zu einem Sonderpreis an. Sprechen Sie uns dazu bitte an.

Im Einzelnen geht das Forum auf folgende Fragen ein:

- Was leistet eine IP-basierende Infrastruktur im Bereich der Gebäudemeldetechnik heute?
- Welche Akzeptanz finden IP-basierende Lösungen bei den Versicherungen oder Sachverbänden?
- Welche Grundelemente sind vorzusehen, um Überwachungs- und Meldtechnik in IP-basierenden Netzen zu implementieren?
  Wie sehen die Erfahrungen bei erfolgreicher Einführung dieser neuen Techniken aus?

- Sind besondere QoS-Anforderungen an moderne Datennetze zu stellen, die eine Einführung erst möglich machen?
- Sind IP-basierende Netze wirklich so unsicher, dass sie nicht für „Security Anwendungen“ genutzt werden können?
- Wie ist ein Netz aufzubauen, um höchste Verfügbarkeit sicherzustellen?
- Welche Vorteile liefert eine Netzstrukturierung auf der Ebene 3?
- Wie lassen sich die aktuellen Entwicklungen im Bereich der WLAN-Techniken nutzen
  (Beispiel: IEEE 802.11n)?
- Warum steigt die Verfügbarkeit einer Videoüberwachung durch Nutzung von IP?
- Wo liegen die qualitativen Unterschiede der verschiedenen Überwachungstechniken?
- Welche Normen lassen netzwerkbasierende Gefahrenmeldetechniken zu?
- Müssen andere Komponenten eingesetzt werden oder lassen sich Standard-Bürokomponenten verwenden?

Folgende Vortragsthemen sind unter anderem vorgesehen (Änderungen vorbehalten):

- Nutzbarkeit von modernen Kommunikationsnetzen für Gefahrenmanagement
- Nutzbarkeit von modernen Kommunikationsverkabelungen für Meldeanlagen
- Flexible Gebäudeautomatisierung mit Ethernet am Beispiel eines konkreten Projektes (Planung, Realisierung)
- Videoüberwachung über IP
  (Anforderungen, Lösungen, Grenzen, Marktübersicht)
- Quality of Service
- Bewertung der IP-basierenden Lösungen durch Normen, Versicherungen oder anderen zertifizierenden Institutionen
- Funküberwachung: Stabilität, Verfügbarkeit, Sabotierbarkeit

Dieses Forum bietet die ideale Basis für eine Standortbestimmung.

Wer immer beabsichtigt in Gebäuden eine IP-basierende Gefahrenmeldetechnik bzw. Objektüberwachung einzuführen oder sein Netz darauf vorzubereiten, der sollte dieses Forum nicht verpassen.

Durch das Forum führt Dipl.-Ing. Harmut Kell von der ComConsult Beratung und Planung GmbH.

Im Anschluss an sein Studium als Nachrichtentechniker spezialisierte sich Herr Kell auf die Datenkommunikation in lokalen Netzen und kann bis heute auf eine mehr als 15-jährige Berufserfahrungen in diesem Bereich verweisen. Als langjähriger Mitarbeiter der ComConsult Beratung und Planung GmbH hat er umfangreiche Praxiserfahrungen bei der Planung, Projektüberwachung, Qualitätssicherung und Einmessung von Netzwerken gesammelt. Ergänzend zu diesen projektbezogenen Arbeiten vermittelt Herr Kell sein umfangreiches Fachwissen in Form von Fachpublikationen und Seminaren.

Gefahrenmeldetechnik und Objektüberwachung im Netz 2006

10% Frühbucherrabatt bis 15.03.06

Gefahrenmeldetechnik und Objektüberwachung im Netz 2006
15.05. - 16.05.06 in Bad Neuenahr

Für Besucher unserer bisherigen Kongresse bzw. für die Teilnehmer am VIP-Verteiler bieten wir auch in diesem Jahr exklusiv eine Vorbuchungsphase für das Forum Gefahrenmeldetechnik und Objektüberwachung im Netz 2006 bis zum 15.03.2006 für eine rabattierte Teilnahmegebühr an.

Gefahrenmeldetechnik und Objektüberwachung im Netz 2006
zum Preis bei Buchung bis 15.03.06 von € 1.390,-
statt regulär € 1.590,- zzg. MwSt.

Die Buchung innerhalb der Frühbucherphase ist verbindlich, kann aber jederzeit auf einen anderen Mitarbeite Ihres Unternehmens übertragen werden.

Fax-Antwort an ComConsult 02408/955-399

Anmeldung
Gefahrenmeldetechnik und Objektüberwachung im Netz 2006

Ich buche den Kongress
Gefahrenmeldetechnik und Objektüberwachung im Netz 2006

___ vom 15.05. - 16.05.06 in Bad Neuenahr

zum Preis von € 1.390,- zzgl. MwSt.*
*gültig bis 15.03.06
(regulärer Preis € 1.590,- zzgl. MwSt.)

☐ Bitte reservieren Sie für mich ein Hotelzimmer

vom_____bis_____06

Buchen Sie über unsere Web-Seite
www.comconsult-akademie.com

_____ Vorname	_____ Nachname
_____ Firma	_____ Abteilung
_____ Telefon	_____ Fax
_____ Straße	_____ PLZ,Ort
_____ eMail	_____ Unterschrift

Zweitthema

RFID-Lösungen, große Architekutren für kleine Chips

Fortsetzung von Seite 1

Dipl-Ing. Frank Lange-Lietz ist Berater bei deconis gmbh. Er war mehrere Jahre als IT-Leiter verantwortlich für den IT-Betrieb in einem Systemhaus für Broadcast-Technik und berät seit einigen Jahren Unternehmen verschiedener Größe zu Themen des Einsatzes und der Betriebsorganisation von IT-Infrastrukturen.

Natürlich hat auch die RFID-Technologie ihre Problemzonen, über die man kontrovers diskutieren kann und sollte - ganz vorne das Thema Sicherheit. Aber diese Schwierigkeiten können nicht mehr als Kinderkrankheiten bezeichnet werden, vielmehr sind es normale fachliche Fragestellungen, wie sie sich auch in vielen anderen Bereichen der Informationstechnologie stellen.

Kurzum: RFID etabliert sich und hat den Punkt der experimentellen Technologie schon länger überschritten. Mit derzeitigen Kosten von 30 US-Cent für Passiv-Tags lassen sind diese zwar noch zu teuer für Joghurtbecher, doch ist ein wirtschaftlicher Einsatz für Behälterobjekte (Paletten, Container, Kisten, etc.) durchaus möglich und es ist zu erwarten, dass die Kosten mit weiterer Verbreitung weiter sinken. Auch in technischer Hinsicht stabilisiert sich die Situation. So existiert mit dem EPCglobal Class1 Generation 2 Standard seit Dezember 2004 ein neuer Standard mit breiter Akzeptanz, der stark auf die bestehenden ISO-Standards zugegangen ist und von dem zu erwarten ist, dass er auch von der ISO übernommen wird. Von vielen Herstellern sind bereits RFID-Tags und Reader am Markt verfügbar, die diesen Standard unterstützen. Generell zeigt auch die Vielfalt an Lesegeräten und RFID-Lösungen, wie sehr sich diese Technik bereits durchgesetzt hat.

RFID hat die Phase der Pilotprojekte und Vorläufer überwunden und erfährt einen immer breiteren Einsatz.

Für den effizienten Einsatz ist aber nicht nur ein adäquater Preis der RFID-Tags und eine verlässliche Etablierung von Standards notwendig. Eine RFID-Lösung bewegt sich auf verschiedenen Ebenen einer IT-Umgebung. Das RFID-System muss nicht nur technisch auf Reader- und RFID-Tag-Ebene realisiert werden, auch die Verbindung der RFID-Daten und Events in die bestehende Enterprise-Applikation ist zwingend notwendig, da ohne diese Integration ein RFID-Projekt wenig Sinn machen würde. Das Lösen der verschiedenen Herausforderungen auf unterschiedlichen Ebenen stellt besondere Ansprüche an eine erfolgreiche Projektabwicklung.

Ich werde in diesem Artikel nicht nur auf aktuelle Neuerungen und verschiedene RFID-Architekturen eingehen, sondern auch auf Methoden eines RFID-Projektes. Doch verschaffen wir uns zunächst noch einmal einen Überblick über die RFID-Technik und RFID-Architektur.

Die RFID-Technik im Überblick

RFID bezeichnet die Technik von winzigen Schaltkreisen mit Hilfe von speziellen Antennen (sogen. RFID-Tags), Daten über kurze Funkdistanzen auszulesen. Passive RFID-Tags besitzen keine eigene Stromversorgung, sondern werden von dem Lesegerät, dem RFID-Reader, über eine bestimmte Trägerfrequenz mit der notwendigen Energie versorgt. Dies funktioniert im HF-Bereich über kurze Distanzen von wenigen Zentimetern durch den Aufbau eines elektromagnetischen Feldes, welches entsprechend der im RFID-Tag gespeicherten Daten verändert wird.

Im UHF-Bereich wird vom Reader eine Trägerfrequenz ausgesendet. Der RFID-

Sektor	Einsatzbeispiele
Einzelhandel	Warenverfolgung Produktrückrufe Automatische Rechnungserstellung
Gesundheit	Überwachung von Blutbanken Überwachung und Verfolgung von Medikamenten in Krankenhäusern Dokumentation von Produktionsreihen in der Pharmazie
Logistik	Überwachung, Verfolgung und Instandhaltung von Transportmitteln (z.b. Container, LKW) Auslastungsplanung von Transportkapazitäten
Fahrzeugindustrie	Anlagemanagement: Container und Werkzeugmanagement Teileverfolgung: Inventarmanagement, Montage, Diebstahlkontrolle, Verteilung, Wiederverwertung Fahrzeugidentifikation, Zugangskontrolle, Reifendruckkontrolle
Lebensmittelindustrie	Dokumentation der Herkunft von Vieh/Vögel Schlachtviehverfolgung bis zur Theke
Militär	Teilemanagement, Auslastung, Verfolgung und Wartung
Luftfahrt	Gepäckverladung
Quelle: EPCglobal, “The EPCglobal Network: Overview of Design, Benefits & Security”, September 2004	

RFID-Lösungen, große Architekturen für kleine Chips

Tag moduliert bei der Reflektion auf die Trägerfrequenz die im RFID-Tag gespeicherten Daten. Auch dafür wird neben der Trägerfrequenz keine zusätzliche Energie benötigt. UHF-Tags besitzen eine Reichweite von mehreren Metern. Je nach der eingesetzten Klasse der RFID-Tags können nicht nur Daten gelesen, sondern auch auf die RFID-Tags geschrieben werden.

Aktive RFID-Tags besitzen eine eigene Energiequelle (meist Akku oder Batterie). Es gibt sie in den HF- und UHF-Frequenzbereichen der passiven RFID-Tags, wie auch im Frequenzbereich der „klassischern" WLAN-Technologie. Aktive WLAN-RFID-Tags arbeiten dann mit herkömmlichen Access-Points zusammen und benötigen keine speziellen Reader.

Aber die reine Technik allein bringt noch keinen Gewinn. Es ist nicht damit getan eine Kiste voll RFID-Tags und einen Reader zu kaufen und sie an Container zu schrauben. Die gewonnenen Daten müssen mit den Daten einer Enterprise-Applikation (z.b. Enterprise-Resourceplaning, Supply-Chainmanagement) verbunden werden.

Eine RFID-Architektur besteht aus 3 Ebenen. Auf der untersten Ebene (Technische Ebene) findet sich die Technik mit RFID-Tags, Antennen, Readern und deren Schnittstellen. Reader können die Daten der RFID-Tags über die beschriebenen Verfahren ohne Sichtverbindung lesen. Dabei ist bei UHF-Tags auch die Lage der RFID-Tags zu den Readern nicht entscheidend, so dass ein Lesevorgang auf einfache Weise automatisiert werden kann. Reader sind zudem in der Lage, je nach verwendetem Standard Tags in hoher Geschwindigkeit (bis zu 1000 Tags pro Sekunde) zu lesen.

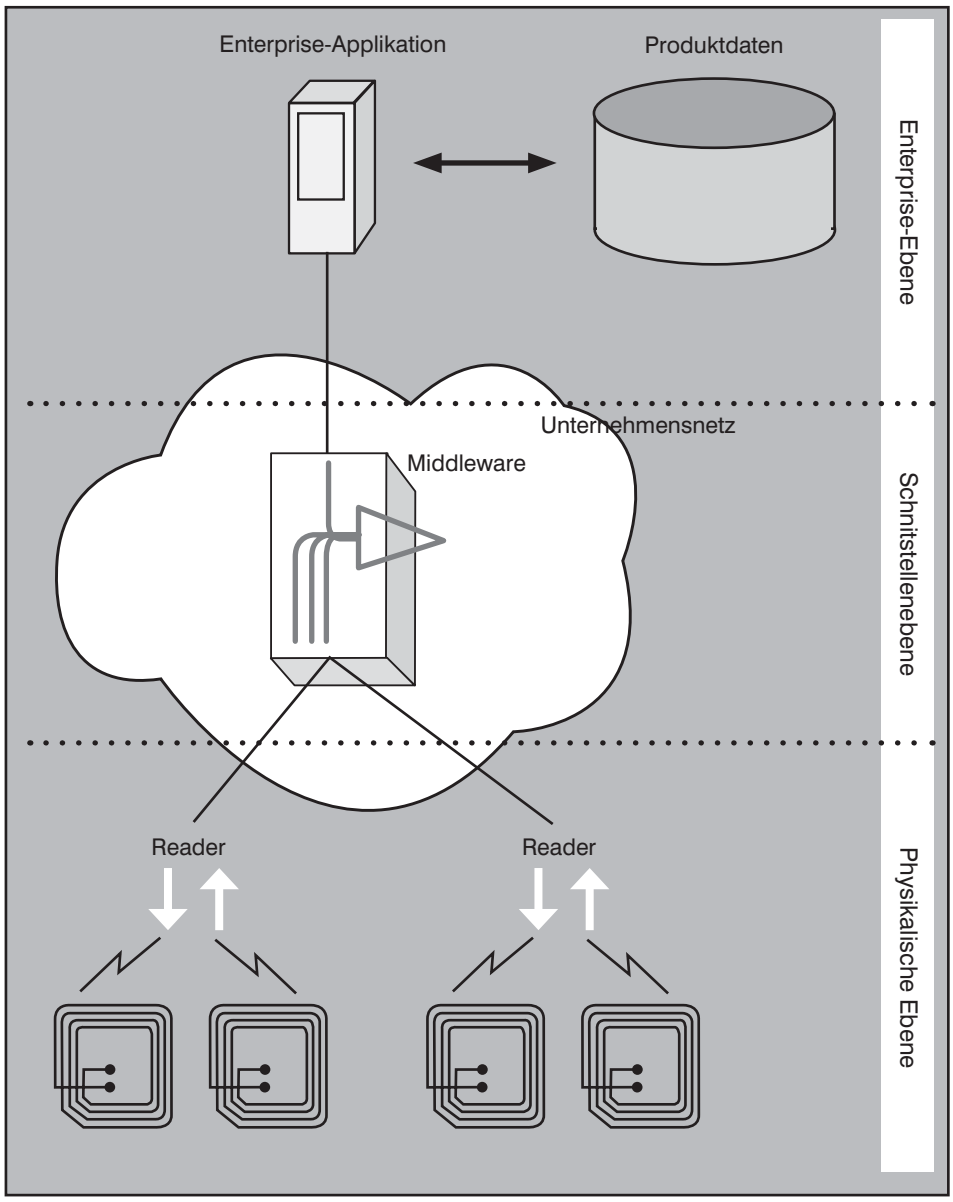


Abbildung 1: Ebenen einer RFID-Lösung

Auf der Schnittstellen-Ebene ist eine Middleware zu realisieren, welche die gelesenen Daten sinnvoll zusammenfasst, resultierende Events generiert und Fehler erkennt. Die Applikationen der Middleware gelten als intelligenter Konzentrator, der einerseits den Datenstrom zwischen den Readern und den beteiligten Enterprise-Applikationen überwacht und andererseits quasi „im Auftrag" einer Enterpriseapplikation Daten auswertet und Events generiert. Stellen Sie sich beispielsweise ein Schließsystem auf RFID-Basis vor, bei dem an jeder Tür auf jeder Seite ein Reader montiert ist und Mitarbeiter mit einer RFID-Plastikkarte die Türen geöffnet können. In der Enterprise-Applikation werden zwar die Berechtigungen festgelegt, doch können die Berechtigungen in den Reader geladen werden, damit der Reader selber den Türmechanismus anstoßen kann. Die Berechtigung könnte auch über einen RADIUS-Server erteilt werden. In diesem Fall müsste die Middleware die RFID-Daten in eine RADIUS-Abfrage umwandeln. Wenn zwei Mitarbeiter aus verschiedenen Richtungen gleichzeitig die Tür öffnen wollen, würde die Middleware theoretisch einen der beiden RFID-Datensätze verwerfen können, müsste aber darauf achten, dass die Tür trotzdem geöffnet wird, wenn nur einer der beiden Mitarbeiter die Berechtigung dazu besitzt. Die Datenmenge mag in diesem kleinen Beispiel noch überschaubar sein, aber die mögliche Intelligenz und Konsolidierung der Daten in der Middleware wird deutlich. Bedenkt man zudem, dass in anderen Umgebungen beispielsweise in der Produktion viele Objekte mit RFID-Tags pro Sekunde einen Lesebereich passieren können, ist klar, dass diese Intelligenz und Konsolidierung nicht nur möglich, sondern zwingend notwendig ist. Die Middleware bringt Funktionalität einer Enterprise-Applikation an Netzwerkgrenzen, die Middleware nimmt der Enterprise-Applikation quasi bestimmte Funktionen ab. Damit dieses in einem Gesamtkonzept flexibel umsetzbar ist, sollte ein System auf Basis einer Service Orientated Architecture (SOA) geplant werden. In einer SOA werden nicht bidirektionale Schnittstellen, sondern Service-orientierte Schnittstellen zwischen den verschiedenen Schichten eingerichtet. Eine für RFID-Systeme weit verbreitete Architektur besteht aus 5 Layern. (siehe Abbildung 2)

RFID-Lösungen, große Architekturen für kleine Chips

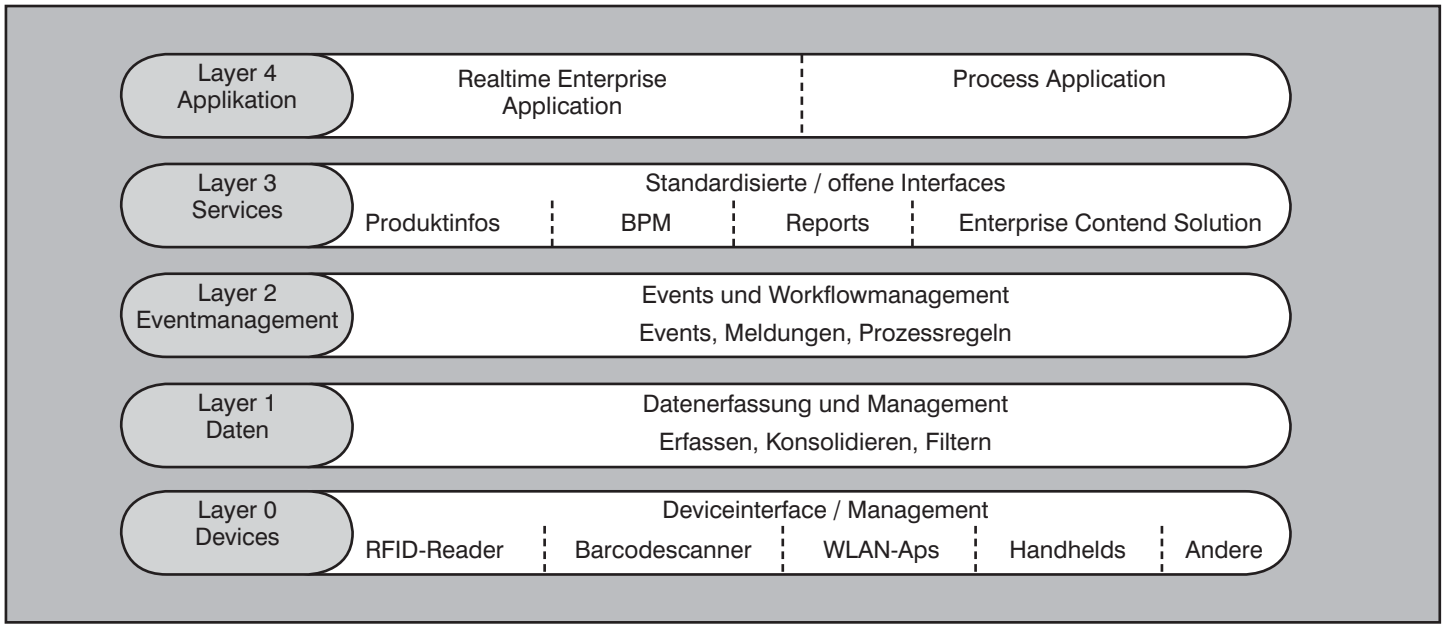


Abbildung 2: Software-Architektur für Real-Enterprise (Quelle: Microsoft)

Auf dem Layer 0 (Device-Layer) befinden sich neben den Readern auch alternative ID-Erfassungsdevices, wie z.B. Barcode-Scanner und WLAN-Access-Points, die als Reader für aktive RFID-Tags gelten können. Die verschiedenen Erfassungsgeräte stellen die gelesenen Daten über unterschiedliche Schnittstellen zur Verfügung. Die Palette der Schnittstellen reicht von einfachen seriellen Schnittstellen (RS232 oder RS422) über SNMP (simple network management protocol) bis hin zu XML (extensible Markup Language). Diese verschiedenen Schnittstellen werden von einem geeigneten Device-Management auf eine Service-orientierte Schnittstelle projeziert. Die verbreitetste Art der Service-orientierten Schnittstellen ist mittlerweile XML, das sich auch in anderen Bereichen durchgesetzt hat.

