Software-Aspekte sicherer Datenkommunikation

Software aspects of multi-level secure data communications

Elektron. Rechenanl. 25 (1983), H. 4, S. 170–177
Manuskripteingang: 11. Februar 1983

von B. WALKE
AEG-TELEFUNKEN, Anlagentechnik
Geschäftsbereich Hochfrequenztechnik, Ulm

Ziel dieses Beitrages ist, alle für die Übertragung militärisch eingestufter Daten relevanten Software-Gesichtspunkte darzustellen und zueinander ins Verhältnis zu setzen.

Als besonders sicherheitsempfindlich erweist sich die Datenübertragung nach Standard X.25 (= Paketvermittlungstechnik). Es zeigt sich, daß alle mit der Datenvermittlung befaßten Rechner sogenannte „sichere" Betriebssysteme und zusätzlich „vertrauenswürdige" Software besitzen müssen.

Der Unterschied zwischen sicherer und korrekter Software wird erklärt, wobei klar wird, daß korrekte Software einen deutlich aufwendigeren Entwicklungsgang erfordert als sichere SW (dies bezieht sich insbesondere auf die Spezifikationsphase).

Für eine Reihe von Problemen werden erste Lösungen vorgestellt und diskutiert. U.a. wird deutlich, daß die bei militärischen Netzen in Westeuropa übliche Praxis, sich auf öffentliche Netze abzustützen, im Bereich der Paketvermittlung nur mit sehr starken Einschränkungen zulässig ist. Ein Ausblick auf zukünftige, digitale leitungsvermittelnde Netze zeigt, daß sie geeignet sein könnten, viele Sicherheitsprobleme von PV-Netzen zu beseitigen.

This paper aims at presenting and discussing the main software aspects being relevant for transmission of classified military data via wide area networks.

It appears that transmission of classified data does introduce a very high security risk when using not specially equipped packet switching networks. This risk can substantially be lowered by introducing multilevel secure operating systems and trusted software to perform the switching functions of such networks. A distinction is made between correct and secure (trusted) software, the former being much more expensive to develop than the latter.

First solutions are presented to solve problems being related to secure data comms. Besides others it is demonstrated that common practice with military data networks in Europe, namely to use public networks as fall-back resources, must be forbidden for packet switched applications, whenever classified data are to be transmitted. It is pointed out that future digital circuit switched networks might be better suited to perform transmission of classified data, than is possible via packet networks.

1 Einleitung

Die Datenkommunikation zwischen Teilnehmern an einem Verarbeitungsprozeß kann man, aus der Sicht des Kommunikationssystems, in drei Teilbereiche gliedern:

- Datenfernübertragung (mehr als 10 km Abstand zwischen Teilnehmern),
- Kommunikation in verteilten Systemen über lokale Netze (weniger als 10 km),
- Kommunikation innerhalb von Rechnersystemen (weniger als 100 m).

Im Fernbereich dominiert heute noch die für das analoge Fernsprechen entwickelte Leitungsvermittlungstechnik, bei der (nach neuerem Stand) in der Regel durch speicherprogrammierte Steuer-Rechner in Vermittlungsstellen physikalische Leitungen oder logische Kanäle zwischen ankommenden und abgehenden (Fern-)Leitungen durchgeschaltet werden. Die hierbei verfügbar gemachten zweigerichteten Telefonie-Sprechkanäle kann man nach Vorschaltung von MODEMs (Modulator-Demodulator) auch zur Verbindung von Datenendgeräten benutzen, wobei ein Sprechkanal eine Datenübertragungsrate bis zu 4.8 kbit/s erlaubt. Größere Datenraten sind erreichbar durch Benutzung parallelgeschalteter Sprechkanäle. Das Datex-L-Netz der Deutschen Bundespost verwendet diese Möglichkeiten und ist – von außen gesehen – ein Beispiel eines leitungsvermittelten Datennetzes.