Der Layer 1 (Daten-Layer) ist die unterste Ebene der Middleware, in der die RFID-Daten gesammelt, gefiltert und zusammengefasst werden. Es werden doppelte, mehrfach gelesene Daten bzw. überflüssige oder fremde Daten herausgefiltert. Es können z.B. Daten von Objekten zusammengefasst werden, die sich auf einer Palette oder in einer Kiste befinden. Zusätzlich sollte eine gewisse Fehlererkennung und- beseitigung realisiert werden, wobei auch schon im Device-Layer so genannte simple-Filter implementiert werden können.

Zusätzlich befindet sich in diesem Layer ein Reader-Management für die verschiedenen Reader und anderen Erfassungsgeräte. In den meisten Fällen wird der Daten-Layer in der Middleware implementiert sein. Es kann auch spezielle Anwendungsfälle geben, in denen diese Funktionalität schon in dem Reader integriert ist. So gibt es beispielsweise komplette Dock-Door-Readersysteme, die bereits gefilterte und verdichtete Daten über XML zur Verfügung stellen. Ob die in solchen Systemen realisierbaren Regeln ausreichen, kann erst am konkreten Fall entschieden werden.

In jedem Fall werden die gesammelten und zusammengefassten Daten dem Event-Management des Layer 2 (Event-Layer) wiederum über eine Service-Schnittstelle zur Verfügung gestellt. Auf dieser Ebene werden aus den gewonnenen Realtime-Daten so genannte ALEs (application level event) generiert, die Prozesse in einer Enterprise-Applikation auslösen. Dabei ist es durchaus sinnvoll und

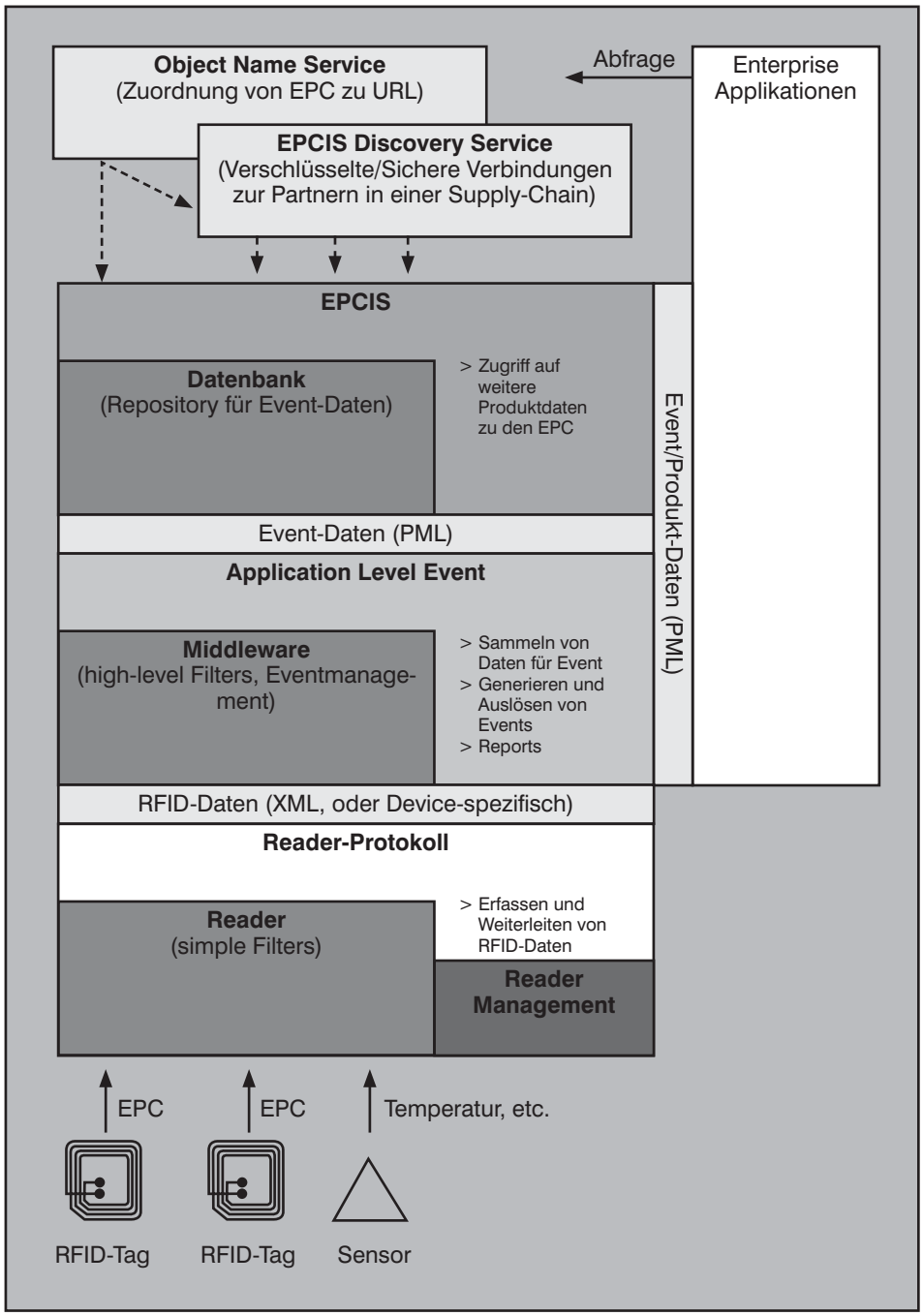


Abbildung 3: EPC Network Architecture (September 2004)

in den meisten Fällen auch notwendig, dass die im Layer 2 generierten ALEs für unterschiedliche Enterprise-Applikationen sowohl Bereichs- als auch Geschäftsübergreifend bestimmt sind.

Die Funktionen im Layer 3 (Service-Layer) beziehen sich auf Dienste, die für ein übergreifendes RFID-System notwendig sind. Ähnlich der aus dem Internet bekannten Dienste wie DNS, befinden sich in diesem Layer unter anderem Namensdienste, die einen EPC (electorinc product code) in einen Produktnamen bzw. eine zu einem Produkt zugehörige URL auflösen können. Dazu kommen weitere Produkt- und Objektinformationsdienste, die mit Hilfe einer Datenbank weitere Informationen zu einem Produkt liefern können.

Im Layer 4 (Application-Layer) befinden sich die verschiedenen Enterprise-Applikationen wie Supply-Chain-Management (SCM) oder Enterprise-Ressource-Planing (ERP), deren Prozesse mit Hilfe dieser Architektur RFID-unterstützt ablaufen sollen und die Ergebnisse für den Anwender darstellt.

Ziel der automatischen Identifikation über RFID und der dargestellten Systemarchitektur ist es, möglichst auf manuelle Eingriffe in einer Logistikkette zu verzichten. Hierfür ist es notwendig, dass die jeweilige Applikation die Möglichkeit besitzt, die gelesenen RFID-Daten nicht nur zu sammeln, sondern sie auch zu interpretieren.

Realisieren von machine-to-machine Prozessen

Dies ermöglicht der EPC Information Service (EPCIS), der auf einem WebService basiert und Informationen zu einem Produkt global zur Verfügung stellt. Das Finden des zu einem bestimmten Produkt gehörenden EPCIS wird über das Object Naming System (ONS) realisiert. Für die Kommunikation mit dem EPCIS wird derzeit vom AutoID-Center die Physical Markup Language (PML) entwickelt. Diese PML basiert auf dem XML-Standard und soll für die Beschreibung von EPC-Produkten eingesetzt werden. PML-Dateien sind in einer EPCIS-Datenbank gespeichert. In früheren Architekturen wurde an dieser Stelle von PML-Servern gesprochen. (siehe Abbildung 3)

Die Funktionen der Layer 1 und 2 (Daten-Layer und Event-Layer) werden auch als „Savant“ (dt.: Gelehrter) bezeichnet, da sie auf Basis zusätzlicher Informationen, die letztendlich aus dem Design der Enterprise-Applikation bzw. deren modellierter Abläufe stammt, Entscheidungen treffen können und Events generieren. Hier ist im Business Process Management (BPM) ein altbekannter Schritt nahe liegend, der schon vor längerer Zeit in der Softwareentwicklung vollzogen wurde und auch im Datenbankdesign mit XML schon Einzug gehalten hat. Der Schritt von einer ablauforientierten Prozessdarstellung zur objektorientierten Darstellung.

RFID-Events mit Hilfe von objektorientierter Prozessdarstellung planen

Bisher wurden Prozesse meist aus kontrollflussorientierter Sicht betrachtet und modelliert, Aktivitäten und Ereignisse wurden gemäß der notwendigen Abfolge verkettet. Mit dem Speichern von Informationen auf einem bestimmten Objekt und insbesondere mit der automatischen Erfassung erhält dieses Objekt selber die Möglichkeit, in Abhängigkeit von Daten, Ort und Zeit Ereignisse auszulösen. Natürlich wurden die gleichen Ereignisse

auch in bisherigen Systemen ohne RFID generiert, doch ist in der objektorientierten Sichtweise die Quelle der jeweiligen Ereignisse das Objekt selber. Es ist nicht mehr die Entnahme des letzten Teiles aus einem Materialcontainer, die den Prozess des Auffüllens anstößt, sondern der Container selber, der in einem Lesebereich das Event „Ich bin Leer“ auslöst und damit ein Auffüllen anstößt.

Damit kommt in der Planung und Modellierung der neuen RFID-gestützten Prozesse die objektorientierte Darstellungsform zum Tragen. Am Beispiel der oEPK wird deutlich, dass im Unterschied zu den kontrollflussorientierten Diagrammen eine integrierte Beschreibung zwischen Objektklassen und Prozessen im Vordergrund steht. Den einzelnen Objekten werden Methoden zugeordnet, die Aktivitäten bezeichnen, welche mit dem jeweiligen Objekt durchgeführt werden können. Es werden außerdem die Daten dargestellt, die ein Objekt besitzt oder die ein Objekt beschreiben sollen. Diese können auf dem RFID-Tag gespeichert werden, oder bei komplexen und sicherheitsrelevanten Daten in einer Enterprise-Datenbank. Zudem sind nicht aller RFID-Tag-Typen in der Lage, veränderliche Daten zu speichern. Die in einer Enterprise-Datenbank gespeicherten Daten müssen über den Produkt-Code verknüpft und von dem Event-Management in der Middleware dann bei Bedarf beschafft werden. In dem objektorientierten Diagramm werden ferner Ereignisse dargestellt, die von einem Objekt ausgelöst werden können und die dann wiederum Methoden/Aktivitäten anderer Objekte auslösen. Dabei müssen nicht alle Objekte auch mit RFID-Tags ausgestattet/unterstützt werden. Da es sich bei der objektorientierten Darstellung nur um eine bestimmte RFID-konforme Sichtweise handelt, sind weitere angrenzende Objekteklassen in der Darstellung notwendig. (siehe Abbildung 4)

In dem Beispiel wird ein Materialcontainer in einem einfachen Kanban-Kreislauf dargestellt. Die Materialbox besitzt die Methoden „Material entnehmen“ und „Material hinzufügen“. Zusätzlich sind Methoden zur Fehlererkennung denkbar und sinnvoll, dadurch kann z.B. vermieden werden, dass ein leerer Container in ein Pufferlager geliefert wird. Beschreibende Daten sind in diesem Fall lediglich Informationen zum Materialbestand im Container, die auf dem Tag gespeichert werden können, unter der Voraussetzung, dass wiederbeschreibbare Tags zum Einsatz kommen. Der Materialcontainer kann die Ereignisse „leer“ und „voll“ auslösen. Das Ereignis „leer“ wird ausgelöst, wenn

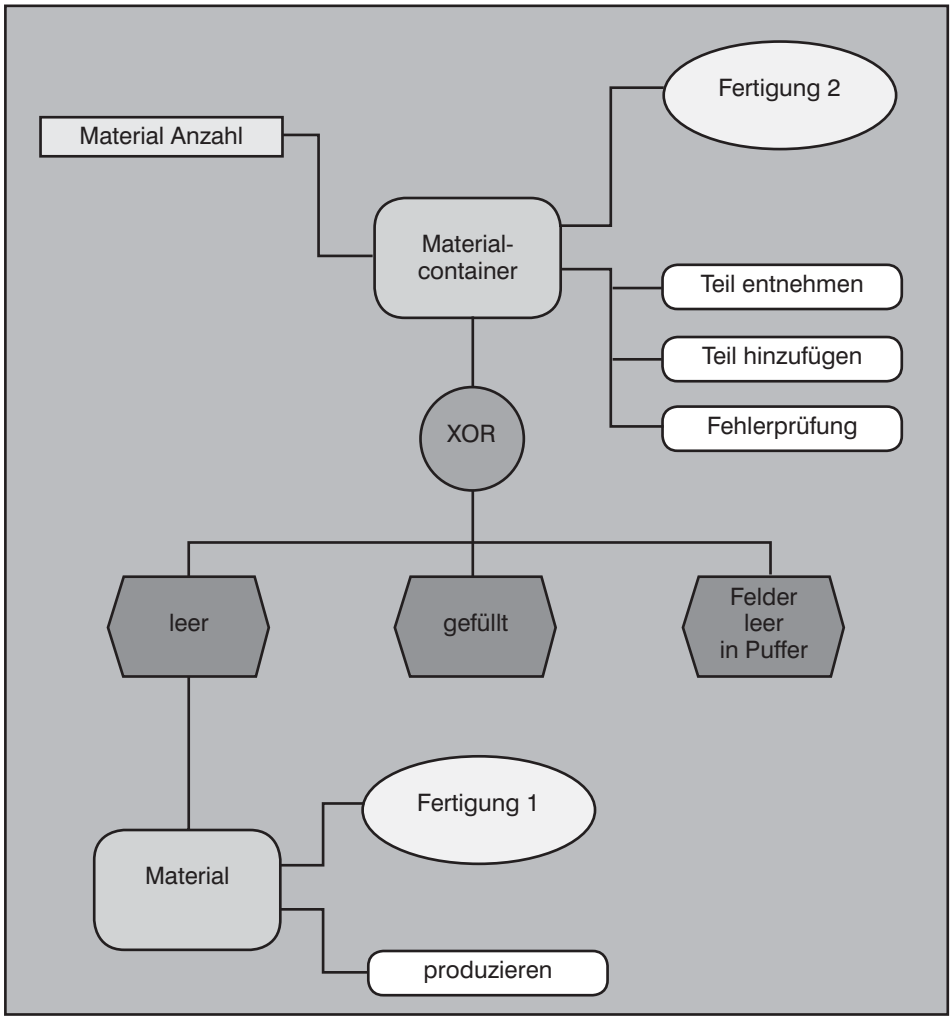


Abbildung 4: Objektorientierte EPK (oEPK)

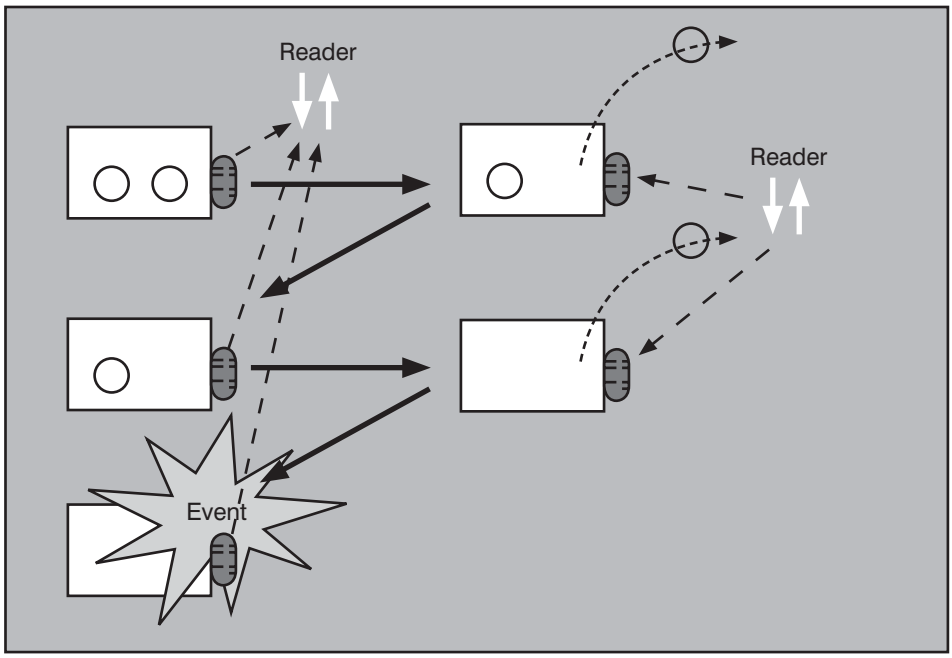


Abbildung 5: RFID-Event in einer Logistikkette

RFID-Lösungen, große Architekturen für kleine Chips

Der neue RFID-Standard EPCglobal ClassI Gen.2
Derzeit gibt es im wesentlichen 2 Institutionen, die Standards für die Kommunikation zwischen RFID-Tag und Reader festlegen. Zum einen hat die ISO mit der ISO 18000 Familie mehrere Standards für verschiedene Tag-Typen definiert. Andererseits finden die Festlegungen der EPCglobal allgemeine Anerkennung und eine weite Verbreitung. Natürlich gibt es, wie in vielen anderen Bereichen noch weitere proprietäre Protokolle für die Tag-Reader-Kommunikation, die weit verbreitet sind, doch ist zu erwarten, dass auch diese Protokolle langfristig nicht parallel zu den sich jetzt entwickelnden Standards bestehen bleiben oder gar weiter entwickelt werden.

Die EPCglobal teilt die RFID-Tags entsprechend ihrer Funktionalität in verschiedene Klassen, die zunächst noch nichts über die eingesetzten Protokolle aussagen:
- Class0 / Class0+: Passive Readonly-Tags, die nur eine fest eingestellte/einmalig programmierbare Seriennummer besitzen.
- ClassI: Passive Readonly-Tags, die neben einer einmalig programmierbaren Seriennummer noch zusätzlichen Speicher enthalten
- ClassII: Passiver Read/Write-Tag mit zusätzlichem Speicher.
- ClassIII: Semipassiver Class II-Tag, der durch eine eigene Batterie die Reichweite erhöhen und daneben noch Sensorik enthalten kann.
- ClassIV: Aktiver Tag, der mit anderen aktiven Class IV-Tags und Readern kommunizieren kann.
- ClassV: Aktiver Tag, der mit anderen Class IV und Class V-Tags und Readern kommunizieren und passive Tags (Class0, I und II) lesen kann.

Für die Class0 und ClassI-Tags gab es bisher von der EPCglobal standardisierte Protokolle der Generation 1. Seit Dezember 2004 gibt es das ClassI Gen. 2-Protokoll. Neben der funktionalen Verbesserung gegenüber den bisherigen Protokollen war ein wesentliches Ziel dieses Standards die Annährung an die ISO-Protokolle, um ein einheitliches Protokoll zu schaffen. Die Verabschiedung in der ISO scheiterte bisher nur noch an einem AFI-Feld (Application Familiy Identifier) in den Daten der RFID-Tags. Bisher hat jedes ISO-RIFD-Protokoll dieses 8 Bit große AFI-Feld. Auch in dem EPCglobal ClassI Gen. 2 Protokoll ist ein 8-bit Feld vorhanden, welches als AFI-Feld genutzt werden könnte. Dies ist im vorliegenden Standard jedoch nicht zwingend vorgeschrieben, um einen flexibleren Einsatz zu ermöglichen. Allerdings werden unabhängig von diesen Differenzen bereits RFID-Tags und Reader entwickelt, die das neue Protokoll unterstützen, was die Verbreitung der EPCglobal-Protokolle verdeutlicht. So ist es nach Meinung vieler Experten nur noch eine Frage der Zeit, bis auch die ISO das Protokoll in seine 18000-Familie aufnimmt. Das neue EPCglobal ClassI Gen. 2 Protokoll realisiert verschiedene Verbesserungen zu den bisherigen Protokollen:

Schnellere und flexible Lese-Raten
Ganz wie bei der menschlichen Verständigung, die in einem Vier-Augen-Gespräch in einem geschlossenen Raum (meist) leise und schnell abläuft und auf einem vollen Bahnhof lauter und langsamer wird, kann auch der Reader durch das Verändern von Sendeleistung und Übertragungsgeschwindigkeit die Kommunikation des Lese- und Schreibvorgangs an die herrschenden Umgebungsbedingungen anpassen. Abhängig von dem verfügbaren Frequenzspektrum kann eine Lesegeschwindigkeit bis über 1000 RFID-Tags pro Sekunde erreicht werden. Bei dem Schreibvorgang wird eine Geschwindigkeit von mindestens 5 RFID-Tags pro Sekunde garantiert, diese kann, abhängig von den Bedingungen, bis auf 30 Tags/s wachsen. Allein bei diesen Werten wird klar, dass der Vergleich zwischen Barcodes und RFID-Tags nur ein oberflächlicher Vergleich ist, der die hinzu gewonnene Funktionalität außer Acht lässt.

Robustere Kommunikation
Eine Schwierigkeit besteht in der Kommunikation mit mehreren RFID-Tags, die sich gleichzeitig im Lesebereich eines Readers befinden. Dabei generiert jeder RFID-Tag im Lesebereich eine Zufallsnummer, über die er vom Reader adressiert wird. Dadurch ist es möglich, auch RFID-Tags mit gleichen EPCs (electorinc product code) in einem Lesebereich zu erfassen und zu lesen. In früheren Protokollen wurden die gelesenen RFID-Tags in einen Sleep-Modus gesetzt, damit sie bei der Kommunikation mit weiteren RFID-Tags nicht störten. In dem aktuellen Protokoll wurde ein Dual-State-Mechanismus eingerichtet. Der Reader erfasst alle RFID-Tags im Status „A“. Jeder gelesene RFID-Tag wechselt automatisch in den Status „B“ und meldet sich erst wieder, wenn der Reader alle RFID-Tags im Status „B“ erfasst und abfragt. Dieser Statuswechsel wird mehrmals wiederholt, bis alle RFID-Tags im Lesebereich erfasst wurden. Dieses Verfahren ist schneller als eine mehrfaches „Schlafen-legen“ und „Wiederaufwecken“ der Tags.

Reader-Sessions
Um in bestimmten Umgebungen mehrere Reader in einem Lesebereich zu ermöglichen, wurden so genannte Sessions eingeführt. Es stehen 4 Sessions zur Verfügung, so dass beispielsweise fest installierte Reader bestimmte SessionIDs benutzen können und mobile Lesegeräte eine andere SessionID verwenden, damit die jeweiligen Kommunikationen nicht gestört werden. Es ist möglich, dass ein RFID-Tag mit mehreren Readern unterschiedlicher Sessions parallel kommuniziert, wodurch ein Reader nicht auf das Ende eines Kommunikationszyklus eines anderen Readers einer anderen Session warten muss.

Erweiterte Sicherheit
Es ist ein 32-bit-Passwort implementiert, mit dem ein RFID-Tag dauerhaft deaktiviert werden oder der Speicherbereich des RFID-Tags verschlossen und wieder geöffnet werden kann. Außerdem kann ein vom RFID-Tag zufälliges16-bit Handle für die jeweiligen Kommunikationszyklus generiert werden, welches die Schreib/Lese-Befehle zusätzlich absichert.
Auch wenn das Gen2-Protokoll zusätzliche Möglichkeiten bietet, bedeutet dies nicht, dass die bisherigen Protokolle (von EPCglobal oder ISO) nicht ausreichend Funktionalität beinhalten. So haben sich schon die großen Vorreiter der RFID-Gemeinde (Wal Mart und das amerikanische Verteidigungsministerium) für die Beibehaltung der Gen1-Tags ausgesprochen. Der Migrationsaufwand für bestehende Lösungen ist zu groß, als dass er sich wirtschaftlich lohnen würde, auch wenn viele Reader durch (einfache) Software-Updates auf das neue Protokoll aufgerüstet werden können. Es werden also zunächst die Protokolle beider Generationen parallel existieren. Dies stellt zwar bei globaler Betrachtung eine gewisse Herausforderung da, diese dürfte jedoch mit dem Einsatz von Multi-Protokoll-Readern lösbar sein.

das gesamte Material in der Fertigung 2 entnommen wurde (Bestand gleich Null) und der Container sich in einem Lesebereich eines Readers befindet. Das Ereignis „voll“ wird ausgelöst, wenn der gefüllte Container das Pufferlager erreicht. Ist der Materialcontainer an dieser Stelle nicht vollständig gefüllt, kann ein Fehler-Ereignis ausgelöst werden.

Eine vollständige RFID-gestützte Supply-Chain ist nicht in einem Schritt realisierbar. Dafür gibt es zu viele Einsatzmöglichkeiten und entsprechende Herausforderungen in einer Produktions-Kette. (siehe Abbildung 5)

Sicherheitsaspekte der RFID-Technik

Wenn die Entwicklung tatsächlich auf eine weite Verbreitung der RFID-Technologie in den unterschiedlichsten Supply-Chains und Produktionsketten hinausläuft - und das ist allem Anschein nach der Fall - muss natürlich auch die Frage der Sicherheit gestellt werden. Hierbei geht es nicht um die Sicherheit vor Datenverlust, letztendlich muss jedes System selber für die notwendigen Redundanzen bei einer ungewollten Zerstörung oder Beschädigung der RFID-Tags sorgen. Vielmehr ist der Schutz der Daten vor einer Nutzung durch Unbefugte zu diskutieren. Dies bezieht sich sowohl auf persönliche Daten eines Einzelnen, der mit RFID-Tag ausgestatteten Produkte kauft und trägt, als auch auf geschäftskritische Daten, die aus verschiedenen Gründen nicht in „fremde Hände“ gelangen dürfen. Dies ist insofern zu unterscheiden, als die Frage der Sicherheit geschäftskritischer Daten sich bei den meisten aktuellen RFID-Projekten stellt, da es sich bei diesen Lösungen um interne Abläufe handelt.

Auf die globale Supply-Chain, in der jede Puppe, jede Pizza und jede Jeans mit einem RFID-Tag ausgestattet wird, müssen wir sicherlich noch etwas warten. Vor dem Hintergrund der aktuellen Möglichkeiten für die Erstellung persönlicher Profile scheint es fraglich, ob ein bestimmtes persönliches Verhalten anhand eines RFID-Tags an der Jacke einfacher und detaillierter zu ermitteln ist, als über Rabattmarken, Internetkäufe oder die Ortung eines Handy. So gesehen eilt die in der allgemeinen Presse vorzufindende Diskussion nicht nur den technischen Möglichkeiten weit voraus, sondern liegt vielfach auch neben den aktuell diskussionsbedürftigen Sicherheitsfragen. Natürlich dürfen in dem aktuellen Entwicklungsstadium der RFID-Technologie die Sicherheitsfragen nicht gänzlich außer Acht gelassen werden, doch ist die Sicherheitsfrage beispielsweise bei den aktuellen Standards angemessen berücksichtigt. So sind im EPCglobal Classl Gen. 2 Standard Authentifizierung, Verschlüsselung und auch eine dauerhafte Zerstörung der Tags mit einem Kill-Komando vorgesehen.

Kanban
Das in den 50ger Jahren bei Toyota entwickelte Kanban-System ist ein Instrument mit dem ein Materialfluss in der Fertigung gesteuert werden kann. Hierbei wird davon ausgegangen, dass sich jeder Herstellungsprozess selber das benötigte Material aus einem Pufferlager abholt. Dies wurde zunächst über eine Karte (jap. Kanban) realisiert, die an jedem Materialcontainer befestigt war, der das Pufferlager erreicht. Wurde ein Materialcontainer geleert, so wurde die Kanban-Karte zunächst gesammelt und dann in regelmäßigen Abständen wieder an die zuständige Produktionsstellen zurückgegeben. Dadurch wird ein selbstregulierender Regelkreis geschaffen, der nicht über eine zentrales Prozessmanagement gesteuert werden muss. Dieses System kann sowohl in internen Produktionszyklen eingesetzt werden, wie auch zwischen Produktion und Zulieferern.

Die Möglichkeiten sind demnach vorhanden, müssen aber in den konkreten Projekten und Lösungen auch angemessen berücksichtigt werden.

Sicherheitsrelevante Daten sollten nicht auf den RFID-Tags gespeichert werden

Es ist nicht sinnvoll und in der dargestellten Systemarchitektur auch nicht notwendig, sicherheitskritische Daten auf den RFID-Tags zu speichern. Alles was auf einem RFID-Tag gespeichert wird, kann gelesen werden, wenn der RFID-Tag das System verlässt. Sicherheitskritische Daten, wie sie beispielsweise in Krankenhäusern anfallen können, sind besser in einer Enterprise-Datenbank aufgehoben, aus der sie von der Middleware in realtime bezogen werden können. Es ist also unerheblich, ob die Daten auf dem Armband eines Patienten oder in einer zentralen Datenbank gespeichert sind, wichtig ist, dass die Daten zum Lesezeitpunkt von der Middleware zu Verfügung gestellt werden können. An dieser Stelle können mit Hilfe von RFID neue Sicherheitsmechanismen realisiert werden, da der RFID-Tag als eine Art Schlüssel zum entsprechenden Datensatz in der Enterprise-Datenbank gelten kann.

Dies bedingt natürlich, dass sowohl die Enterprise-Datenbank, die Middleware, als auch der Zugang zu den jeweiligen Ressourcen, also zum Netzwerk, entsprechend der Anforderungen geschützt ist. Aber diese Notwendigkeit existiert unabhängig vom Einsatz der RFID-Technologie. Ein weiterer Aspekt der Sicherheit ist die Störsicherheit durch ungewollte Fehler oder auch gewollte Fremdeinflüsse. So müssen eigene RFID-Tags von fremden RFID-Tags unterschieden werden, um eine Beeinflussung des Systems über diesen Weg auszuschließen. Genauso sollten falsche oder veränderte Daten auf einem RFID-Tag durch eine geeignete Konsistenzprüfung erkannt werden.

Wie in vielen anderen Bereichen auch, ist es Aufgabe der jeweiligen Projekt-Planung die möglichen Sicherheitsmaßnahmen bedarfsgerecht anzuwenden.

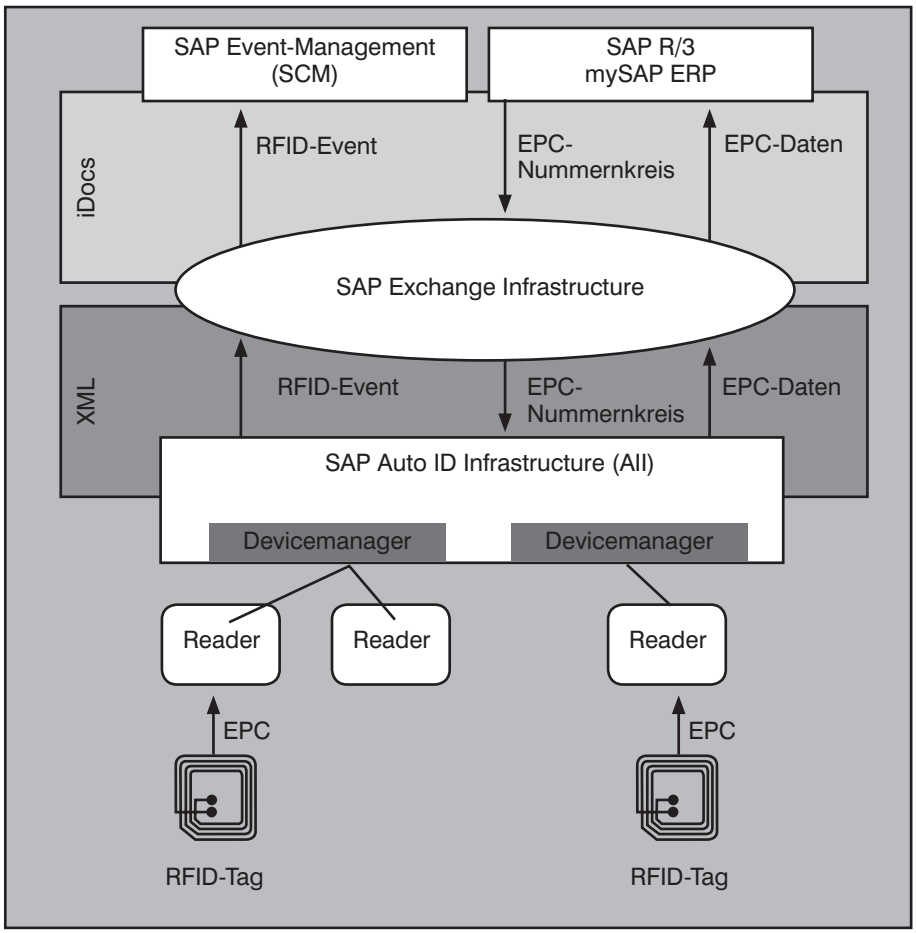
RFID in Beschaffungs- und Produktionslogistik

Die Einsatzbereiche von RFID-Lösungen können in Beschaffungslogistik und Produktionslogistik unterschieden werden. In beiden Bereichen werden Materialflüsse mit Hilfe von RFID in Echtzeit verfolgt. Aufgrund der Komplexität einer RFID-Lösung und der Verkettung mit den verschiedenen anderen Ebenen der gesamten IT- und Applikations-Infrastruktur im Unternehmen ist die Umsetzung einer RFID-Lösung in einem abgeschlossenen Bereich als Pilotprojekt aus mehreren Gründen unbedingt empfehlenswert:

- Hohe Investitionskosten in Technologie und Systemintegration verursachen zu Beginn meist ein negatives Kosten-Nutzen-Verhältnis. Durch den Einsatz in einem überschaubaren Prozessbereich bleiben auch die Investitionskosten im Rahmen.
- Erfahrung und Kompetenz im Untenehmen lassen sich mit einem Pilotprojekt effizienter aufbauen.
- Die Integration ist wesentlich einfacher, je weniger Enterprise-Applikationen an einer Pilot-Lösung beteiligt sind.
- Das Realisierungsrisiko bei einer neuen Technologie ist in einem kleinen, abgeschlossenen System geringer.
- Verwendung hochwertiger RFID-Tags, die noch nicht als Verbrauchsmaterial eingesetzt werden, da sie in geschlossenen Systemen wieder verwendet werden können.

SAP-AutoID-Infrastructure

Mit der AutoID-Infrastructure realisiert SAP in verschiednen SAP-Enterprise-Umgebungen (SAP R/3, mySAP ERP, mySAP SCM) die Einbindung von RFID. Dabei übernimmt die AutoID-Infrastructure (AII) die Verbindung zu den Readern und damit zu den Erfassungsgeräten des Device-Layer. Für die eingesetzten Reader kommen Devicemanager (DM) zum Einsatz, die entweder von SAP oder von den jeweiligen Readerherstellern realisiert werden. Insbesondere bei der Koordination mehrerer Lesegeräte ist ein DM vom jeweiligen Readerhersteller meist sinnvoller einzusetzen.



SAP RFID-Infrastruktur

Die SAP-AII erhält von der Enterprise-Applikation sowohl operative Daten über erwartete Ereignisse als auch Informationen über einzusetzende Nummernkreise, im Fall der Programmierung neuer RFID-Tags. Der Datenaustausch erfolgt über XML und wird über die SAP Exchange Infrstructure (SAP XI) gesteuert. Die SAP-AII übernimmt die Aufgaben des Daten-Layer, also das Filtern und Zusammenfassen der Tag-Daten. Die SAP XI verbindet die SAP-AII mit der eingesetzten Enterprise-Applikation. Dabei werden die XML-Daten in IDocs umgewandelt. Ziel ist es, an dieser Stelle eine offene Schnittstelle zur Verfügung zu stellen, die nicht nur die Kommunikation mit SAP Enterprise-Systemen ermöglicht. Neben dem Mapping ist die SAP XI auch für das Nachrichtenrouting an eine oder mehrere Enterprise-Applikationen zuständig.

Ein Return-on-Investment ist in den großen Supply-Chains aufgrund der bereits bestehenden hohen Automatisierung bei der Einbringung von RFID in Teilbereiche nur sehr schwer zu erreichen. Erst mit einer in RFID-gestützten, übergreifenden Supply-Chain ist langfristig ein ROI zu erwarten und sind Einsparungspotenziale auszuschöpfen. Deshalb ist zur Zeit vor allem der RFID-Einsatz in Closed-Loop-Systemen wirtschaftlich sinnvoll. Closed-Loop-Systeme bezeichnen im Gegensatz zu Open-Loop-Systemen unternehmensinterne, in sich geschlossene Logistikketten. Bei den Open-Loop-Systemen beginnt eine Logistikkette aus der Sicht eines einzelnen Unternehmen bei dem Zulieferer und reicht bis zum jeweiligen Kunden. Dabei reicht

die Logistikkette über den Zulieferer und den Kunden hinaus, auch der Zulieferer kann diese Logistikkette betrachten.

Pilot-Projekte in Closes-Loop-Systemen

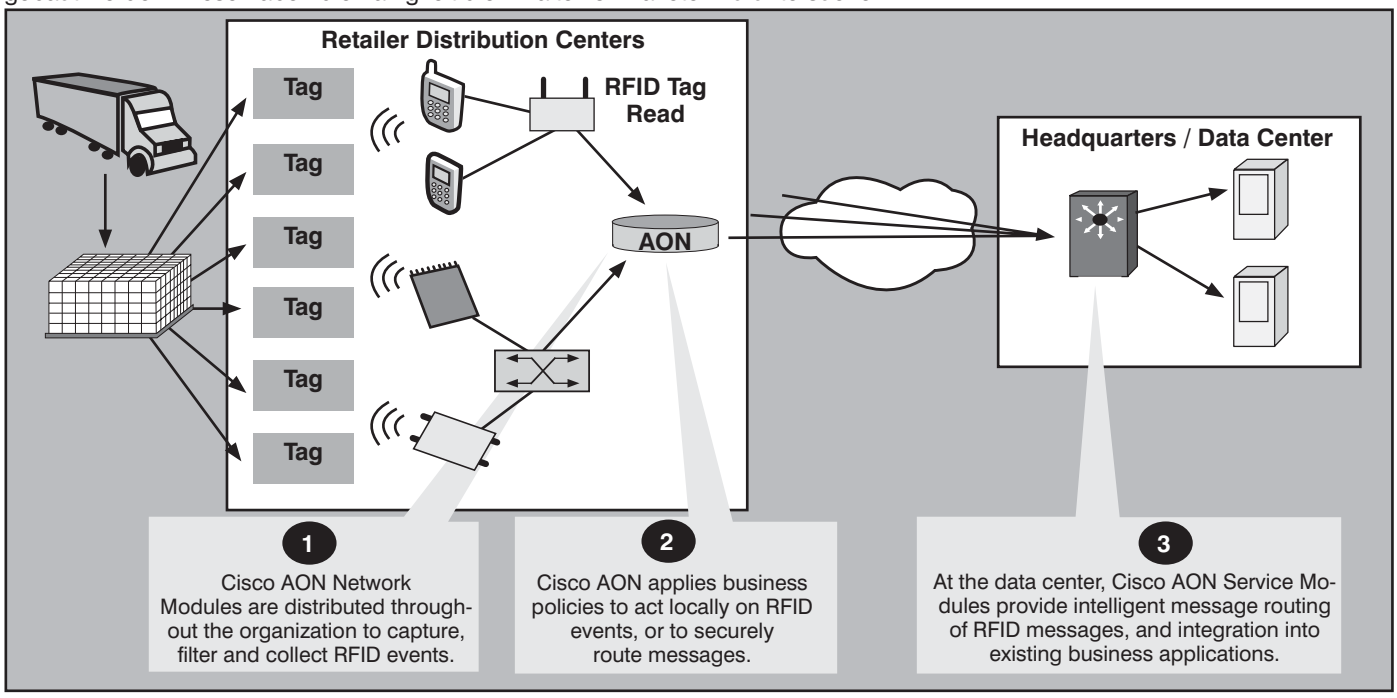
In diesen geschlossenen Prozessketten, die sich meist in der Produktionslogistik befinden, sollten Pilotprojekte implementiert werden. Hier bietet sich beispielsweise ein Werkzeugmanagement oder ein Containermanagement an. Auch eine Unterstützung bei der Anlagenwartung ist ein sinnvoller Einsatzbereich, wie beispielsweise die RFID-Lösung bei der Fraport AG zeigt. Hier wurden mit dem SAP mobile asset management und entsprechend ausgestatteten Handheld Computern die Wartung von sensiblen technischen Komponenten, wie Brandschutzklappen optimiert.

In der Realität zeigt sich, dass in der großen Anzahl der produzierenden Unternehmen bereits RFID-Pilotlösungen eingesetzt werden oder sich in der Umsetzung befinden. Überwiegend werden diese in Close-Loop-Systemen eingesetzt, eine solche Close-Loop-Lösung ist beispielsweise auch in der Automobilindustrie bei BMW realisiert, wo an den Produktionsförderanlagen RFID-Tags angebracht sind, die Informationen über das jeweils beförderte Fahrzeug enthalten.

An dem relativ breiten Einsatz von RFID in Close-Loop-Systemen, als auch an den sich mehrenden „Pilot"-Anwenungen in Open-Loop-Systemen zeigt, dass die Verbreitung von RFID Fahrt aufnimmt. Voraussetzung für den breiten und in Zukunft wahrscheinlich selbstverständlichen Einsatz von RFID-Tags ist eine entsprechende globale EPC-Unterstützung. Hier werden neben der Implementierung RFID-gestützter Prozesse in der nächsten Zeit große Herausforderungen liegen.

Cisco Application-Orientated Netorking

Da die Kommunikation der einzelnen Reader über Ethernet und IP durchgeführt wird, ist der Ansatz von Cisco die Middlewarefunktionalität in leistungsfähigen Netzwerkkomponenten zu integrieren. Eine auf diesem Ansatz basierende Lösung ist das Cisco Application-Orientated Networking (AON). Dies wird erreicht, indem in die jeweiligen modularen Switches oder Router AON-Module eingebaut werden. Diese haben die Fähigkeit die Inhalte von Paketen zu untersuchen.