Datenverkehr hat in vielen Anwendungen einen deutlich anderen Charakter als das Fernsprechen: Selbst auf nur einer der beiden Leitungen der Vollduplex-Verbindung kann man keinen kontinuierlichen, sondern nur burstartigen Verkehr (kurze Sendedauer, lange Pause) beobachten. Diese Tatsache führte aus Wirtschaftlichkeitsüberlegungen dazu, eine im Bereich der lokalen Rechner-Terminal-Verbindung entwickelte Technik, die Paketvermittlung, auch im Fernbereich einzuführen. Dabei werden die Leitungen der Datenendgeräte auf einen nahen

000 243 779

2425/2/07/B 2

Multiplexer geführt, der eine Konzentratorfunktion ausübt und selbst über nur wenige (meist eine) Multiplex-Leitungen mit der Vermittlung des Fernnetzes verbunden ist. Auf der Multiplexleitung wird in das Netz abgehender Verkehr der verschiedenen Datenendgeräte zeitlich verschachtelt, paketweise, nach dem asynchronen Zeitmultiplex-Verfahren übertragen. Die einzelnen Pakete gehören eindeutig bestimmten Verbindungen an und tragen entsprechende Adreßinformation. Ebenso ist auch der aus dem Fernnetz ankommende Verkehr paketiert und wird in der konzentrierenden Einrichtung auf die verschiedenen Datenendgeräte aufgeteilt (Demultiplex-Funktion).

Das Fernnetz selbst ist als Paketvermittlungs(PV)-Netz ausgeführt, d.h., es verwendet netzintern keine durchgeschalteten, sondern sogenannte *virtuelle* Verbindungen. Jede virtuelle Verbindung ist gekennzeichnet durch einen Listeneintrag und einen reservierten Pufferbereich in jedem der von dieser Verbindung berührten Vermittlungsknoten des Fernnetzes.

Einer virtuellen Verbindung wird eine physikalische Leitung nur dann zugeteilt, wenn ein Datenpaket zur Übertragung vorliegt (Speichervermittlung, store and forward). Das Datex-P-Netz der Deutschen Bundespost arbeitet nach diesem Prinzip. Die Vermittlungsfunktion eines Netzknotens wird jedesmal benutzt, wenn ein Datenpaket angekommen ist und auf eine von mehreren abgehenden Leitungen weitergegeben werden muß. Man verwendet speicherprogrammierte Vermittlungsrechner, die aus dem Inhalt jedes zu vermittelnden Paketes die Zugehörigkeit zu einer virtuellen Verbindung erkennen und demgemäß Pakete weiterleiten.

Sowohl bei Leitungs- als auch Paketvermittlung folgt auf den Verbindungswunsch eines Teilnehmers die Verbindungsaufbau-Phase, danach die Übertragungsphase und schließlich der Abbau der Verbindung. Evtl. werden permanente Verbindungen benutzt.

Im Gegensatz zum leitungsvermittelnden Netz nutzt der Vermittlungsrechner des PV-Netzes Daten, die während der Übertragungsphase anfallen, für die Vermittlungsaufgabe; er hat Zugang zu diesen Daten.

Gemeinsam ist beiden Vermittlungstechniken, daß die Vermittlungsrechner während der Verbindungsauf- und -abbau-Phase verbindungsbezogene, z.T. von den Endgeräten erzeugte, Daten handhaben.

Im folgenden wird anstelle von Vermittlungsrechner allgemeiner der Begriff Kommunikationsrechner verwendet. Damit wird ausgedrückt, daß u.U. nicht nur die Vermittlung (im Sinne der gezielten Weitergabe empfangener Daten), sondern auch weitere Funktionen wahrgenommen werden können.

Beispiele solcher Funktionen sind
- Geschwindigkeitsumsetzung
- Codewandlung
- Prozedurwandlung
- (De)-Multiplexen.

Alle eben für das Fernnetz beispielhaft geschilderten Vermittlungsaufgaben fallen im Bereich lokaler Netze oder in Rechnersystemen (mit mehreren Prozessoren) ebenfalls an und werden entsprechend gelöst [41]. Man kann deshalb die Vermittlungsaufgabe bei der Datenkommunikation unabhängig von der Entfernung zwischen den beteiligten Teilnehmern betrachten. Das gilt jedenfalls für den hier betrachteten Teilbereich, der sich mit der sicheren und korrekten Funktion der Vermittlungssoftware in Rechnern befaßt.

Die Datenübermittlung stellt gegenüber dem Fernsprechen weit härtere Forderungen.

1) Die vermittlungsbedingte Fehlerrate muß deutlich kleiner sein.
2) Der Datenschutz muß gewährleistet sein (Übersprechen).
3) Die Abhörsicherheit muß garantiert werden usw.

Solche Forderungen lassen sich bei digitaler Übertragung leichter als bei analoger erfüllen, führen aber zu komplizierteren Verarbeitungsprozessen innerhalb des Netzes und erhöhen das Risiko von (un)beabsichtigten Fehlern.

Digitalisierte Daten werden zunehmend, nach ihrer Eingabe vom Menschen in ein Rechnersystem, automatisch verteilt, verwaltet und verarbeitet, ohne wesentliche ständige Kontrolle durch Menschen. Die Frage nach der Sicherheit der Verarbeitung innerhalb von Rechnern und der Vermittlung an die richtigen Empfänger ist ohne die Verarbeitung schutzbedürftiger Daten gegenstandslos.

Beispiele schutzbedürftiger Daten sind
- Bilanzen von Firmen,
- Konten von Privatpersonen,
- Personaldaten,
- Bestell-/Lagerbestands-Daten von Firmen,
- militärische Daten usw.

Wir gehen im folgenden davon aus, daß vermittelnde Einrichtungen softwaregesteuert arbeiten und Zugang zu Daten der Übertragungsphase haben. Als Hauptbeispiel wird die Paketvermittlung über ein Fernnetz betrachtet. Die Empfehlung X.25 der CCITT für die Gestaltung der Schnittstelle zwischen Datenendgerät und Netzeingang ist heute weltweit akzeptiert und wird angewendet. Deshalb wird hier von PV-Netzen nach X.25 bzw. kurz X.25-Netzen gesprochen. Es bleibt zu erwähnen, daß diese Empfehlung X.25 den gesicherten Datentransport zwischen Endgeräten ermöglicht, indem die an der Netzschnittstelle angewandten Regeln analog innerhalb des Netzes fortgeschrieben werden.

Von den drei oben genannten Forderungen werden 1) und 2) vom Ansatz her erfüllt.

1.1 Komponenten eines X.25-Netzes

Bild 1 zeigt die Struktur eines PV-Netzes und die beteiligten Komponenten.

Alle in Bild 1 zum X.25-Netz gehörigen Prozessoren und Leitungen bilden den Netzkern. Außerhalb des Netz-

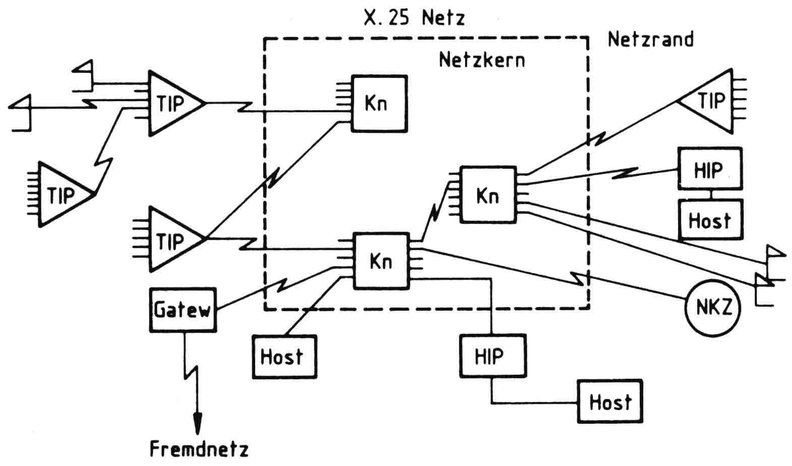


Bild 1. Beispiel für die Struktur eines Rechnernetzes mit Paketvermittlung nach X.25.