Auf diese Weise können Inhalte von HTML, XML und anderen höheren Protokollen untersucht werden und anhand definierter Regeln bestimmte Aktionen durchgeführt werden. Damit es möglich sowohl die Funktionen des Daten-Layers, also das Sammeln und Filtern von Daten, als auch ein Eventmanagement zu implementieren. Das AON-Modul ist damit in der Lage z.B. Anzeigen zu steuern oder andere Application-Level Events zu generieren. Für die Entwicklung der Paketanalysen und Verarbeitungsmethoden auf Applikationsebene bietet Cisco ein AON Development Studio. Speziell für RFID-Lösungen können Application-Level Policies erstellt werden um bestimmte Funktionen auszuführen und ALEs zu generieren. Mit Hilfe einer AON Management Console können die einzelnen AON-Devices verwaltet werden.

Eine weitere sinnvolle Anwendung im RFID-Bereich ist die Cisco Wireless Locaten Service. Zunächst ist diese Wireless-Anwendung losgelöst von RFID. Mit Hilfe verschiedener Applikationen und entsprechenden Funktionen in den WLAN-Access-Points ist einerseits die Steuerung der Access-Points und die Erkennung von fremden Access-Points möglich. Außerdem kann in einer entsprechenden WLAN-Infrastruktur eine genaue Ortung der WLAN-Clients vorgenommen werden. Dieser Ansatz ist auch für RFID-Anwendungen im Rahmen des Asset-Tracking interessant. Werden Objekte mit aktiven RFID-Tags ausgestattet, kann über den Cisco Wireless Location Service ein genauer Standort bestimmt werden und abhängig davon können weitere Events und damit Prozesse ausgelöst werden.

Interessante Möglichkeiten ergeben sich in der Verbindung beider Services. So kann beim Einsatz von mobilen RFID-Scannern (tragbar oder auch an einem Gabelstapler) der Standort eines erfassten Objektes über den Wireless Location Service ermittelt werden, während die Daten des RFID-Tags über das WLAN an die zuständige Middlewareapplikation weitergeleitet werden. Die Scanner können in diesem Fall als eine Art ClassV-Tag angesehen werden.

IT-Sicherheits-Kongress

IT-Sicherheits-Forum 2006

Die Comconsult Akademie veranstaltet zusammen mit der GAI NetConsult GmbH Berlin vom 08. - 11. Mai das „IT-Sicherheits-Forum 2006“ in Bad Neuenahr.

Das IT-Sicherheits-Forum 2006 wird auch in diesem Jahr wieder die gerade aktuellen Themen zu Bedrohungsszenarien der IT-Sicherheit und zu den wichtigsten Schutzmaßnahmen aufgreifen. Dabei wird ein äußerst großer Wert auf Praxisnähe gelegt, dies zeigt sich insbesondere bei den technisch orientierten Workshops und den Praxisvorträgen, die direkt anwendbare „Tipps & Tricks“ für den Tagesbetrieb weitergeben. Das Forum hat sich deshalb in den letzten Jahren zu einem stark besuchten Treffpunkt für alle Sicherheitsinteressierten entwickelt. An insgesamt vier Tagen werden angeboten:

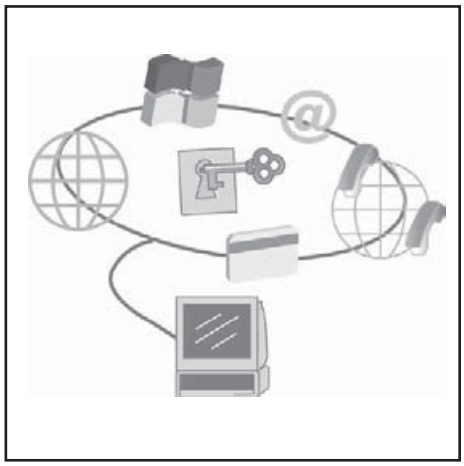
- Erfahrungen aus aktuellen Sicherheitsvorfällen und Aufzeigen absehbarer Trends
- Neue Entwicklungen bei Sicherheitstechnologie und Sicherheitsorganisation
- Moderierte Workshops mit Produktvergleichen und Live-Demos
- Vertiefende Seminare und Tutorien

Der (optionale) 1. Tag hat einführenden Charakter mit insgesamt drei parallelen Seminaren. Am 2. und 4. Tag werden durch erfahrene Referenten aktuelle Fachthemen analysiert und Praxisszenarien vorgestellt. Der 3. Tag ist mehreren Workshops für Produktvergleiche und Fallstudien zu aktuellen Sicherheitsthemen vorbehalten. Da diese parallel ablaufen, kann jeder Teilnehmer das für ihn optimale Programm selber zusammenstellen.

Als inhaltliche Schwerpunkte des IT-Sicherheits-Forums 2006 sind bisher vorgesehen:

Netzwerk-Redesign unter Sicherheitsaspekten
- Dezentralisierung der Netzgrenzen (deperimeterization)
- Überfällige Segmentierung des internen Netzes
- Identifikation und besonderer Schutz kritischer Systeme
- Anpassung von Identitäten, Zugriffskontrollen und Alarmierung

Gefahren durch zunehmende Kriminalisierung des Internets
- Industriespionage durch gezielte Spyware-Angriffe
- Massenattacken mit Phishing und Pharming
- Erpressungsversuche mit DDoS-Attacken



- Möglichkeiten des Identitätsdiebstahls

Application Security
- Neuartige Angriffe auf Webapplikationen
- Absehbares Gefahrenpotenzial bei Web-Services
- Sicherheit des SAP Enterprise Portals
- Schwachstellen bei Oracle DB

Best Practice Sessions (Praxistipps für typische Problembereiche)
- Sichere Konfiguration von Webbrowser und Webserver
- Aufbau einer sicheren Abwehr von Malware / Spyware
- Aufbau einer sicheren Adminumgebung
- Vorkehrungen für den sicheren Betrieb von mobilen Devices

Weiterhin sind folgende Themen vorgesehen:

Sicherheit bei Voice-over-IP
- Verwendete Technologien (SIP, H.323, proprietäre Protokolle)
- Schwachstellen und mögliche Angriffsszenarien
- Auswirkungen der Sicherheitsinfrastruktur auf die QoS bei VOIP
- Technische und organisatorische Schutzmaßnahmen

Sichere Nutzung von BlackBerry
- Analyse und Bewertung der Sicherheitsarchitektur
- Schutz der Übertragung, der Daten im Smartphone und des Mail-Servers
- Vorstellung zusätzlicher Schutzmaßnahmen
- Empfehlungen zum Einsatz von BlackBerry im Unternehmen

Schutz kritischer Infrastrukturen
- Ausfälle im Zusammenhang mit Fehlfunktionen der Informationstechnik
- Bedrohungen von SCADA-Systemen (Supervisory Control and Data Acquisition)
- BSI und seine Hilfsmittel zu KRITIS (Richtlinien, Sicherheitscheck)
- Grenzen der Zuständigkeit zwischen Unternehmen und Politik

Security Management
- Problem der fehlenden Sicherheitsstandards
- Lösungen zum Security Information Management (SIM)
- Event-Aggregation und Event-Correlation
- Probleme von SIM-Tools in stark heterogenen Netzen

Business Continuity Management
- Sicherung kritische Geschäftsprozesse bei Störungen oder Notfällen
- Best Practice Prozesse nach ITIL, BCI und DRII
- Vorgehensmodell: BIA, Strategie, Implementierung, Pläne, Tests
- Empfehlungen zum Tooleinsatz

Compliance / Risk Management
- Berücksichtigung staatlicher, industrieller und rechtlicher Vorgaben
- Informationssicherheit und Management von IT-Risiken
- Einschätzung der RM-Ansätze von BSI, ISO 17799 und IOS 13335
- Aufbau, Monitoring und Audit bei RM

Security Awareness und Governance
- Einbeziehung der IT-Prozesse in das interne Kontrollsystem
- Bekanntmachung und Durchsetzung einer SecPol im Konzernumfeld
- Durchführung einer Security Awareness-Kampagne

Das IT Sicherheits-Forum zählt seit Jahren zu den herausragenden Events im diesem Bereich. Das Programm aus Fachvorträgen hersteller-unabhängiger Referenten und Workshops mit live durchgeführten Produktvergleichen und Praxis-Demos hat einen hohen praktischen Wert für die Teilnehmer bewiesen. Daneben werden aber auch neue Entwicklungen aufgezeigt, die sowohl Bedrohungen als auch Schutzmaßnahmen umfassen. Diese eher technischen Informationen werden ergänzt durch Empfehlungen zur Sicherheitsorganisation und zu ihrer Einbettung in interne Geschäftsabläufe, da hier aller Erfahrung nach immer noch die größten Defizite anzutreffen sind. Damit spricht das IT Sicherheits-Forum sowohl Techniker als auch Manager an.

IT-Sicherheits-Kongress

10% Frühbucherrabatt bis 15.02.06

IT-Sicherheits-Forum 2006
08.05. - 11.05.06 in Bad Neuenahr

**4 Tage IT-Sicherheits-Forum 2006 mit „Tutorium“
zum Preis bei Buchung bis 15.02.06 von € 1.990,-
statt regulär € 2.190,- zzg. MwSt.**

**3 Tage IT-Sicherheits-Forum 2006 ohne „Tutorium“
zum Preis bei Buchung bis 15.02.06 von € 1.590,-
statt regulär € 1.790,- zzg. MwSt.**

Die Buchung innerhalb der Frühbucherphase ist verbindlich, kann aber jederzeit auf einen anderen Mitarbeiter Ihres Unternehmens übertragen werden.

Fax-Antwort an ComConsult 02408/955-399

Anmeldung
IT-Sicherheits-Forum 2006

Ich buche den Kongress
IT-Sicherheits-Forum 2006
vom 08.05. - 11.05.06 in Bad Neuenahr

☐ **mit Tutorium am ersten Tag**
zum Preis von nur € 1.990,- zzgl. MwSt.*

☐ **ohne Tutorium am ersten Tag**
zum Preis von nur € 1.590,- zzgl. MwSt.*
***gültig bis 15.02.06**

☐ **mit Report**
„Sicherheit in Enterprise-Netzen durch den Einsatz von 802.1X“
zum Preis von nur € 338,- zzgl. MwSt.

☐ **ohne Report**

☐ Bitte reservieren Sie für mich ein Hotelzimmer

vom_____bis_____06

Buchen Sie über unsere Web-Seite
www.comconsult-akademie.com

_____ Vorname

_____ Nachname

_____ Firma

_____ Abteilung

_____ Telefon

_____ Fax

_____ Straße

_____ PLZ,Ort

_____ eMail

_____ Unterschrift

Report des Monats

Neuerscheinung Februar 2006
Fehlersuche in konvergenten Netzen

Dieser Report gibt einen Leitfaden zur systematischen Fehlersuche mit einer umfangreichen Bewertung verfügbarer Hilfsmittel. Dieses umfassende Werk behandelt alle Aspekte der Fehlersuche in kabelgebundenen Netzwerken, vom physikalischen Kabel über Ethernet, Switching, TCP/IP, Windows bis zur Applikation. Lesen Sie im Folgenden eine kurze Leseprobe.

Low-Cost-Lösungen

Heute ist es in der Regel erforderlich, das Netzwerk- und Systemmanagement und damit auch die Fehlersuche nach den Vorgaben existierender Service Level zu gestalten. Das heißt im Klartext: die Bereitstellung und der Betrieb der IT-Lösungen hat auf einem hohem und gleich bleibendem Leistungsniveau zu erfolgen. Für die angebotene Dienstleistung werden immer höhere Leistungs- und vor allem Verfügbarkeitsanforderungen an den IT-Dienstleister herangetragen.

Unter diesen Voraussetzungen erlangen Begriffe wie Performance-Management und proaktives IT-Management eine völlig neue Bedeutung, und die erforderlichen Verfügbarkeiten setzen eine Fehlersuche mit optimaler Effizienz voraus. In dieser Situation kann nur überleben, wer auf eine geeignete Werkzeugunterstützung zurückgreifen kann.

Allerdings kann bei Beschaffung ausschließlich von High-End-Lösungen zur Abdeckung der Gesamtheit aller in der oben gezeigten Tabelle mit Funktionalitäten und Werkzeugtypen leicht Kosten in Höhe von mehreren 100 TEuro entstehen. Hier können Low-Cost-Tools eine echte Alternative sein. Bei überlegtem Rückgriff auf solche Lösungen können sich folgende Möglichkeiten ergeben:

- In kleineren Umgebungen wird man Service Level-fähig, ohne ein Missverhältnis zwischen IT - und Werkzeugkosten zu erzeugen.
- Die Einführung von Werkzeugen zum Service-Level-Management kann über Phasenkonzepte realisiert werden, ohne in frühen Phasen auf Wichtiges / Notwendiges zu verzichten.

- Spezialisten-Ausstattung kann durch Low-Cost-Tools sinnvoll ergänzt oder ein Mehrfachbedarf an Tools wirtschaftlich gestaltet werden.
- Ursprünglich „zentrale“ Tools könne mobil einsetzbar gemacht werden, um damit Fehlerdiagnose vor Ort zu betreiben.

Überlegungen in dieser Richtung ergeben natürlich nur Sinn, wenn auch ein geeignetes Angebot an Low-Cost-Lösungen vorhanden ist - und das ist der Fall! Neben „Light“-Versionen von großen Lösungen, die zur Verfügung stehen, werden mittlerweile auch Produkte gezielt mit „kompaktem“ Umfang zu niedrigen Preisen entwickelt. Eine weitere Bezugsquelle für Low-Cost-Tools ist das Internet. Hier erhältliche Tools muss man mittlerweile nicht mehr automatisch als Spielerei abtun: Auch wenn diese Tools nicht die Leistungsfähigkeit professioneller Tools erreichen, so können sie doch als Alternative angesehen werden.

Wer weiß, was er tatsächlich und mit welchen Schwerpunkten braucht, kann also gezielt eine gesunde Mischung aus High-End-Lösungen und Low-Cost-Ergänzungen zusammenstellen bzw. gezielt in die High-End-Ausstattung hineinwachsen.

Beispiel „Multi Router Traffic Grapher“

Als erstes Beispiel für die Einsatzmöglichkeiten von Low-Cost-Tools wird hier das vielleicht bekannteste Open-Source-Tool kurz vorgestellt mit seinen Möglichkeiten für die Fehlersuche: MRTG ist eine Tool mit dem man nicht nur Verkehrsdaten eines Netzwerkes aufzeichnen kann.

MRTG basiert auf den Programmiersprachen Perl und C und ist somit nahezu Betriebssystem-unabhängig. Eine detaillierte Auflistung der Installationsvoraussetzungen, eine recht leicht verständliche Dokumentation sowie das Tool selbst sind im Internet unter www.mrtg.org zu finden.

Die von MRTG gesammelten Daten werden in Logdateien abgelegt, die automatisch so konsolidiert werden, dass sie nicht unaufhörlich wachsen und dennoch alle erforderlichen Daten enthalten um auch Langzeitstatistiken (bis zu zwei Jahren) erstellen zu können. Allerdings bedeutet die gewählte Konsolidierungsmethode frühen und unwiederbringlichen Verlust der Detaildaten.

Die Darstellung der gesammelten Daten erfolgt durch die Generierung von HTML-Seiten mit einer Real-Time-Anzeige der abgefragten Werte in Form von PNG-Images. (siehe Abbildung 25)

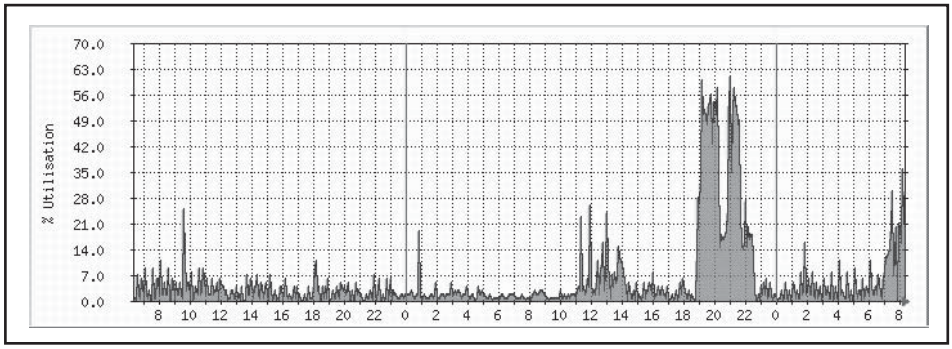


Abbildung 25: Port-Auslastung, ermittelt mit MRTG

Als Datenquelle für die Abfrage mit MRTG dienen in der Regel beliebige MIB-Variablen, die von einem SNMP-Agenten zur Verfügung gestellt werden kann. Und wies sieht es mit der Einbindung neuerer Themen und Produkte aus? Kein Problem: MRTG bietet die Möglichkeit, MIBs zu laden und somit auch Werte neuester Technik abzufragen.

Für den Fall, dass sich der gewünschte Anzeigewert aus mehreren Parametern zusammensetzt (z.B. die Port-Auslastung in %), können auch Formeln aus den MIB-Variablen gebildet werden. MRTG zeigt dann den Ergebniswert zur Formel. Ob aufwändigere Formel oder nur Darstellung eines aus einer abfragefähigen Quelle gewonnenen Einzelwerts, immer muss man eine bestimmte Abfolge von Schritten durchlaufen, um MRTG entsprechend vorzubereiten.

Dies wird im folgenden Beispiel erläutert.

1. Schritt:
Hier muss mit der folgenden Befehlszeile eine Basiskonfigurationsdatei erstellt werden.

perl cfgmaker read-community@IP-Adresse --global „WorkDir: beliebiges Verzeichnis“ --global „RunAsDaemon: Yes“ --output Dateiname.cfgzum

Beispiel:
perl cfgmaker public@149.224.129.14 --global „WorkDir: e:\mrtgdata\switch“ --global „RunAsDaemon: Yes“ --output switch.cfg

2. Schritt:
Nun werden globale Parameter durch bearbeiten der erstellten cfg-Datei mit einem Texteditor festgelegt

Zu diesen Parametern gehören:
- Arbeitsverzeichnis
- Dienstparameter
- Grafische Parameter
- Beschriftungsparameter

3. Schritt:
Festlegen der Abfrage-Werte.
Wie diese Festlegung erfolgt, wird am Beispiel des Aspekts „Auslastung eines Links“ erläutert.

Die Auslastung ist keine SNMP-Variable, die abgefragt werden kann, sondern wird ermittelt über eine Formel, die sich aus einzelnen SNMP-Variablen zusammensetzt. MRTG fragt diese SNMP-Variablen ab, errechnet mit der gewünschten Formel die Ergebnisse und stellt dies grafisch dar.

Die Formel für die Auslastung wird nun wie folgt aufgebaut:

$$\text{„Auslastung“ (in\%)} = \left(\frac{(\text{„InOctets“} + \text{“OutOctets“}) * 8}{\text{„max.Linkspeed“}} \right) * 100$$

Für die einzelnen SNMP-Variablen müssen die Objekt-Ids ermittelt werden, hier etwa folgende Werte:
InOctets => 1.3.6.1.2.1.2.2.1.10
OutOctet => 1.3.6.1.2.1.2.2.1.10

Die außerdem für die Formel notwendige max. Linkspeed wird von MRTG ermittelt.

Diese Informationen müssen nun in die Formel eingebaut und in eine für MRTG „verständliches“ Format gebracht werden:

((1.3.6.1.2.1.2.2.1.10.Interface-Nummer & 1.3.6.1.2.1.2.2.1.10.Interface-Nummer:Read-Community@IP-Adresse + 1.3.6.1.2.1.2.2.1.16.Interface-Nummer & 1.3.6.1.2.1.2.2.1.16.Interface-Nummer: Read-Community@IP-Adresse) / (Bandbreite/8)) * 100

4. Schritt:
Setzen des Maximal-Wertes
Die Festlegung des Maximal-Wertes ist notwendig, damit MRTG die Ergebnisse richtig berechnet und diese auch richtig in der Grafik dargestellt werden. Diese Festlegung erfolgt ebenfalls in der Konfigurationsdatei, und zwar wie folgt:

```
###Interface 1 >> Descr: ‚Serial2/0:1.142‘ | Name: ‚Se2/0:1.142‘ | Ip: ‚149.224.129.250‘ | Eth: ‘###
Target[149.224.129.250_1]: (( 1.3.6.1.2.1.2.2.1.10.1&1.3.6.1.2.1.2.2.1.10.1:public@149.224.129.250+
1.3.6.1.2.1.2.2.1.16.1&1.3.6.1.2.1.2.2.1.16.1:public@149.224.129.250) / (248000/8) ) * 100
SetEnv[149.224.129.250_1]: MRTG_INT_IP=“10.144.115.234“ MRTG_INT_DESCR=“Serial2/0:1.142“
MaxBytes[149.224.129.250_1]: 100
Title[149.224.129.250_1]: Traffic Analysis for 1 -- switch
PageTop[149.224.129.250_1]: <H1>Traffic Analysis for 1 -- switch </H1>
<TABLE>
```

5. Schritt:
Starten der Abfrage
Der Befehl zum Starten von MRTG muss im bin-Verzeichnis von MRTG mittels Kommandozeile ausgeführt werden. Nach dem Start des Prozesses darf das Fenster nicht geschlossen werden.

Der Befehl zum Starten sieht wie folgt aus:
perl mrtg Dateiname.cfg

Die Ausgabe erfolgt als html-Datei, die im zuvor festgelegten Arbeitsverzeichnis abgelegt wird und sieht nach erfolgreicher Konfiguration wie folgt aus. (siehe Report)

Mit derart einfachen Mitteln ist es also möglich, Statistikkurven auch zu Werten erzeugen zu lassen, die nicht als einzelne Parameter im Rahmen der Permanentüberwachung bereits kontinuierlich aufgenommen werden. Benötigt man also etwa im Rahmen einer Diagnose eine Statistikkurve zu einem etwas „ausgefalleneren“ Aspekt, so setzt man eine geeignete Formel zusammen und kann loslegen - und das auch vor Ort auf einem mobilen Rechner.

Man kann mit Hilfe der Grafikerzeugung durch MRTG sogar noch weiter gehen und über zusätzliche Scripte andere Quellen nutzen, z.B. den Microsoft Performance-Monitor unter Windows. Somit ist es z.B. möglich, die CPU-Auslastung eines Servers, freien Festplattenplatz, die CPU-Temperatur usw. aufzuzeichnen. Auch Freunden des „Motherboard Monitor“ kann geholfen werden - findige Programmierer der Internetgemeinde bieten frei verfügbare Scripte zur Abfrage von Werten wie Lüftergeschwindigkeit, Boardspannung, Memory-Temperatur usw.

Durch Zusatztools wie „GoofyTG“ (http://wizardsworks.org/GoofyTG/) von Greg Chandler ist es weiterhin möglich, Funktionalitäten komponentenspezifischer Tools wie „CiscoView“ nachzuahmen. „GoofyTG“ stellt HTML-Seiten mit Komponentenimages zur Verfügung bei denen portspezifische MRTG-Grafen durch einen Klick auf einzelne Ports angezeigt werden.

Auch Applikationsüberwachung ist mit entsprechenden Open-Source-Lösungen in begrenztem Umfang möglich. Die Abfrage von Werten wie Sessions auf einer Firewall, Auslastung einzelner Prozesse oder ein- und ausgehenden E-Mails - um nur 3 Beispiele zu nennen, ist realisiert worden. Abbildung 11.28 zeigt die Überwachung des Traffic durch eine „Trend Viruswall“. (siehe Report)

MRTG plus „Zubehör“ kann also prinzipiell schon eine Menge. (siehe Tabelle 14)

Allerdings bleibt der Pferdefuss der für Langzeitmessungen nur mäßig geeigneten Datenhaltung. Zwar ist die Durchführung einer Langzeitmessung erst zur Fehlerdiagnose keine geeignete Maßnahme, da hier ja der Zeitdruck viel zu groß istur Gewinnung von Vergleichswerten (Referenzmessungen) für die Fehlerdiagnose sind solche Langzeitmessungen aber doch wieder Fehlersuche-relevant. Daher soll auch dieses Thema kurz beleuchtet werden.

Hat man zu anderen Zwecken, etwa zur Erfülllung von Berichtspflichten im Rahmen eines Service Level Management, bereits Investitionen in entsprechende Reporting-Tools getätigt, so wird man selbstverständlich zunächst diese nutzen. Auch solche oft schon sehr umfangreichen Angebote können aber im Falle besonderer Überwachungswerte eine Lücke aufweisen. Diese lässt sich dann mit einer Low-Cost-Lösung füllen. Für kleinere Umgebungen lohnen sich kommerzielle Lösungen womöglich aus wirtschaftlichen Gründen nicht / nicht sofort, und man kann einen Grundvorrat von langfristigen Referenzmessungen (Trendanalyse) ausschließlich mit Hilfe solcher Low-Cost-Ansätze sicherstellen.

Ein möglicher Kandidat hierfür ist das im nächsten Abschnitt vorgestellte RRDtool.

Diese Studie eine wertvolle Hilfe und Ergänzung sowohl für jeden Betreiber als auch für Nutzer von IT-Netzen und für jeden Mitarbeiter im Trouble-Shooting-Bereich dar, die sich bereits nach kleinen Störfällen amortisiert haben wird.

Allgemeine Fragen	Antworten
Datenaufbereitung?	Real-Time- und Langzeitanzeige in verschiedenen Grafen
Darstellungsmöglichkeiten?	lediglich Kurvendiagramme
Auswertemöglichkeiten?	durch MRTG oder Export der Daten nach Excel etc.
Datenhaltung?	ASCII-Dateien, die regelmäßig überschrieben werden
Datengewinnung?	ständiges Abfragen (Polling) der gewünschten Variablen
Vorbereitungen?	PC mit Betriebssystem, Download und Installation von Perl und MRTG
Einrichtungsaufwand?	abhängig von der Anzahl der zu überwachenden Komponenten und dem Know-how des Einrichters
Einbindungsmöglichkeiten?	ja, z.B. in HP OpenView Network Node Manager
nächste Release?	ja
Billing- und SLM-relevante Daten?	in begrenztem Umfang und über Zusatztools
themenspezifische Fragen	**Antworten**
Betriebssysteme?	alle gängigen Betriebssysteme SNMP Versionen?
SNMP Versionen?	SNMPv1 und SNMPv2c
IPv6?	ja
VLANs?	ja
Wireless LAN?	ja
DHCP, DNS, WINS, NIS, etc?	ja
Verschlüsselung, RADIUS, etc.?	bedingt
Applikationen überwacht?	bedingt
Schwellwertüberwachung?	ja
«Ende zu Ende»-Überwachung?	ja, allerdings nur durch Zusatztools

Tabelle 11.4: Werkzeuganalyse MRTG + Erweiterungen

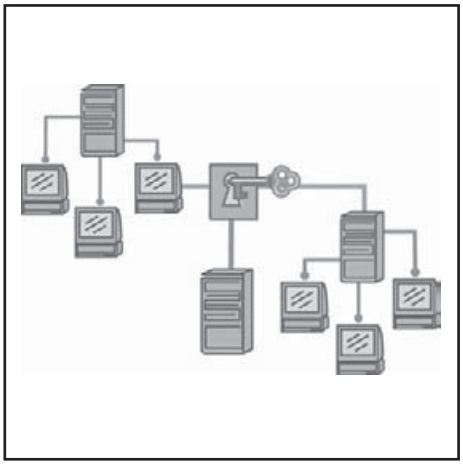
Neues Seminar

Sicherheit im Netzwerk: Trennung von Benutzergruppen und Zugriffsschutz auf Benutzer-Ebene

Die Comconsult Akademie veranstaltet vom 24. - 26. April erstmalig ihr neues Seminar “Sicherheit im Netzwerk: Trennung von Benutzergruppen und Zugriffsschutz auf Benutzer-Ebene“ in Aachen.

Dieses Seminar richtet sich an Planer und Betreiber von Netzwerken mit einer Zentralen Authentifizierung. Weitere Schwerpunkte sind die Einräumung von Zugangsrechten, die Überprüfung von Patchleveln vor dem Netzwerk-Access und die Überwachung des Netzes auf abnormales Verhalten.

Seit der Einführung von WLANs ist die Authentifizierung zum Thema auch für Lokale Netze geworden, schließlich möchte man sein Netz nicht via WLAN vom Parkplatz aus für die breite Öffentlichkeit zugänglich machen. Die Zugangskontrolle ist jedoch ein isoliertes WLAN Problem, das sich auf die Frage „Wer darf rein und wer nicht?“ reduzieren lässt. Zum einen will man nun einen kontrollierten Zugang, d.h. nicht jeder, dem ein WLAN-Zugang eingeräumt wird, darf auch alles (bspw. Gastzugänge, externe Berater, Hot-Spots). Zum anderen ist Authentifizierung nicht auf die kabellose Umgebung beschränkt: für WAN/VPN-Zugriffe ist sie schon lange etabliert.



Netzwerksicherheit beschränkt sich aber nicht auf den Zugriffschutz und die Einschränkung von Benutzerrechten, denn auch zugangsberechtigte Maschinen und Personen können Gefahrenquellen sein. Für einen entsprechend hohen Sicherheitsbedarf muss zusätzlich das Netz auch überwacht werden.

Dieses Seminar richtet sich an Planer und Betreiber von Netzwerken mit einer Zentralen Authentifizierung für verschiedene Zugangsverfahren. Weitere Schwerpunkte sind die über die reine Authentifizierung hinausgehende Einräumung von Zugangsrechten, die Überprüfung von Patchleveln vor dem Netzwerk-Access und die Überwachung des Netzes auf abnormales Verhalten.

In diesem Seminar lernen Sie

- welche Bereiche müssen geschützt werden?
- was ist der Stand der Technik:
  - welche Standards gibt es?
  - wie funktionieren die Herstellerlösungen?
- wie sieht eine bedarfsgerechte Lösung aus?
  - was ist wann sinnvoll?
  - worauf muss man achten?
  - was sind typische Fallstricke?
  - welche Möglichkeiten und Grenzen gibt es?

Fax-Antwort an ComConsult 02408/955-399

Anmeldung

Sicherheit im Netzwerk: Trennung von Benutzergruppen

☐ Ich buche das Seminar
Sicherheit im Netzwerk:
Trennung von Benutzergruppen
vom 24. - 26.04.06 in Aachen
zum Preis von € 1.690,- zzgl. MwSt.

☐ Bitte reservieren Sie für mich
ein Hotelzimmer
vom_____bis_____06

Buchen Sie über unsere Web-Seite
www.comconsult-akademie.com

_____ Vorname	_____ Nachname
_____ Firma	_____ Telefon/Fax
_____ Straße	_____ PLZ,Ort
_____ eMail	_____ Unterschrift

ComConsult Veranstaltungskalender

Aktuelle Veranstaltungen

Projektmanagement I:
Projekte erfolgreich leiten, organisieren und optimieren, 13. - 17.02.06 in Bonn

In diesem 5-tägigen Intensiv-Kurs lernen Sie, ein Projekt erfolgreich zu leiten und organisieren. Es werden bewährte Wege aufgezeigt, wie Sie die Projektabwicklung im Alltag in Ihrem Unternehmen konkret optimieren.

Preis: € 2.290,- zzgl. MwSt.

TCP/IP und SNMP - Intensiv Seminar, 13.02-17.02.06 in Bonn

Dieses 5-tägige Seminar vermittelt systematisch die Grundlagen TCP/IP, beleuchtet Vor- und Nachteile und gibt wichtige Empfehlungen für den erfolgreichen Einsatz. Dies betrifft speziell auch die wichtigen IP-Infrastrukturdienste von der Adressierung über ARP bis zu DHCP, DNS, DDNS und NAT und die Management-Funktionalität SNMP.

Preis: € 2.290,- zzgl. MwSt.

Session Initiation Protocol - Basis-Technologie der IP-Telefonie, 13.02-15.02.06 in Köln

Dieses 3-tägige Seminar vermittelt Planern und Betreibern Anforderungen und Technologien für den Einsatz von Telefonie und Mehrwertdiensten auf Basis des neuen Standards SIP. Chancen und Risiken werden anhand von Einsatzszenarien bewertet und kontrovers diskutiert.

Preis: € 1.690,- zzgl. MwSt.

Ethernet Technologien neuester Stand, 20. - 24.02.06 in Aachen

Dieses Seminar stellt die neuesten Ethernet- und Wireless-Varianten vor und zeigt, nach welchen Regeln und Auslegungsvorschriften diese zu konfigurieren sind. Mit besonderem Blick auf die Praxis werden Komponenten- und Kabeltechnik erläutert, auch wichtige Betriebsfragen werden vorgestellt. Im Besonderen wird die Bedeutung der IP-Telefonie für die Gestaltung von Ethernet-LANs analysiert. Abgerundet wird das Seminar um wichtige Fragen des Trouble-Shootings.

Preis: € 2.290,- zzgl. MwSt.

WAN-Planung für zentrale Dienste, 20. - 22.02.06 in Köln

Wide Area Networks (WAN) müssen kostengünstig, leistungsfähig, skalierbar, hochverfügbar, sicher und managebar sein. Während bis vor wenigen Jahren langfristige WAN-Verträge von drei bis fünf Jahren abgeschlossen wurden, legt die dynamische Entwicklung nahe, die Vertragsbindung zu verkürzen, was mit einem ständigen Planungsprozess einhergeht. Dieser Umstand und die fortlaufenden Veränderungen im Markt zwingen zu einem permanenten Lern- und Informationsprozess.

Preis: € 1.690,- zzgl. MwSt.

Sicherheit im LAN mit IEEE 802.1X, 20. - 21.02.06 in Köln

Dieses 2-tägige Seminar vermittelt den optimalen Umgang mit IEEE 802.1X, erläutert die Einsatzvarianten, beschreibt die gegebenen Fallstricke und liefert die ideale Basis zur Vorbereitung eines Einsatzes.

Preis: € 1.390,- zzgl. MwSt.

IP-Telefonie: Markt und Produkte in der Analyse, 20. - 22.02.06 in Aachen

Die Auswahl eines geeigneten Produkts für IP-Telefonie ist für jedes Unternehmen nicht leicht. Hier setzt die 3-tägige Sonderveranstaltung an, die Sie umfassend in Markt und Produkte einführt. Sie erfahren, was IP-Telefonie-Produkte leisten, worauf Sie bei der Auswahl achten müssen, wo Probleme liegen und welche Strategien ausgewählte Hersteller verfolgen.

Preis: € 1.990,- zzgl. MwSt.

Internetworking:
optimales Netzwerk-Design mit Switching und Routing, 06. - 10.03.06 in Aachen

Dieses 5-Tages-Intensiv-Seminar vermittelt dem Einsteiger Methoden und Technologien zur erfolgreichen Strukturierung von Enterprise Netzwerken. Dabei wird das komplette Spektrum vom L2/L3 Switching über Redundanz/Routing bis hin zu Themen wie VLAN, WLAN-Integration, Multicast-Routing, VPN, MPLS, abgedeckt. Es werden sowohl die theoretischen Hintergrundkenntnisse als auch die Konsequenzen für den praktischen Betrieb von Netzwerken dargestellt.

Preis: € 2.290,- zzgl. MwSt.

IP-Telefonie: Vorbereitung, Migration, Management, 06. - 08.03.06 in Düsseldorf/Kaarst

Die Referenten dieses 3-tägigen Seminars vermitteln ihre jahrelangen Projekt-Erfahrungen bei der Nutzung und des Betriebs von IP-Telefonie sowie bei der Durchführung hochkomplexer Projekte in diesem Umfeld.

Preis: € 1.690,- zzgl. MwSt.

Planung und Betrieb mobiler Kommunikation, 06. - 07.03.06 in Düsseldorf/Kaarst

Dieses Seminar analysiert die beim Betrieb von mobilen Teilnehmern und Geräten zu lösenden Aufgaben und gibt Empfehlungen zur optimalen Umsetzung. Auch die typischen Fallstricke werden benannt. Auf der Basis von vielen Beispielen wird die geeignete Handhabung der verschiedenen Technikbereiche erklärt.

Preis: € 1.390,- zzgl. MwSt.

Sicherheit 2: VPN Virtuelle Private Netze:
Planung, Konfiguration, Betrieb, 20.03. - 22.03.06 in Bad Neuenahr

VPN-Technologie sind ein unverzichtbarer Teil jeder Netzwerk-Sicherheits-Lösung. Ebenso vielfältig wie die Nutzungsformen sind die Realisierungs-Alternativen und die Integration in bestehende Netzwerk-Infrastrukturen. Dieses 3-tägige Seminar bewertet die bestehenden Alternativen und gibt direkt in der Praxis umsetzbare Empfehlungen zur optimalen Nutzung von VPN-Technologien.

Preis: € 1.690,- zzgl. MwSt.

Projektmanagement II: Sitzungen moderieren, Projekte präsentieren, erfolgreich verhandeln und Projektteams leiten, 20.03. - 24.03.06 in Aachen

In diesem 5-tägigen Intensiv-Seminar steht das Führungsverhalten des Projektleiters eindeutig im Mittelpunkt. Professionelles Moderieren, Präsentieren, Verhandeln und Teamleiten ist eine Kunst, die trainierbar ist. Anhand begleitender Rollenspiele und Praxisübungen werden die führungsrelevanten Eigenschaften klar verbessert.

Preis: € 2.290,- zzgl. MwSt.

Schwerpunktthema

Gefahrenmeldetechnik und Objektüberwachung über IP-basierende Netze

Fortsetzung von Seite 1

Im Anschluss an sein Studium als Nachrichtentechniker spezialisierte sich Dipl.-Ing. Hartmut Kell auf die Datenkommunikation in lokalen Netzen und kann bis heute auf eine mehr als 10-jährige Berufserfahrungen in diesem Bereich verweisen. Als langjähriger Mitarbeiter der ComConsult Beratung und Planung GmbH hat er umfangreiche Praxiserfahrungen bei der Planung, Projektüberwachung, Qualitätssicherung und Einmessung von Netzwerken gesammelt. Ergänzend zu diesen projektbezogenen Arbeiten vermittelt Herr Kell sein umfangreiches Fachwissen in Form von Fachpublikationen und Seminaren.

Auf Basis der bisherigen Erfahrungen kann prognostiziert werden, dass die IT-Spezialisten mit der Devise „IP kann alles“ in die Diskussion starten und die Überwachungsspezialisten sich in großen Teilen mit dem Motto „IP ist zu unsicher“ vehement gegen die neue Technik wehren werden.

Im Oktober 2005 hat die ComConsult Akademie und ComConsult Beratung und Planung GmbH das Thema „Gefahrenmeldetechnik und Objektüberwachung im IP-Netz“ mit Hilfe eines eigenständigen, zweitägigen Kongresses zunächst an die Zielgruppe der IT-Spezialisten adressiert. Ziel des Forums war es, die Technologie-, Markt- und rechtliche Situation zu analysieren und Empfehlungen zur Einführung dieser neuen Techniken zu geben. Dabei wurde neben dem Dialog auch die kontroverse Diskussion mit „der anderen“ Seite, den Überwachungsspezialisten, gesucht, indem einzelne Vorträge von Fachleuten aus diesem Kreis gehalten wurden. Die Resonanz war unerwartet groß, sowohl die Anzahl der Teilnehmer als auch das Interesse während des Forums. Aus diesem Grunde lag es nahe, die wichtigsten Inhalte und Aussagen des Forums in einem Netzwerk Insider-Artikel zu publizieren und damit einem breiteren Leserkreis deutlich zu machen, dass

- es erste Lösungen auf dem Markt gibt, die eine weitere Konvergenz der Netze möglich machen;
- viele vorhandene IP-Netzinfrastrukturen bereits heute in der Lage sind diese neuen Techniken einzuführen;
- die Ablösung der alten Techniken aber weder vollständig noch kurz- oder mittelfristig erfolgen wird;
- eine Einführung nur in enger Abstimmung mit den Überwachungsspezialisten sinnvoll sein kann.

Dieser Artikel wird neben einer Beschreibung der allgemeinen Ziele und Probleme dieser Konvergenz die besonders heiklen Fragen nach einer ausreichenden Verfügbarkeit, Sicherheit und ersten Lösungsmöglichkeiten (am Beispiel der Videoüberwachung) aufgreifen, er soll Basis für weitere Diskussionen sein.

Sinn und Zweck der Integration

Beginnen wir mit der Frage, was zu dem Bereich der Gefahren- und Meldetechnik gehört? Einige Varianten sind jedem geläufig, Brandmeldetechnik, Einbruchtechnik, Zugangskontrolle und Videoüberwachung gehören dazu. Doch damit hört das Spektrum nicht auf, auch Bereiche wie Fluchtwegesteuerung, Lichtruf, Zeiterfassung, Aufzugsteuerung, Zaunüberwachung sind zu nennen, diese sind in ihrem Grundprinzip eher passive Techniken, rein „meldende“ Techniken. Daneben existieren aktive Techniken, also Lösungen, bei denen etwas gesteuert wird. Beispiele hierfür sind Rolladensteuerungen, Heizungen, Lüftungen, Notstromversorgungen oder auch Sprachkommunikation. Lässt man einmal die Sprachkommunikation außer Acht, hier wird die Gegenwart bereits durch die IP-basierende Technik VoIP bestimmt, so werden heute fast alle aufgelisteten Melde- und Steuerungstechniken mit Hilfe von eigenständigen, weitestgehend inkompatiblen Lösungen realisiert. Es werden weder einheitliche Verkabelungen, noch einheitliche aktive Hardware- oder Software-Komponenten eingesetzt. Auch im Bereich der Protokolle ist man noch weit von einheitlichen Standards entfernt. Eine Metapher aus einem der Vorträge beschreibt die Situation in der Protokollwelt sehr gut: Der Turmbau zu Babel scheiterte an der Vielfalt der Sprachen, keiner wollte seine Sprache aufgeben und der Turm wurde nie fertig. Wenn sich diese Situation im Gefahrenmeldebereich wiederholen sollte, so wird eine Konvergenz der Techniken nur sehr schleppend stattfinden (man vergleiche die bis heute andauernde, relativ langsame Einführung der Ethernet-Technologie im Industrie-Bereich).

Eine Vereinheitlichung der Techniken und Integration in die IP-basierende Welt („ein Netz für alles“) würde mehrere Vorteile mit sich bringen. Da ist zunächst einmal die Nutzung einer zentralen Plattform zu nennen, von der aus viele Sicherheits- und Gebäudetechniken, z.B. über eine WEB-Oberfläche, zentral und einheitlich überwacht und gesteuert werden können. Mit Hilfe von visuellen Verknüpfungen ließen sich z.B. über einen CAD-Grundrissplan solche Gebäudetechniken erfassen, überwachen oder auch steuern. Das Beispiel der „Buchung von Besprechungsräumen“ aus einem Vortrag des Forums veranschaulicht eine weitere Entwicklung dieses integrativen Ansatzes: In Outlook wird ein Besprechungsraum gebucht, anschließend wird automatisch geprüft, ob der Raum, die Technik und die Teilnehmer verfügbar sind. Sind entsprechende Verfügbarkeiten gegeben, wird der Raum reserviert und die Teilnehmer werden per E-Mail eingeladen. Der Einlass der Teilnehmer könnte zudem über RFID-Chips kontrolliert werden. Mit Beginn und im Laufe der Besprechung werden im Raum Klima, Lüftung, Verdunkelung, Licht automatisch passend zur Anzahl der Teilnehmer sowie zur Jahres- und Tageszeit eingestellt.