TIP = Terminal Interface-Prozessor
Kn = Vermittlungsknoten
Host = DV-Anlage
Gatew = Anpaßrechner zwischen zwei unterschiedlichen Netzen
NKZ = Netz-Kontrollzentrum
HIP = Host-Interface-Prozessore
—— = Datenübertragungs(DFÜ)-Leitung

kerns liegt der Netzrand, der die Terminals, Terminal-Interface-Prozessoren (TIP), Host-Interface-Prozessoren (HIP), Hosts und alle Leitungen sowie das Netzkontrollzentrum (NKZ) umfaßt.

Das X.25-Netz bildet das Transport- und Vermittlungssystem zwischen Terminals und/oder Hosts und hat die Aufgaben [11]

- Vermittlung der Pakete, gestützt auf das netzspezifische evtl. lastabhängige Routingverfahren unter Nutzung der paketspezifischen Adreßinformation,
- Abhandlung der ISO-Protokolle bis X.25 am Netzrand mit entsprechender Anwendung im Netz zwischen den Knoten und X.75 beim Übergang zu anderen X.25-Netzen,
- Verwaltung des gesamten Netzes einschließlich der daran angeschlossenen Komponenten zur Erkennung bestimmter Betriebssituationen mit Möglichkeiten für geeignete Reaktion darauf sowie für Statistik-Zwecke.

● Terminal-Interface-Prozessor (TIP)

Er dient zum Anschluß von entfernten Terminals (Fernschreiber, Sichtgerät, Drucker, Leser, Stanzer, Speicher) an die Anwendungssysteme in den Hosts unter Zwischenschaltung des X.25-Netzes und hat u.a. folgende Aufgaben, vgl. Bild 2:

- Darstellung einer X.25-Schnittstelle zum Netz hin.
- Abhandlung der Terminalschnittstellen (= Gerätsteuerung) entsprechend den Ebenenprotokollen 1 bis 7 des ISO-Architekturmodells [11], wobei die Strukturierung meist terminalspezifisch, d.h. abweichend vom ISO-Modell ist.
- Evtl. Umsetzung der Protokollebenen 4–7 (Transport-, Sitzungs-, Präsentations- und Anwendungsprotokoll) der Terminals gegenüber dem Host bzw. seinem Kommunikationsprozessor, falls kein kompatibles Gerät.
- Anschluß von X.25-Terminals (falls erlaubt, dann diesbezüglich Verhalten wie Knoten).
- Administrative Aufgaben bzgl. Host und des benachbarten Netzknotens.
- Recovery-, Lade- und Überwachungsfunktionen.
- Funktionen zur Erhöhung der Zuverlässigkeit für die Terminals.

Der TIP hat eine Konzentratorfunktion, indem er vom Netz entfernt liegende Terminals über kurze Leitungen anschließt und deren Verkehr über eine (bzw. wenige parallele) Leitungen an das Netz weitergibt. Aus der Sicht des Netzes wirkt der TIP wie ein X.25-tüchtiges Endgerät. Der TIP heißt im folgenden auch Konzentrator.

● Host-Interface-Prozessor (HIP)

Er dient netzseitig dem Anschluß des Hosts an das X.25-Netz und hat dabei die gleiche Aufgabenstellung wie der Konzentrator. Hostseitig hat der HIP eine Kanalschnittstelle, und es gibt üblicherweise die Varianten

- alle Funktionen des ISO-Modells plus Netzverwaltung residieren im HIP. Dann verkehren Anwendungen im Host mit Funktionen der Ebene 7 (Anwendungs-Schnittstellenprotokoll) der Kommunikations-Software im HIP.