Ein weiterer bedeutender Vorteil liegt in der Verwendung von Standardprodukten

Gefahrenmeldetechnik und Objektüberwachung über IP-basierende Netze

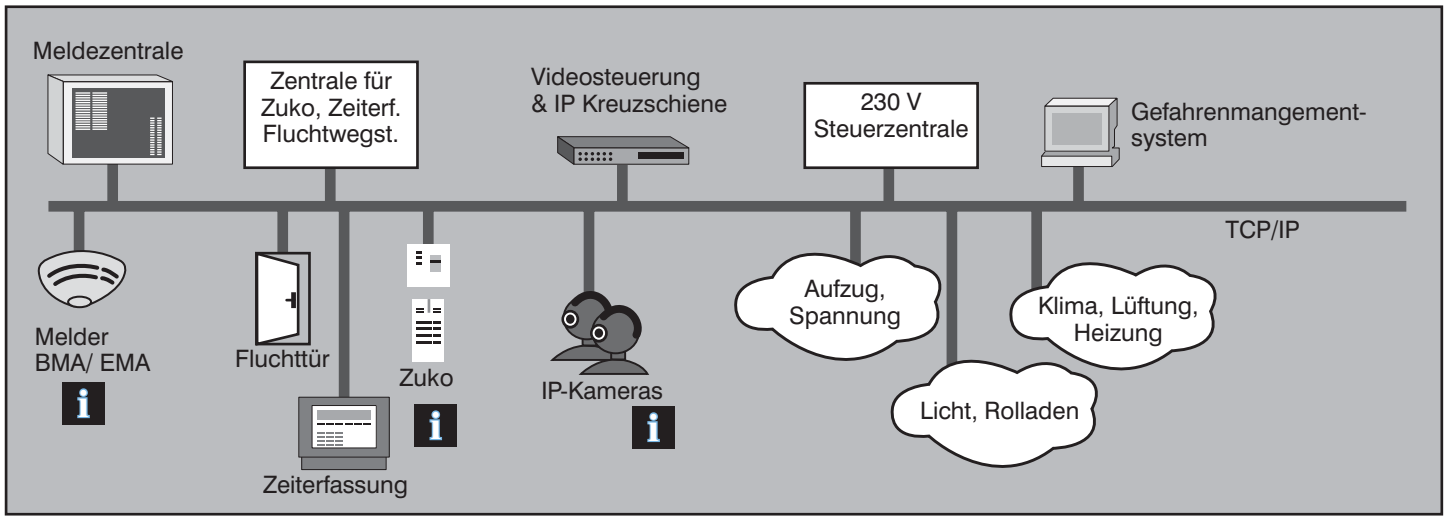


Abbildung 1: Integration morgen (Bild: SSM-Gruppe)

und wenigen standardisierten Protokollen. Dies würde zu einer deutlicheren Herstellerunabhängigkeit führen, gefolgt von geringeren Investitionskosten.

Aktuelle Lösungen beschränken sich jedoch zumeist noch auf das erwähnte zentrale, manuell gesteuerte Gebäudemanagement unter Hinzunahme von IT-Servern und speziellen Konvertern, die für eine Umsetzung der notwendigen proprietären Protokolle ins IP-Protokoll genutzt werden. Am weitesten fortgeschritten bei der Integration in IP-Netze ist neben der Sprachkommunikation/Überwachung (VoIP) mit Sicherheit die Video-Überwachung, hier gibt es bereits umfangreiche Produkte, deren Einsatz einen nennenswerten Mehrwert mit sich bringen kann.

Neben den angesprochenen Schwierigkeiten bei der Vereinheitlichung bzw. Standardisierung der Techniken gibt es noch einen weiteren Grund, der die Integration erheblich bremst. Dies ist die Unsicherheit, ob die existierenden IP-Netzwerke in der Lage sind, eine ausreichende Verfügbarkeit und Sicherheit bereitzustellen und vor allem, ob dies auch aus Sicht der entsprechenden Normierungs- und Zertifizierungsinstitutionen so gesehen wird.

Verfügbarkeit

Wie bereits bei der Einführung von VoIP oder Industrial Ethernet wurde seitens der Spezialisten aus der klassischen Sprachkommunikation oder Automatisierungstechnik der neuen Technik der Vorwurf gemacht, dass derartige Kommunikationsabläufe nicht über derart „unsichere“ Technologien realisiert werden können bzw. dürfen. Die Realität zeigt jedoch, dass sich dieses Vorurteil nicht halten kann. Auf der einen Seite ist festzuhalten, dass bereits die typischen IT-Applikationen wie E-Mail-System, SAP oder andere eine derart hohe Verfügbarkeit an das Netz stellen, dass ein Netzausfall „nur“ bei diesen Diensten bereits zu einer Katastrophe für ein Unternehmen führen kann; man stelle sich die Frankfurter Börse mit einem LAN-Zusammenbruch vor. Ist die Verfügbarkeitsanforderung anders bei einer Abbildung von Gefahren- und Meldediensten auf einem IP-Netz? Diese Frage ist ohne Zweifel mit „ja“ zu beantworten, der einfache Grund liegt darin, dass die meisten IT Dienste bei Versagen heute keinen direkten Einfluss auf die Unversehrtheit von Gebäuden oder gar Menschen nehmen, was bei einer Nutzung des IT-Netzes z.B. durch eine Brandmeldeanlage anders wäre. Demzufolge ergibt sich die Schwierigkeit, dass - selbst bei einer technischen Lösung für IP-basierende Gefahren- und Meldesysteme - grundsätzlich eine normative Instanz wie z.B. eine staatliche Einrichtung oder eine Institution wie der Verband der Sachversicherer diese Lösung freigeben muss. Diese Notwendigkeit wird sicherlich zu einem verlangsamten Einzug der neuen Techniken führen und es muss der Dialog mit den freigebenden Institutionen gesucht werden. In jedem Falle sind folgende Fragen unbedingt zu analysieren und zu beantworten:

- Können sich kritische Systeme und Gewerke auf das IP-Netz verlassen?
- Ist es fahrlässig, Menschenleben Systemen anzuvertrauen, die über IP miteinander kommunizieren?
- Kann man sorgenfrei die herkömmlichen Netzstrukturen 1:1 auf kritische Bereiche übertragen?
- Was ist zu machen, damit die erforderliche Verfügbarkeit von IP-Netzen erreicht wird?
- Was setzt heute die IP-Netze außer Gefecht?

Um eine IT-Anwendung erfolgreich nutzen zu können, müssen viele Dinge funktionieren. Dabei ergibt sich die Gesamtverfügbarkeit aus einer Kette von Einzelverfügbarkeiten. Die Kette ist im Wesentlichen vom schwächsten Glied abhängig und es nützt nichts, ein einzelnes Glied besonders stark zu machen und gleichzeitig bei scheinbar weniger wichtigen Punkten nachlässig zu werden. Was nützt ein hochredundanter Switch Core, wenn der Standortverteiler, also der Hauptverteiler eines Campus-Netzes, in einer Teeküche aufgebaut wird?

Was ist also zu beachten? Nach allgemeinen Erfahrungen steigt die Ausfallwahrscheinlichkeit nach dieser Reihenfolge:

- Hardware
- Software
- Fehlkonfiguration / Fehlbedienung

Die meisten Ausfälle werden also bei heutigen Netzen durch den Faktor Mensch verursacht. Eine fatale Konfigurationsänderung, ein falsches Kabel, das man zieht, ein nicht kompatibles System, das man anschließt, wer kennt solche Fehlbedienungen nicht. Ausschließen kann man diese nie. Das gilt im gleichen Maße bei klassischen Gefahren- und Meldetechniken. Allerdings ist hier die Komplexität wesentlich geringer und damit reduziert sich die Wahrscheinlichkeit einer Fehlbedienung. Wie schützt man IP-Netze vor solchen Szenarien? Nur eine Kombination von Mechanismen kann helfen. Hierfür kristallisieren sich einige „Goldene Regeln der Hochverfügbarkeit“ heraus.

Als eine Grundregel hat sich bewährt, dass Software grundsätzlich als fehlerhaft einzustufen ist. Der im Markt herrschende Innovationsdruck, den sich die Hersteller aus eigenem Verschulden ausgesetzt haben, hat die Entwicklungs- und Testzyklen für Software auf ein nicht akzeptables Maß verkürzt. Je verbreiteter der Einsatz einer Software ist, desto mehr Fehler werden im Laufe der Zeit entdeckt und behoben. Es entsteht ein Konflikt zwischen dem Interesse an aktuellen Produkten, die in einer möglichst frühen Phase ihres Lebenszyklus zum Einsatz kommen sollen, und der Forderung nach stabilen Produkten. Damit ist eine goldene Regel im Zusammenhang mit Software, nach der Markteinführung von neuen Komponenten nicht gleich zu den ersten Kunden bzw. Anwendern zu gehören. Denn diese werden von den Herstellern bekanntlich als Testkunden missbraucht. Erprobtes Einsetzen hilft natürlich sowohl gegen Software- als auch gegen Hardware-Fehler.

Da anzunehmen ist, dass jede Software fehlerhaft ist und der Nutzungsgrad der Features einer Software höchst unterschiedlich ist, ist die Nutzung von exotischen Features, die nur von wenigen genutzt werden, zu vermeiden. Es sollten nur Features eingesetzt werden, die alle anderen auch einsetzen und vermeide möglichst solche, die nicht von allen genutzt werden. Einfachheit ist hier das Stichwort. Historisch gewachsene IT-Umgebungen neigen mit der Zeit dazu, chaotisch, komplex und unübersichtlich zu werden (Entropiegesetz). Daher gilt es, in der Designphase konsequent auf Vereinfachung zu setzen. Wird diese goldene Regel nicht eingehalten, ist es nicht verwunderlich, wenn eine IT-Umgebung mit der Zeit unübersichtlich und unbeherrschbar wird. Je einfacher und übersichtlicher die IT-Umgebung, desto unwahrscheinlicher werden die aus Fehlbedienung und Fehlkonfiguration resultierenden Probleme.

Neben der beschriebenen Softwareproblematik würde auch die Einführung bzw. Nutzung einer Vielfalt an Übertragungsprotokollen zu einer ernsthaften Bedrohung der Verfügbarkeit führen. Deshalb sollte man sich, falls möglich, ausschließlich auf IP beschränken. Zudem sind Individuelle Konfigurationen möglichst auf zentrale Komponenten zu beschränken und die Masse der Netzkomponenten ist ohne individuelle Konfiguration einzusetzen, komplizierte Mechanismen sollten nur dann implementiert werden, wenn dies zwingend erforderlich ist.

Eine produktive, genutzte IT-Infrastruktur ist vor Auswirkungen des Einsatzes ungeprüfter Verfahren und Konfigurationen zu schützen. Neuheiten sind zunächst in einer Testumgebung zu verifizieren. Natürlich behält das Gesetz seine Gültigkeit, dass die Realität nie hundertprozentig auf eine Laborumgebung abgebildet werden kann und viele Probleme erst in der produktiven Umgebung entdeckt werden. Aber die Erfahrung bestätigt, dass ca. 80 % der Probleme mit neuen Verfahren und Konfigurationen mit Labortests zu vermeiden wären.

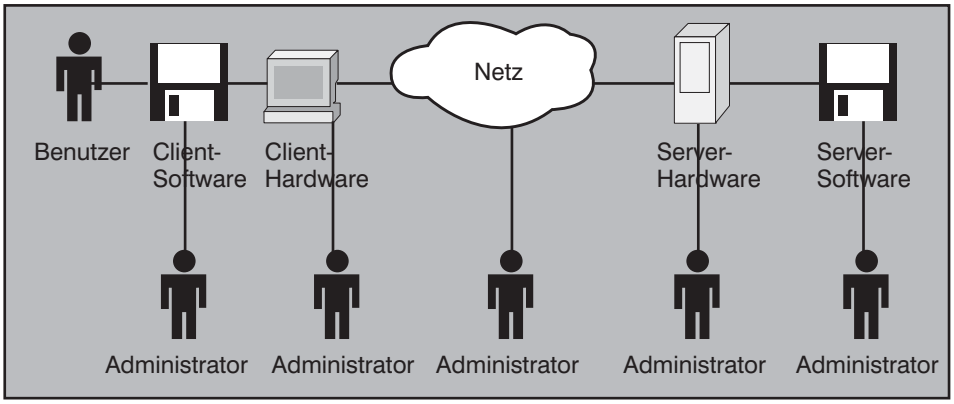


Abbildung 2: Produkt von Einzelverfügbarkeiten

Bei der Betrachtung der Verfügbarkeit wird in der Regel als erstes an Hardware-Verfügbarkeit gedacht. Jedoch redundante Hardware ist nicht alles, im Gegenteil: redundante Hardware ist mit hohen Invest-Kosten verbunden und erhöht damit den Erwartungsdruck hinsichtlich Verfügbarkeit, dabei sind, wie bereits erläutert, die Faktoren Fehlbedienung/Fehlkonfiguration und Software die Hauptverursacher von Ausfällen. Hardware-Redundanz hilft - was nicht minder wichtig ist - vor allem bei geplanten Abschaltungen; beispielsweise werden Wartungsfenster immer knapper und Hardware-Redundanz kann dieses Problem lösen.

Die Sicherheit ist ein weiteres Glied der Kette „Verfügbarkeit“ und wird in den nachfolgenden Absätzen näher betrachtet.

Sicherheit

Die Herstellung von Sicherheit dient auf der einen Seite dazu, dafür zu sorgen, dass nichts passiert, was den Betrieb stören oder Menschen und Material beschädigen könnte (Thema Verfügbarkeit). Für den Fall, dass etwas passiert, muss dann die Alarmauslösung sicher, schnell und fehlerfrei erfolgen. Mit der Alarmmeldung hört der Funktionsumfang der Gefahren- und Meldetechnik nicht auf, durch das System sind weitere alarmabhängige Steuerungen und Reaktionen einzuleiten (beispielsweise das Schließen von Brandschutzklappen im Falle eines Feuers). In einem der kritischeren Vorträge auf dem Forum wurde die Frage gestellt, ob bei der netzwerkbasierenden Technik diese Sicherheit möglicherweise auf der Strecke bleibt. Ein paar Beispiele für die dort geäußerte Kritik sollen nachfolgend aufgeführt werden. Dabei ist erkennbar, dass der Begriff „Sicherheit“ weniger mit dem IT-Begriff „Security“, sondern eher mit der bereits beschriebenen Verfügbarkeitsproblematik assoziiert wurde.

Der Datenverkehr in einem IT-Netz lässt sich wesentlich leichter durch Unberechtigte aufzeichnen als in den proprietären Netzen. Diese Kritik ist ohne Zweifel grundsätzlich berechtigt. Allerdings lassen sich Maßnahmen ergreifen, um das Aufzeichnen zu erschweren, Techniken wie VLANs, Layer-2/3-Switches, Firewalls sind zu nennen. Ganz verhindern wird man dies aber kaum. Demzufolge muss neben diesen Maßnahmen dafür gesorgt werden, dass sicherheitskritische Informationen verschlüsselt übertragen werden. All diese Maßnahmen sind aber in heutigen Netzen keine Hexerei mehr und können implementiert werden.

Wer stellt bei gemeinsam genutzten Infrastrukturelementen (aktive und passive Komponenten) sicher, dass z.B. eine Umrangierung oder Port-Deaktivierung nicht unbemerkt die Deaktivierung einer Überwachungseinheit zur Folge hat? Diese Gefahr ist in einem konvergenten Netz technikbedingt höher. Die Risiken lassen sich hier aber mit Polling-Mechanismen, wie sie z.B. auch im Bereich der SNMP-Überwachung „normaler“ Netzwerk-Komponenten genutzt werden, reduzieren wenn nicht sogar ausschließen. Was aber geschieht in folgenden, aus der Praxis bekannten Szenarien:

- Der DNS-Dienst wird verändert, die Namensauflösung funktioniert nicht mehr.
- Die Einstellungen der Firewall wurden verändert, können die mit der Gebäu-

deüberwachung verbundenen Dienste noch übertragen werden?

- Die Treiber der Grafikkarten werden einem Update unterzogen, danach ist insbesondere bei der Videoüberwachung eine Verwertbarkeit der Anzeigen nicht mehr gewährleistet.

Eine Reduzierung dieser Risiken ist nur mit einem geregelten und organisierten Change-Management möglich, dies ist zwingende Voraussetzung zur Einführung der neuen Techniken.

Eine weitere Bedrohung wurde im Vortrag anhand der Virenproblematik beschrieben. Doch wie wahrscheinlich ist die Nutzung von konventioneller Sicherheitstechnik ohne Einsatz von File- oder Applikations-Servern mit üblichen Betriebssystemen? Auch hier würden Viren bei entsprechenden Systemen zu einem Totalausfall führen können. Das Problem muss also in jedem Falle gelöst werden, nicht nur in einem IP-basierenden Gefahren- und Sicherheitsnetz.

Ein Datennetz nach heutigem Stand der Technik kann möglicherweise keine ausreichenden Signallaufzeiten garantieren, damit verschlechtert sich die Echtzeitfähigkeit. Dies ist ein ernstzunehmender Aspekt und es wird im Rahmen der Ablösung von konventionellen Sicherheitstechniken zu analysieren sein, welche konkrete Echtzeitfähigkeit gefordert wird. Es sei auf den Vergleich zu einer identischen Anforderung bei der Einführung von Industrial Ethernet hingewiesen: Auch hier hieß es zunächst, dass die Eigenschaften des Ethernets eine Verwendung des Verfahrens im Produktionsbereich nicht möglich machen, erst nach und nach wurden verschiedene Klassen von Echtzeitanforderungen definiert und dabei festgestellt, dass so genannte „weiche“ Echtzeitanforderungen den Einsatz durchaus zulassen.

Der abschließende Hinweis der Kritik auf die besondere Beachtung der psychologischen Komponente zum Thema Sicherheit ist in jedem Falle ernst zu nehmen. Sicherheit ist letztendlich ein Akzeptanz- und Kommunikationsproblem und kann nur durch kompetenten und ehrlichen Dialog erreicht werden. „Maßnahmen ohne Akzeptanz laufen ins Leere“ so die Kernaussage.

Bei einer Betrachtung der Elementarmaßnahmen, die zur Erhöhung der Sicherheit (diesmal in Sinne von „security“, nicht von Verfügbarkeit) sinnvoll sind, können nachfolgende Regeln herangezogen werden. Ein potenzieller Angreifer könnte über das IP-Netz das Gefahrenmanagement außer Funktion setzen. Kommunikation zum Gefahrenmanagement muss aber nicht in dem selben IP-Netz übertragen werden, welches für Videoüberwachung und Brandmeldesysteme einerseits und E-Mail sowie Internet-Zugriff andererseits verwendet wird, IP-Netze können segmentiert werden. Es gilt der Grundsatz „die beste Verteidigung gegen potenzielle Angreifer ist es nicht da zu sein“. Durch „Nichtsichtbarkeit“ eines separierten Netzes werden die Möglichkeiten zum Angriff erheblich reduziert und es bietet sich an, ein IP-Netz z.B. ausschließlich für das Gefahrenmanagement zu nutzen und die verschiedenen Anwendungen im Rahmen des Gefahrenmanagements zu integrieren, ohne dass es eine Kopplung zu anderen IP-Netzen gibt. Das ist der sicherste Schutz auch gegen solche Szenarien wie Virenausbreitung. Diese Sicherheit kann jedoch zu anderen Anforderungen wie „Offenheit“ in Konflikt geraten: will man jedem Mitarbeiter ermöglichen, dass er von seinem Arbeitsplatz aus die Türöffnung bedienen kann, braucht man zwischen dem Gebäudemanagementsystem und dem Bürokommunikationsnetz eine wie auch immer geartete Kopplung. Je sicherer diese Kopplung ist und je mehr Funktionalität sie anbieten muss, umso größer ist in der Regel der Aufwand für deren Gestaltung. Weitere Motivationspunkte für die Netztrennung sind:

- Die Umgebungen für Büro und Gefahrenmanagement können mit verschiedenen Sicherheitsrichtlinien und –interessen definiert und aufgebaut werden.

- Es können unterschiedliche Netzstrukturen und Netzverfahren eingesetzt werden.

- Im Bereich Gefahrenmanagement existieren oft Systeme, die nicht den Unternehmensrichtlinien für Sicherheits-Patches und Updates unterliegen, sondern als „Black Box“ geliefert werden und eingesetzt werden müssen.

- Eine Separierung der teilweise nicht nur zu den Bereichen Büro und Gefahrenmanagement gehörenden Informationsströme, sondern auch der Zuständigkeiten für den Betrieb der beiden Netzbereiche ist möglich.

Es sind bei der Netzwerktrennung drei Grundmodelle zu unterscheiden:

- Trennung der gesamten Infrastruktur (passiv/aktiv)

- Trennung aller aktiven Bestandteile

- Logische Trennung der Netze (also gemeinsam Nutzung aller aktiven/passiven Bestandteile)

Eine Trennung der gesamten Infrastruktur widerspricht der Idee des konvergenten Netzes. Sie würde zwar wirtschaftliche Einsparungen mit sich bringen, nicht aber in dem Maße, wie man sich das erhofft. Damit liegt es nahe, mindestens die Verkabelung gemeinsam zu nutzen. Ob es eine vollständig gemeinsam genutzte Verkabelung geben wird ist eher zweifelhaft, zu verschieden sind die technischen Anforderungen bei der Kommunikation mit Wärmemeldern, Rolladensteuerungen oder ähnlichem (dazu später mehr). Eine gemeinsame Nutzung der Backbone-Verkabelung dagegen ist sehr wahrscheinlich. Ähnlich ist die Trennung der aktiven Bestandteile zu betrachten. Getrennte

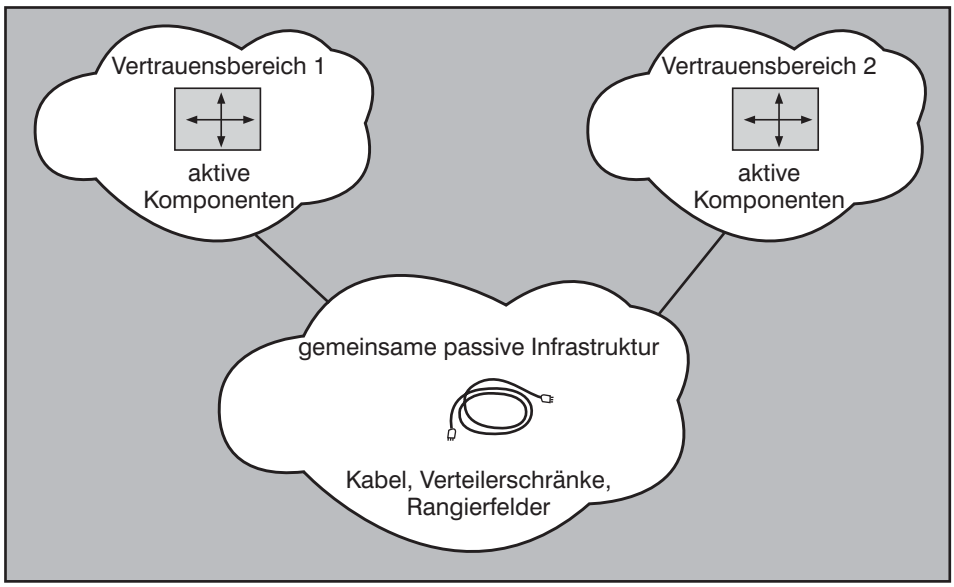


Abbildung 3: Grundmodell zur Netztrennung

Backbone-Komponenten (Core- und Distribution-Bereich) werden aufgrund von wirtschaftlichen Erwägungen keinen Sinn machen, eine Separierung des Access-Bereiches dagegen schon. Je nach Sicherheitsrichtlinien der beiden Bereiche und anderen relevanten Randbedingungen wie Verantwortung für den Betrieb kann die Nutzung getrennter Distribution- und Core-Switches durch die beiden Bereiche jedoch notwendig sein. Den Ansatz unterschiedlicher Access Komponenten verfolgt man - aus anderen Gründen allerdings - heute zum Teil bereits beim Design von Wireless-Infrastrukturen, Access Points werden über eigene Access Switches (oder gar Wireless LAN Controller) angebunden. Ein Problem bei dieser restriktiven Trennung besteht jedoch darin, dass bei geringer Anzahl von Anschlüssen für ein Gefahren- und Meldesystem im jeweiligen Verteilungspunkt eigene aktive Komponenten zu teuer wären (soll man für ein halbes Dutzend Anschlüsse eigene Access Switches vorsehen?). Dem Ruf nach einer möglichst wirtschaftlichen Lösung folgt dann häufig die Empfehlung zu einer VLAN-basierenden Netztrennung: Man nehme einen Access Switch und richte auf diesem die entsprechenden Netze als getrennte VLANs ein. Im Falle einer solchen Lösung ist jedoch auf folgende Nachteile hinzuweisen:

- Broadcast-Stürme können sich auf die Verfügbarkeit der gemeinsamen Layer-2-Infrastruktur negativ auswirken.
- Die Flutung von Unicasts durch die Fehlkonfiguration von Servern oder ähnliche Ursachen kann ein Problem darstellen.
- Viren und Würmer, die sich in einem Büro-VLAN ausbreiten, legen unter Umständen auch die vom Gefahrenmanagement-VLAN genutzten aktiven Netzkomponenten lahm.
- Nachteile bei einer gelände-weiten Spanning-Tree-Struktur in Punkto Stabilität und Skalierbarkeit sind einzukalkulieren.
- Eine manuelle Einrichtung von Änderungen an VLAN-Zuordnungen wird sehr aufwändig und fehleranfällig.
- Wartungsarbeiten mit den Verantwortlichen für die Büro- und die Gefahrenmanagementumgebung müssen sehr gut koordiniert werden.

Deshalb wird empfohlen, nach Möglichkeit separate Access-Switches (Layer-2-Switches) für den Büro- und den Gefahrenmanagementbereich einzusetzen. Die daraus ermöglichte Zuordnung von Büro und Gefahrenmanagement zu verschiedenen Broadcast-Domänen bringt automatisch folgende Vorteile:

- Die Broadcast-Stürme, die sich im Bürobereich ausbreiten, wirken sich in der Regel nicht mehr auf den Gefahrenmanagementbereich aus.
- Doppelte Adressen im Bürobereich, verursacht zum Beispiel durch Fehlkonfiguration, betreffen nur den Bürobereich und nicht den Gefahrenmanagementbereich.
- Die Flutung von Paketen, verursacht zum Beispiel durch den Überlauf der Adresstabellen von Switches, bleibt auf eine Broadcast-Domäne beschränkt.
- Defekte Netzadapter, die zum Beispiel eine Vielzahl von Paketen ins Netz versenden, beeinträchtigen in der Regel nur die eigene Broadcast-Domäne.
- Die meisten durch Änderungen verursachten undefinierten Netzzustände und Spanning-Tree-Probleme wirken sich nur auf eine Broadcast-Domäne aus.
- Bei Betrieb des Netzes ist es hilfreich, Subnetze und somit IP-Adressen eindeutig einem der beiden Bereiche Büro oder Gefahrenmanagement zuordnen zu können. Dies kann nur mit Hilfe von separaten Subnetzen bzw. Broadcast-Domänen für Büro und Gefahrenmanagement erreicht werden.
- An den Subnetzgrenzen können so genannte Access Control Lists (ACL) dafür sorgen, dass bestimmte Kommunikationsbeziehungen zwischen dem Büro- und dem Gefahrenmanagementbereich unterbunden oder nur namentlich eingestellte Kommunikationsbeziehungen zwischen den beiden Bereichen erlaubt werden. Dies ist bei gemeinsamer Nutzung von Subnetzen nicht möglich.

Eine Kopplung der getrennten Netze ist im Sinne des Strebens nach Konvergenz unvermeidbar, wie sonst sollte z.B. eine effiziente Überwachung der Elemente im Sicherheitsnetz von einem herkömmlichen autorisierten Arbeitsplatz aus möglich gemacht werden, wie sonst kann ein Zugriff von Endgeräten der Gefahrenmanagementumgebung auf Ressourcen in der Büroumgebung, wie z. B. Namensdienste, Proxies etc. stattfinden. Auf der Netzwerkebene bietet sich der Einsatz von Layer-3-Switches an, dieser Lösungsansatz wird bereits häufig beim Design von Industrienetzen angewendet, hier geht es auch darum, klare Trennungen unter Beibehal-

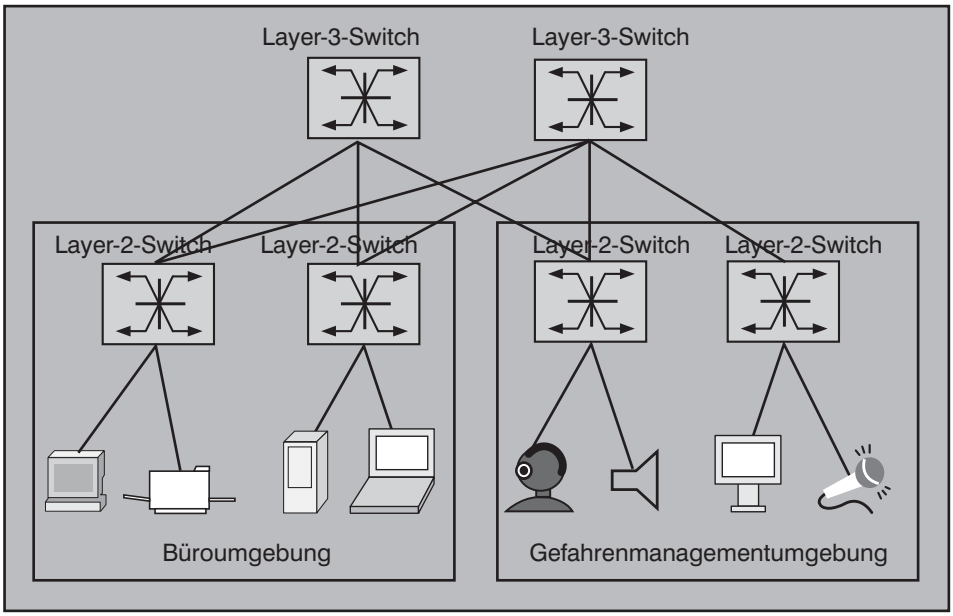


Abbildung 4: Layer-3-Kopplung

tung der Möglichkeit des übergreifenden Zugriffs sicherzustellen.

Über die Anwendung von Access Control Listen z.B. in den Distribution Switches kann zentral und individuell gesteuert werden, wer auf welches Netz Zugriff haben darf und wer nicht. Eine derartige Definition wird z.B. vereinfacht, wenn der Adressraum des Unternehmens mindestens in einen Büro- und einen Gefahrenmanagementbereich unterteilt wird, noch besser wäre es, wenn die Unterteilung der IP-Subnetze in Adressbereiche für bestimmte Endgerätetypen realisierbar wäre. Für jedes umgestellte Gefahrenmanagementsubnetz kann dann eine entsprechende Access Control Liste auf den Interfaces der entsprechenden Distribution Switches eingestellt werden. Vielfältige Filtermöglichkeiten sind denkbar, Beschränkung der subnetzübergreifenden Kommunikation der zu schützenden Endgeräte (IP-Adressen) auf namentlich zu nennende TCP- bzw. UDP-Ports wäre nur eine davon.

Eine zweite Möglichkeit der Abschottung einzelner Access-Bereiche zu den Bereichen des Gefahrenmanagements erfolgt mittels Firewalls. Der wesentliche Unterschied zwischen den beiden Lösungen besteht darin, dass anstelle der Definition von Access Control Listen Firewallregeln auf den Firewalls für die abgetrennten Access-Bereiche definiert werden müssen.

Bleibt noch die Beschreibung einer dritten Möglichkeit, dem Einsatz von Application Level Gateways (ALG) zur Trennung von „Gefahrenmanagementinseln“ vom restlichen Netz. ALG selbst sind weder Layer-2- noch Layer-3-Koppelelemente, sie selbst werden von den Kommunikationspartnern adressiert und müssen auf Anwendungsebene auf beiden Seiten (intern wie extern) eine Kommunikationsbeziehung aufbauen, um zwischen zwei Kommunikationspartnern vermitteln zu können. Zum Beispiel kann es sinnvoll sein, eine Gefahrenmanagementanlage mittels ALG vom restlichen Netz zu trennen und extern nur den Zugriff auf einen in der Anlage implementierten Server zu ermöglichen, der die Gefahrenmanagementdaten aufbereitet. Der ALG vermittelt zwischen diesem Server und dessen externen Kommunikationspartnern. Umgekehrt kann aus der Gefahrenmanagementanlage selbst ein Endgerät als Client über den ALG eine Kommunikation mit einem externen Kommunikationspartner aufbauen und Gefahrenmanagementdaten austauschen. In jedem Fall bleibt die externe Kommunikation auf den vom ALG vermittelten Datenaustausch beschränkt.

Bei der Kopplung zwischen der Büro- und der Gefahrenmanagementumgebung sind also mehrere Verfahren denkbar, und wenn die die Sicherheitsrichtlinien des Unternehmens es erlauben, können Büro- und Gefahrenmanagementumgebungen auch über eine reine Layer-3-Kopplung miteinander verbunden werden.

Lassen Sie uns im nachfolgenden Teil ein Schwenk machen zu den scheinbar einfachsten Elementen einer IT-Infrastruktur, den passiven Elementen.

Verkabelung

Der Traum einer jeden Verkabelungsplanung ist die Bereitstellung einer Infrastruktur, die an jedem Punkt jede IT-Technik möglich macht. Sowohl die Verkabelungsnormen der EN 51073 (und weitere) wie auch die Berücksichtigung dieser Normen durch die IEEE haben mitgeholfen, dieses Ziel für den Arbeitsplatz zu erreichen. Doch in Zusammenhang mit der Gefahren- und Meldetechnik reicht das nicht, es muss eine „anwendungsneutrale“ Infrastruktur auch für „Nicht-Arbeitsplätze“ bereitgestellt werden und da beginnt das Problem. Zwei Varianten zur Sicherstellung einer neutralen Verkabelung für die Gefahren- und Meldetechnik sind denkbar:

1. Diese anwendungsneutrale Verkabelung wird ausschließlich für eine IP-, sprich ethernet-basierende Gefahren- und Melde-Technik verwendet.

2. Diese anwendungsneutrale Verkabelung wird auch für Nicht-IP-, sprich ethernet-basierende Gefahren- und Melde-Techniken verwendet.

Im ersten Fall resultiert daraus die Konsequenz, dass eine „ganz normale“ EN50173-1-Verkabelung vorzusehen ist (oder eine Verkabelung nach prEN50173-3 für besonders rauhe Umgebungen), so wie sie bereits heute millionenfach geplant wird. Besonders zu berücksichtigen wäre - sofern dies nicht bereits heute gemacht wird - dann Power over Ethernet. Schwieriger gestaltet sich die Frage nach den zentralen „Auflaufpunkten“ der Tertiärverkabelung. Ein anwendungsneutrales Verkabelungssystem gemäß EN-50173 macht im Prinzip nur Sinn, wenn die Kabel im oder in den neutralen Etagenverteiler zusammenlaufen und man erst bei Bedarf entscheidet, welcher Dienst über das Kabel übertragen werden soll. Bei der besonderen Sicherheitsproblematik der in diesem Artikel angesprochenen Nutzung spricht aber dagegen, dass die Sicherheitsdienste im gleichen Technikraum wie ganz normale Büroarbeitsplätze aufgeschaltet würden. Um zu verhindern, dass versehentliche Störungen oder Abschaltungen von „überwachenden“ Anschlüssen erfolgen (Beispiel: Eine Überwachungskamera wird versehentlich auf einen Access-Switch für „normale“ PCs umrangiert, es erfolgt ein VLAN-Wechsel und die Überwachung würde deaktiviert) sind folgende Maßnahmen sinnvoll:

- Der Abschluss der Tertiärkabel für die Gefahren- und Meldetechnik erfolgt auf eigenständigen Rangierfeldern; dies ist jedoch wiederum nicht ganz im Sin-

ne der anwendungsneutralen Verkabelung.

- Die sicherheitskritischen Applikationen sind durch spezielle Anschlussschnüre - z.B. unter Nutzung von speziellen Farben - zu kennzeichnen, dies reduziert die Gefahr von Fehlrangierungen durch Unkonzentriertheit.

- Im Extremfall ist der Aufbau der Ethernet-Infrastruktur für Sicherheitstechnik in eigenen, geschlossenen Schränken durchzuführen.

Eine bewusste Sabotage oder ein Unterlaufen der Sicherheitsfunktionen wäre allerdings kaum zu verhindern.

Für den zweiten Fall (Verkabelung wird auch von Nicht-ethernet-basierenden Techniken genutzt) besteht die Schwierigkeit darin, die nachrichtentechnischen Anforderungen an das Verkabelungssystem zu kennen, die von der eingesetzten Signalisierungstechnik gestellt werden. Zusätzlich steht man wieder vor dem Problem der Netztrennung, wie kann das sinnvoll und praktikabel durchgeführt werden ohne eine Rückkehr zu eigenen, speziellen Verkabelungen mit eigenen Technikräumen heraufzubeschwören.

In allen Fällen stellt sich eine neue, bisher bei der Planung von Office-Verkabelungen so nicht aufgetretene Frage: Wo sind die Anschlüsse vorzusehen, um sowohl die aktuell geplanten Gefahren- und Meldetechnikelemente anzuschließen als auch eventuelle Ergänzungen/Änderungen in Zukunft ohne Nachverkabelung möglich zu machen? Was geschieht z.B., wenn man sich 5 Jahre nach dem Einzug in ein neues Gebäude dazu entschließt, die Rollladensteuerung zentral mit Ethernet-Technik zu regeln? Müssen dann in allen Büros Kategorie-5-Kabel nachgezogen werden, sollte man diese bereits bei der Rohplanung vor dem Bezug des Gebäudes vorsehen? Welcher Planer fragt heute bei einer Neuverkabelung eines normalen Bürogebäudes nach, ob es auf den Etagen, in Fluren, Treppenhäuser, in Garagen oder gar im Außenbereich Anschlüsse geben muss?

Insbesondere im Zusammenhang mit der Festlegung von Anschlüssen, die erst in Zukunft gebraucht werden und deren Position heute vollkommen unbekannt ist, wird nachfolgend kurz ein in hiesigen Landen relativ unbekanntes Verkabelungselement vorgestellt, der Sammelpunkt (consolidation point). Die Idee ist eigentlich nichts Neues, sie kommt aus der Welt der klassischen Telefonverkabelung: Ein Bündel von hochwertigen Installationskabeln wird bis zu einem Punkt verlegt und dort auf Rangierfelder aufgelegt, dies stellt die „feste Verkabelung“ dar. Von hier aus werden bei Bedarf neue Kabel zum Arbeitsplatz bzw. zur Dose verlegt (bedarfsorientierte und damit dynamische Verkabelung“). Die Vorteile bestehen in einer Vereinfachung der Nach- oder Änderungsverkabelung. Bei „normalen“ IT-Verkabelungen gemäß den so genannten 2-Connector-Modellen (eine Verbindung im Rangierfeld und eine in der Dose) muss bei einer Nachverkabelung der gesamte Kabelweg zwischen Dose und Etagenverteiler geöffnet bzw. wieder geschlossen werden. Dies führt zu erheblichen Kosten bei der Sanierung der Kabelinfrastruktur. Im Falle eines Sammelpunktes reduziert sich das Öffnen/Schließen der Kabelwege auf einen in der Regel kurzen Bereich von ca. 20 bis 30 Metern, dies kann wesentlich einfacher und kostengünstiger gemacht werden. Würde man also z.B. in der Planungsphase ausreichende Sammelpunkte vorsehen und diese nicht zu 100% beschalten, so könnte man - man nehme das Beispiel der oben genannten Rollladensteuerung - auch Jahre später zusätzliche Anschlüsse realisieren; im übrigen ist diese Technik auch interessant bei der Planung von Anschlüssen von WLAN-Access Points.

Bisher haben wir also festgestellt, dass es schwierig ist, in einem modernen Gebäude, bei dem irgendwann einmal die Gefahren- und Meldetechnik zu großen Teilen auch über IP oder auch nur über eine anwendungsneutrale Verkabelung betrieben werden soll, die Anschlusszahlen vorherzusehen oder gar festzulegen. Nehmen wir einmal an, diese Anschlüsse wären klar, wie sähe dann das Netz aus? Wieder sind zwei Varianten denkbar:

Das Endgerät der Gefahren- und Meldetechnik, z.B. eine Videokamera oder auch ein einfacher Melder, benötigt ein Kabel bzw. eine Schnittstelle der universellen Verkabelung. Das andere Ende der Kabelstrecke, ob mit oder ohne Sammelpunkt, befindet sich in einem klassischen IT-Etagenverteiler. Die Variante 2 ist identisch zur vorherigen Lösung mit dem Unterschied, dass das Ende der Kabelstrecke nicht in einem IT-Verteiler ist, sondern in einem irgendwie gearteten kleineren Unterverteiler mit aktiven Komponenten. Dies können Ethernet-Switches sein oder auch „proprietäre“ Koppelelemente, der letztere Fall entspricht dann aber nicht mehr einem konvergenten Netz, deshalb wird dieser Fall hier nicht weiter verfolgt. Vergleicht man beide Varianten (Anbindung der Endgeräte am Etagenverteiler oder am Unterverteiler), so fällt die Vorstellung schwer, dass alle Anschlüsse der IP-basierenden Gefahren- und Meldetechnik in den Etagenverteilern enden. Man stelle sich die gewaltige Kabelmenge vor. Deshalb erscheint es aus der Sicht des Autors

nahe liegend, dass aktive Unterverteiler vorgesehen werden, die für ganz bestimmte, logisch oder physikalisch zusammengehörende Bereiche vorgesehen werden. Dieser Unterverteiler wird über ein beliebiges Medium mit dem Etagenverteiler verbunden. Neben der Einsparung der gewaltigen Kabelmengen hätte dies noch einen weiteren Vorteil, der bedeutend für die zukünftige Strategie bei der Implementierung von Gefahren- und Meldetechnik auf IP sein könnte: Die Abwicklung von Überwachungs- und Regelprozessen ist vielfach räumlich begrenzt bzw. ein Großteil dieser Prozesse spielt sich auf der Ebene des einzelnen Raumes ab. Steuer- und Regelungsaufgaben müssen deshalb nicht zentral gelöst werden. Beispiele dafür sind Heizung, Klima, Lüftung oder Beleuchtung. Ein Datenverkehr, der Regel- und Steuerungsprozesse zwischen diesen abgegrenzten Einheiten unterstützen muss, ist kaum zu erwarten.