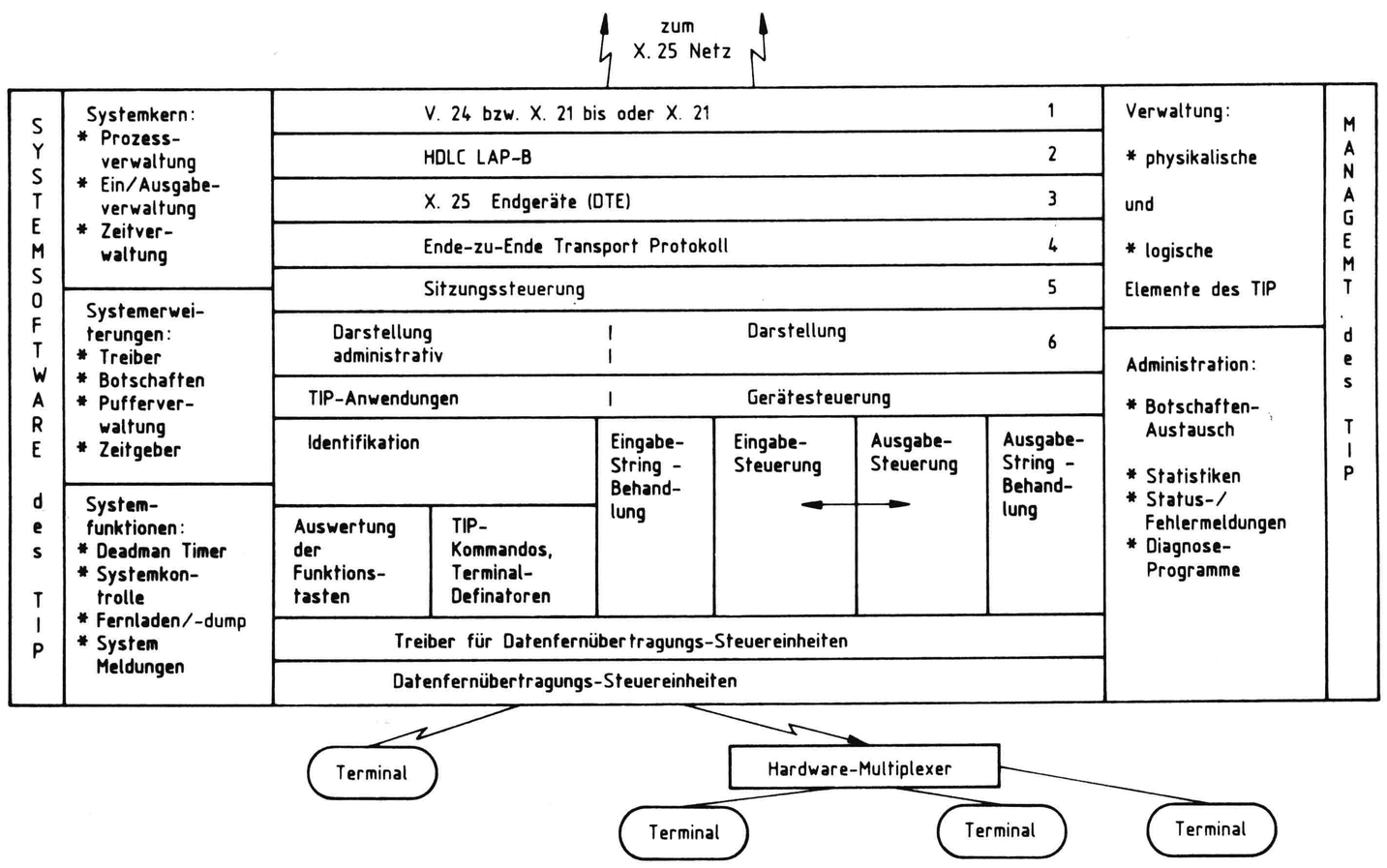


Bild 2. Struktur eines Terminal Interface Prozessors (TIP).

– Der HIP wickelt nur die unteren Ebenenprotokolle 1–4 netzseitig ab und verkehrt mit der Ebene 5 über seine Kanalschnittstelle zum Host.

● Netz-Anpaßrechner (gateway processor)

Er hat netzseitig dieselbe Schnittstelle wie die Knoten untereinander und besitzt bezüglich des nicht gezeichneten Netzes eine X.75-Schnittstelle, falls das Fremdnetz ebenfalls ein X.25-Netz ist, sonst hat dieser Rechner bzgl. des Fremdnetzes ähnliche Anpaßfunktionen wie der TIP bzgl. seiner Terminals. Das bedeutet, die Transportfunktionen der durch diesen Rechner verbundenen Netze sind anzupassen (Ebenenprotokolle 1 bis 3). Dabei sind Formate, Kommandos und Codes umzusetzen (Beispiel: Umsetzung von einem Datagramm-Netz auf ein X.25-Netz mit virtuellen Verbindungen). Flußkontrollmechanismen müssen für eine evtl. nötige Anpassung der Datenraten sorgen.