Die dezentrale Lösung hätte folgende Vorteile:

- Das Delay oder auch der Jitter würden bei einer primär lokal begrenzten Kommunikation besser sein.
- Autark arbeitende Einheiten erhöhen deutlich die Verfügbarkeit. Man stelle sich einen Etagenverteilerausfall vor, von dem auch sämtliche Beleuchtungs- oder Rollladensteuerungen betroffen wären.
- Erweiterungen in Form von zusätzlichen Endgeräten/Meldern/Steuerungselementen lassen sich sowohl auf der passiven wie auch auf der aktiven Ebene schneller durchführen.
- Eine Ablösung von vorhandenen proprietären Signal-, Melde- und Steuerungstechniken könnte wesentlich sanfter erfolgen.

Die dahinter steckende Grundidee ist nichts Neues. Schaut man sich z.B. den Bereich der modernen Industriekommunikationsnetze - insbesondere der Vernetzung von Maschinen - an, so können viele Parallelen festgestellt werden:

- Es wurde ein neuer Verteilertyp definiert, der für einen in der Regel räumlich sehr begrenzten Bereich zuständig ist, der Maschinenverteiler.
- Spezielle passive Komponenten wurde entwickelt und standardisiert wie z.B. rüttelfeste Stecker, flexiblere Kabel (Kabel mit Polyurethan-Aufbau) oder Kabel geeignet für die direkte Steckermontage.

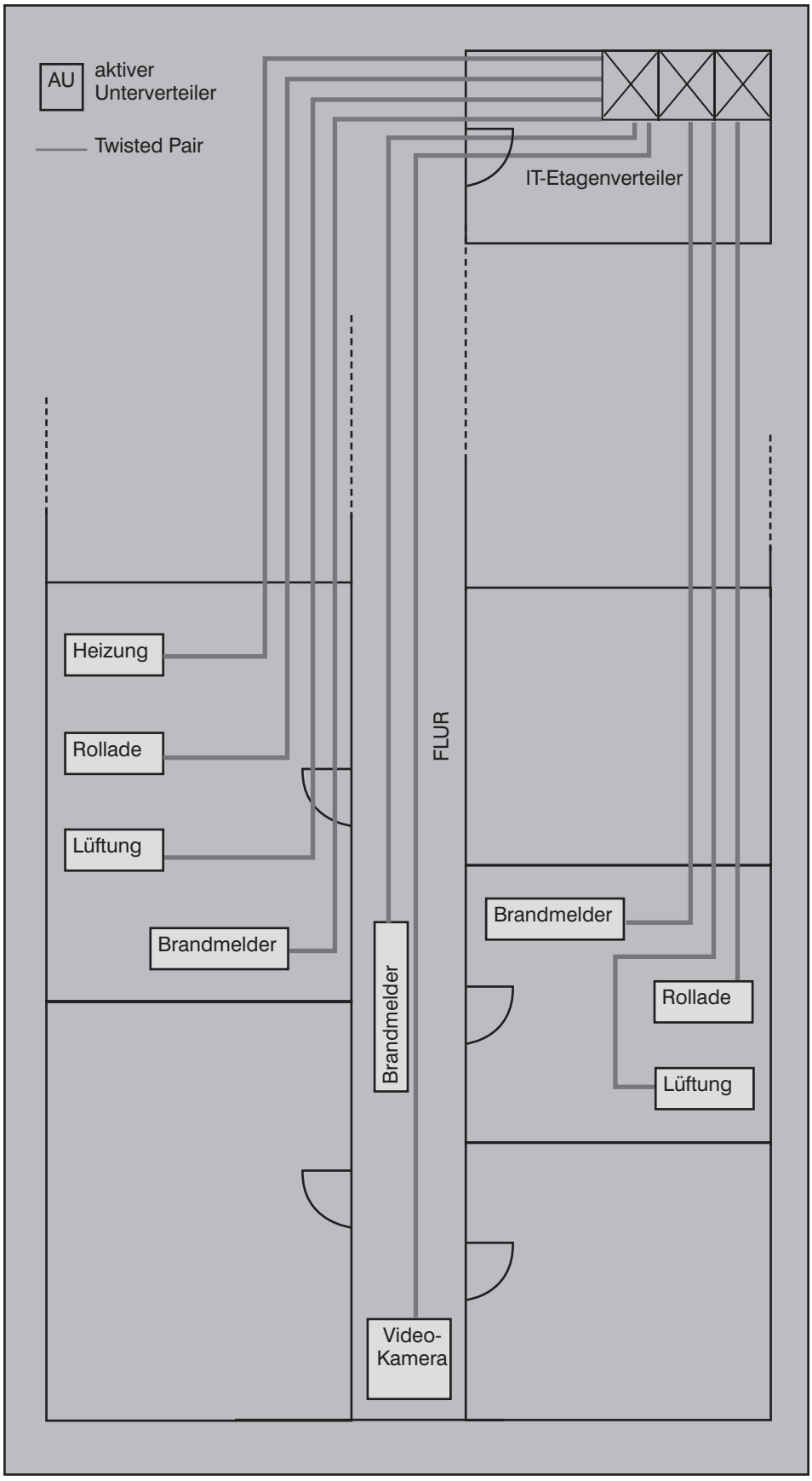


Abbildung 5: Zentrale Lösung für die Gefahren- und Meldetechnik

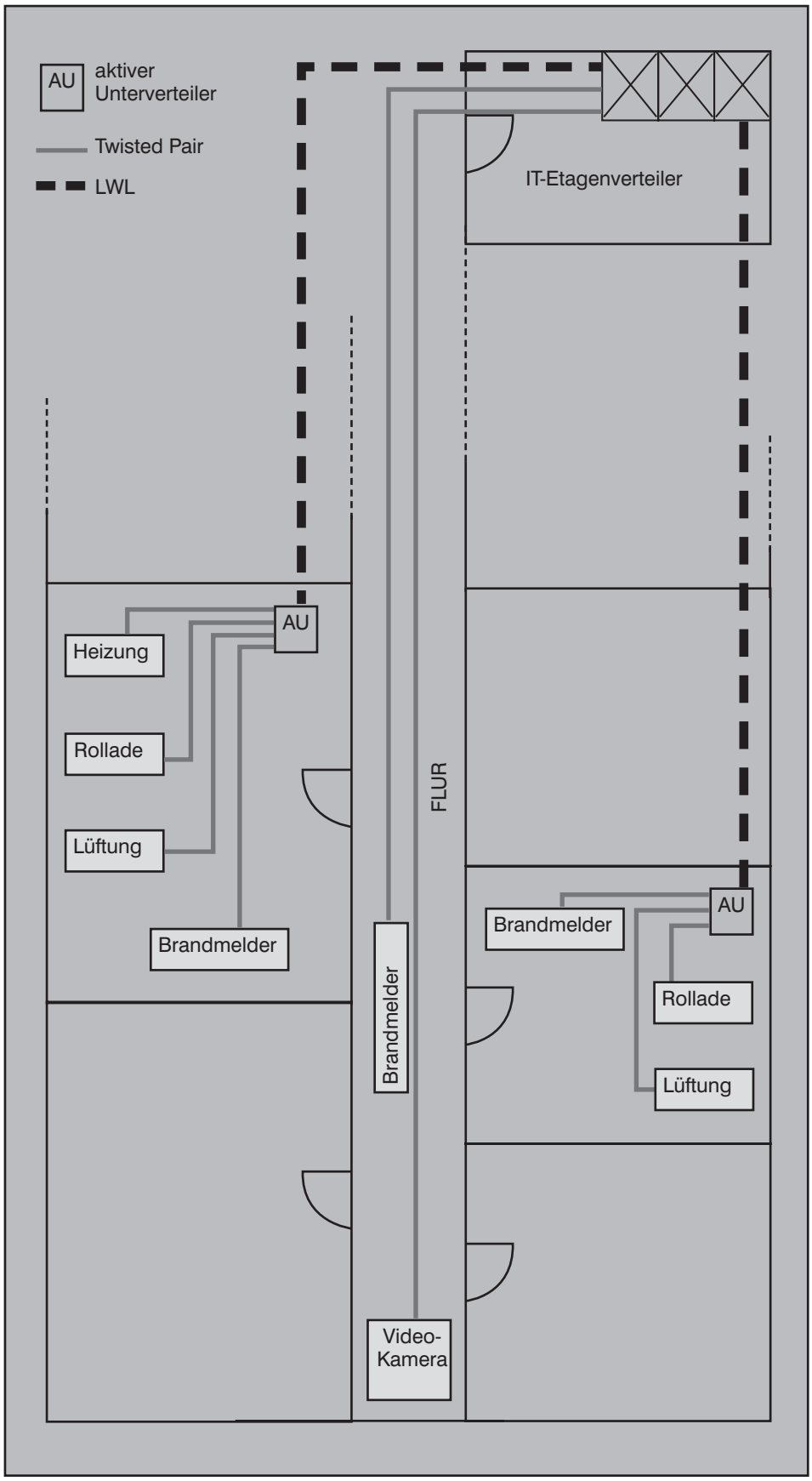


Abbildung 6: Dezentrale Lösung für die Gefahren- und Meldetechnik

- Es werden auf dem Markt zunehmend mehr aktive Komponenten angeboten, die darauf optimiert wurden, in kleinen, nicht 19“-normierten Verteilern eingesetzt zu werden. Diese nutzen z.B. Hutschienentechniken zur Befestigung, arbeiten lüfterlos oder werden mit Gleichstrom versorgt. Wären diese nicht auch prinzipiell gut geeignet für den Aufbau von aktiven Raumverteilern?

Die Zukunft wird zeigen, ob dieser vorgestellte dezentrale Ansatz der beschrittene Weg sein wird. Zum Abschluss soll als praktisches Beispiel ein Kernthema des Kongresses betrachtet werden, die Videoüberwachung.

Videoüberwachung

Die Videoüberwachung bildete aus folgendem Grunde eines der wichtigen Themen des Kongresses: Sie stellt die Überwachungstechnik dar, die heute am weitesten die Migration zur IP-basierenden Überwachungstechnik vollzogen hat. Das Kongressauditorium war beeindruckt von den technischen Möglichkeiten des „Video over IP“ und insbesondere von den Vorteilen, die sich durch den Einsatz solcher Techniken ergeben. Die aktuelle Videoüberwachungstechnik unterscheidet zwischen 3 verschiedenen Lösungsansätzen:

- Analoge Technik ohne Einsatz von IP-basierender Kommunikation
- Analoge Technik unter Einsatz von IP-basierender Kommunikation
- Digitale Technik unter Einsatz von IP-basierender Kommunikation

Die erste Variante setzt ausschließlich auf koaxialkabelbasierende Techniken, dieses vollkommen separate Koaxnetzwerk wird strikt getrennt von IP-basierenden Techniken. Bei der zweiten Variante erfolgt zwar die Kameraanbindung weiterhin koaxbasierend, die Videosignale werden aber in Videoservern gesammelt, welche auf IP-Basis miteinander oder mit zentralen Überwachungseinheiten vernetzt sind. Die dritte Variante sieht weder bei der Signalübertragung noch beim Management der Kameras analoge Techniken vor, es wird ausschließlich eine IP-basierende Infrastruktur genutzt.

Die Vorteile der Variante 1 liegen in der ausgereiften Technik, der breiten Einsatzerfahrung und damit verbunden der großen Palette an kompetenten Installateuren. Neben speziell im Indoor-Bereich sehr kostengünstigen Kameras gibt es eine große Auswahl an Videorekordern und die analoge Technik bedient sich

	.11b	.11g	.11a	.11e	WMM	WEP	WPA Enterprise	WPA-PSK	WPA2 Enterprise	WPA2-PSK
AXIS 206W	x					x		x		
AXIS 207W	x	x				x		x		x
D-Link DCS-5300G	x	x				x				
Provitek IP-Videoserver LAN / WLAN	x	x				x				
Provitek IPCam Netzwerkkamera LAN /WLAN	x	x				x				
SANTEC SDVR-8/XWL	x					x				
SANTEC VTC-215W	x					x				
SANTEC VTC-722WL	x					x				
Siemens Gigaset WLAN Camera	x					x		x		
Sony SNC-M1/2/3/W	x					x				
StarChip Videoüberwachung CAS-200W Internet IP LAN Camera	x					x				

Tabelle 1: Übersicht WLAN-Videokameras

beim Ausgabemedium ganz einfacher Monitor- und Fernsehgeräte. Der in den Vorträgen genannte Hauptnachteil entsteht durch das Koaxialkabelmedium, es erschwert die Kontrolle bzw. Steuerung der Kameras, die Bildgröße wird aus nachrichtentechnischen Gründen begrenzt und die Bildqualität ist oftmals nicht gleich bleibend. Wie man sich leicht vorstellen kann, ist das Koaxkabel im praktischen Betrieb bei Neuanschlüssen oder Änderungen von Kamerapositionen (Stichpunkt: mobiler Kameraeinsatz) z.B. im Vergleich zu einem Twisted Pair-Kabel kein leicht zu handhabendes Medium. Es erfordert spezielles Werkzeug und Messgeräte.

Die Variante 2 übernimmt die koaxialkabeltypischen Vor- und Nachteile der Variante 1. Vereinfacht wird dagegen die Fernadministration über das IP-Netzwerk, der standortübergreifende Bildzugriff, eine Verknüpfung von Kameras über Videoserver und die Skalierbarkeit von Systemen. Neue Nachteile entstehen durch den im Artikel thematisierten Zwang zur Trennung der IP-Netze, einer hohen Netzwerklast, hohen Lizenz- und Software-Installationskosten und Engpässen bei der Dimensionierung der Betriebssysteme.

Bei rein IP-basierenden Lösungen verschwinden die Nachteile, aber auch die Vorteile des Koaxialkabelnetzes (eigenständiges und damit „sicheres“ Netz). Die Videokameras sind eigenständige Einheiten, die zunächst die aufgezeichneten Informationen auf dem Gerät festhalten, eine spürbare Erhöhung der Netzlast ist nicht gegeben. Erst bei einem gezielten Abruf der Videoaufzeichnungen wird das Netzwerk genutzt und dann wird die Bildqualität durch die Bandbreite begrenzt. Hier muss gegebenenfalls eine eigenständige Netzwerkinfrastruktur vorgesehen werden. Dieses Prinzip birgt mehrere Vorteile. Bei Ausfall einer Netzwerkverbindung zur Kamera geht - zumindest über einer begrenzten Zeitraum - keine Bildinformation verloren, dies bedeutet eine Steigerung der Verfügbarkeit. Ein Single-point-of-Failure lässt sich durch Aufbau von hochredundanten Netzen sehr einfach vermeiden, selbst bei Ausfall eines zentralen Video- oder Management-Servers kann man über geeignete Standard-Protokolle (Browser, MxPEG-Viewer) weiterhin auf die Kameras zugreifen.

Eine Erweiterung des Videonetzes ist wesentlich einfacher, es muss kein Koaxialkabel nachgezogen, konfektioniert oder eingemessen werden und es muss auch kein gezielter Anschluss an zentrale Sammelkomponenten wie z.B. einem Videoserver erfolgen. Stattdessen kann die Kamera wie jedes andere IP-Gerät ans Netz angeschlossen werden und erst bei gezieltem Bedarf wird über das Netzwerk die Kamera gesteuert oder die Videoaufzeichnung abgerufen.

Diese primären durch das Netzwerk entstehenden Vorteile sind nach Aussagen der Kamerahersteller zu ergänzen durch bessere Bildqualität, einfachere Möglichkeit zur Bildbearbeitung, Vereinfachung der digitalen Signatur und einfachere Verknüpfung mit Alarm- und Schaltsystemen. Dieser Mehrwert der IP-basierenden Videoüberwachung wird langfristig begleitet durch eine Kostenreduktion, die vor allem aus dem Einsatz von Standardelementen resultiert.

Allerdings beschränkt sich diese positive Einstellung zu Video over IP derzeit auf die Verwendung von kabelbasierenden Videokameras. Es konnte gezeigt werden, dass Video over WLAN noch keine ausreichende Marktreife hat, dabei ist es nicht die fehlende Anzahl an drahtlosen Produkten. Das Kernproblem besteht in den unzureichenden Sicherheitsmechanismen. Die nachfolgende Tabelle verdeutlicht, dass es durchaus genügende drahtlose Kameras gibt, die meisten aber nur den sehr zweifelhaften WEP-Standard unterstützen, WPA ist z.B. eher die Ausnahme.

Fazit

Der Kongress hat gezeigt, dass die Einführung von IP im Bereich der Gefahren- und Meldtechnik viele, heute zum Teil noch nicht erkennbare Chancen bieten wird. Diese Chancen führen sowohl zu einer Reduzierung der Kosten als auch zur Erlangung von Mehrwerten. Bis diese Vorteile genutzt werden können, gilt es noch viele Fragen, auch konzeptioneller Art, zu diskutieren und zu klären. Dass moderne IT-Infrastrukturen bei Beachtung einiger „goldenen Regeln“ in der Lage sein werden, Anwendungen der Gefahren- und Meldetechnik abzubilden, steht außer Frage. Es darf aber auch kein Zweifel darüber auftreten, dass die vollständige Ablösung der klassischen Gefahren- und Meldetechnik länger dauern wird bzw. möglicherweise nie vollkommen stattfinden wird. Bei der Einführung dieser neuen Techniken sollte man die Entwicklung im Bereich des „Industrial Ethernet“ beobachten, es gibt viele Parallelen und Lösungsansätze, die durchaus in einer modifizierten Form übernommen werden können.

Hinweis:
Der Autor hat im vorliegenden Artikel in Teilen Aussagen oder Bilder der Vorträge des Kongresses „Gefahrenmeldetechnik und Objektüberwachung im Netz 2005“ wiedergegeben oder verwendet, er bedankt sich bei den Referenten für die Nutzungsmöglichkeit.

CCNE

ComConsult Certified Network Engineer

Lokale Netze
03.04. - 07.04.06 in D'dorf
26.06. - 30.06.06 in Aachen
23.10. - 27.10.06 in Stuttgart
04.12. - 08.12.06 in Aachen

Internetworking
06.03. - 10.03.06 in Aachen
08.05. - 12.05.06 in Bonn
11.09. - 15.09.06 in Aachen
13.11. - 17.11.06 in Aachen

TCP/IP und SNMP
13.02. - 17.02.06 in Bonn
15.05. - 19.05.06 in Stuttgart
25.09. - 29.09.06 in Köln
27.11. - 01.12.06 in Berlin

Ethernet Technologien - neuester Stand
20.02. - 24.02.06 in Aachen
29.05. - 02.06.06 in Aachen
25.09. - 29.09.06 in Aachen
27.11. - 01.12.06 in Aachen

Paketpreis für alle vier Seminare € 8.244.-- zzgl. MwSt.
(Einzelpreise: je € 2.290.--)

Buchen Sie über unsere Web-Seite
www.comconsult-akademie.com

CCTS

ComConsult Certified Trouble Shooter

Trouble Shooting in Lokalen Netzwerken - Grundlagen
20.03. - 24.03.06 in Aachen
08.05. - 12.05.06 in Bad Neuenahr
04.09. - 08.09.06 in Aachen
06.11. - 10.11.06 in Aachen

Trouble Shooting in geswitchten Ethernet-Umgebungen
27.03. - 31.03.06 in Aachen
19.06. - 23.06.06 in Aachen
18.09. - 22.09.06 in Aachen
13.11. - 17.11.06 in Aachen

Trouble Shooting für TCP/IP- und Windows-Umgebungen
24.04. - 28.04.06 in Aachen
16.10. - 20.10.06 in Aachen

Paketpreis für alle drei Seminare, eine digitale Stromzange, die Prüfung und den Report „Fehlersuche in konvergenten Netzen" € 6.990.-- zzgl. MwSt.
(Einzelpreise: je € 2.490.--)

Buchen Sie über unsere Web-Seite
www.comconsult-akademie.com

CCSE

ComConsult Certified Security Expert

Sicherheit 1: Kernbausteine einer erfolgreichen Sicherheits-Lösung
15.05. - 19.05.06 in Stuttgart
11.09. - 15.09.06 in Bonn

Sicherheit 2: VPN Virtuelle Private Netze: Planung, Konfiguration, Betrieb
20.03. - 22.03.06 in Bad Neuenahr
19.06. - 21.06.06 in Weimar
25.09. - 27.09.06 in Köln

Sicherheit 3: Praxis-Intensiv-Seminar zur erfolgreichen Konfiguration von Firewall, VPN, Windows-Clienten, WLANs
03.04. - 07.04.06 in Aachen
26.06. - 30.06.06 in Aachen
23.10. - 27.10.06 in Aachen

Paketpreis für alle drei Seminare und Report „VPN-Technologien: Alternativen und Bausteine einer erfolgreichen Lösung" € 5.990.-- zzgl. MwSt. (Einzelpreise: € 2.290.-- / € 1.690.-- / € 2.290.-- / Report 398.--)

Buchen Sie über unsere Web-Seite
www.comconsult-akademie.com

Impressum

Verlag:
ComConsult Technology Information Ltd.
121 Paton Rd.
RD1
Richmond
New Zealand
GST Number 84-302-181
Registration number 1260709
Phone: 0064 3 5444632
Fax: 0064 3 5444237

German Hot-line of ComConsult-Research: 02408-955300
E-Mail: insider@comconsult-akademie.de
http://www.comconsult-research.de

Herausgeber und verantwortlich im Sinne des Presserechts:
Dr. Jürgen Suppan
Chefredakteur: Dr. Jürgen Suppan
Erscheinungweise: Monatlich, 12 Ausgaben im Jahr
Bezug: Kostenlos als PDF-Datei
über den eMail-VIP-Service der ComConsult Akademie