● Kommunikationsprozessoren

Konzentrator, Vermittlungsknoten, Host-Interface-Prozessoren und Netz-Anpaßrechner haben von der Art der Aufgabenstellung und der entsprechenden Hardware (HW)-Ausstattung gesehen große Ähnlichkeit. Die hier geeignete HW- und Software (SW) ähnelt sehr der von Prozeßrechnern. Man spricht von Kommunikationsprozessoren. Sie sind gekennzeichnet durch

– Anschlußmöglichkeit sehr vieler Datenleitungen,
– hohe Datenraten interner Verbindungen (Busse, Kanäle),
– sehr kurze Reaktionszeiten auf Interrupts der (Daten)-Peripherie,
– Ausstattung mit speziellen Leitungsprozessoren für übliche Datenübertragungsprozeduren.

2 Sicherheit bei der Datenkommunikation

Datennetze schaffen die Möglichkeit, entfernte Rechner zu verbinden und Benutzern von überall Zugang zu den Rechnern zu ermöglichen.

Die Benutzer unterscheiden sich oft in ihren Berechtigungen für den Zugang zu schutzwürdigen Daten der Rechner. Benutzer mit gleichen Berechtigungen können sich darin unterscheiden, daß sie unterschiedliche Ausschnitte von Daten der gleichen Schutzklasse für ihre Arbeit benötigen (need-to-know-Prinzip).

Offensichtlich muß die Verwaltung des Netzes und seiner Komponenten sicherstellen, daß die verwalteten Daten angemessen unterteilt und so geschützt werden, daß jeder Benutzer nur Zugang zu Daten erhält, für die er ein Zugangsrecht besitzt.

Da dieser Aspekt sowohl beim unmittelbaren Anschluß eines Terminals an seinen Host wie auch über ein Netz gleich wichtig ist, wollen wir generell dieses Problem im Kontext der Datenkommunikation betrachten. Die Zwischenschaltung eines Netzes schafft zusätzliche Sicherheitsprobleme. Es wird sich nachfolgend zeigen, daß solche Probleme mit einer einheitlichen Methodik behandelbar sind.

Die oben beschriebenen Bedürfnisse von Systembetreibern und Individuen bezüglich der Schutzwürdigkeit ihrer Daten führen zu Forderungen nach *Sicherheit* des Betriebes von Rechnern und Rechnernetzen. Die zugehörigen Aspekte sind für den militärischen Bereich bekannt und haben auch für zivile Anwendung Bedeutung.

2.1 Sicherheit und resultierende Forderungen

Sicherheit ist die Gewährleistung der (militärischen) Geheimhaltung aller Informationen und Ausschluß einer Beeinträchtigung der Funktionen des Gesamtsystem (durch sicherheitsgefährdende Kräfte). Dies bedeutet Forderungen nach

– Schutz vor böswilliger Behinderung (denial of service) normaler Arbeit durch Benutzer oder Programme. Mögliche Maßnahmen:
  – Organisatorische (organisations-intern: Klassifikation von Nutzern und Daten).
  – Personelle (Zugangsberechtigung zu Terminals und eingestuften Daten, DV-unterstützte Überwachung aller Abläufe durch Sicherheits-Beauftragte).
  – Infrastrukturelle (Dezentralisierung der Verarbeitung und Datenhaltung, Kommunikation über vermaschtes redundantes Netz, Baumaßnahmen).
  – Fernmeldetechnische (TEMPEST-getestete Geräte mit Unempfindlichkeit gegen Einstrahlung und geringer Abstrahlung).
– Datensicherheit.

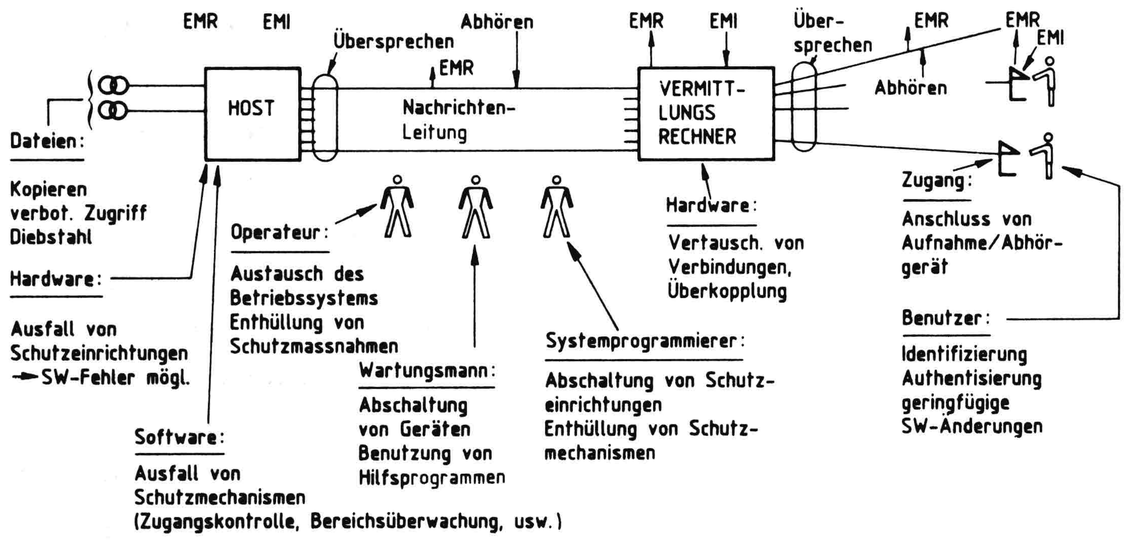
  Mögliche DV-technische und fernmeldetechnische Forderungen:
  – Datengeheimhaltung (Schutz vor unerlaubtem Informationsgewinn).
  – Datenintegrität (Schutz vor unerlaubter Informationsänderung).
  – Sichere Kommunikation (Leitungs- und Ende-zu-Ende Verschlüsselung, traffic flow security, Sicherung der Übertragung durch redundante Codes (CRC, Parity), sichere Vermittlung).

Trotzdem fordert man hohe Bedienqualität und Benutzerakzeptanz, geringe Komplexität und wenig zusätzlichen Aufwand an Rechenkapazität.

2.2 Ansatzpunkte für Sicherheitsbedrohungen

Bild 3 zeigt eine Übersicht über Sicherheitsschwachstellen bei der Datenverarbeitung und -übertragung mit Rechnern. Unterstellt ist, daß Teilnehmer über ein Rechnernetz mit ihrer Datenverarbeitungsanlage (Host) verbunden sind.

Alle bzgl. Hard- und Software des Host aufgeführten Gefahren bzw. Fehlerquellen kommen ebenso für den Vermittlungsrechner in Betracht.



EMI = Electro-Magnetic Interference (Störung)
EMR = Electro-Magnetic Radiation (Abstrahlung)

Bild 3. Sicherheits-Schwachstellen in einem Rechnernetz, nach [25].

Viele der aufgezählten Gefahren gehen von Menchen aus und erfordern entsprechend intelligente Vorbeugemaßnahmen. Darüber wird nachfolgend berichtet, soweit diese Maßnahmen durch Entwurf und Betriebsweise der Rechner ergriffen werden können.

Andere Gefahren ergeben sich deshalb, weil Datenverarbeitung und -übertragung mit elektrotechnischen Einrichtungen erbracht werden. Die diesbezüglichen Schutz- und Sicherheitsmaßnahmen sind nicht Gegenstand dieses Aufsatzes.

Im Bereich der Datenübertragung spielt die sichere Kommunikation mit den zugehörigen Maßnahmen Verschlüsselung und Sicherung durch redundante Codes die entscheidende Rolle, solange kein Netz zwischen Quelle und Senke zwischengeschaltet ist. Sonst kommt der Problemkreis der sicheren Vermittlung mit seinen Forderungen an die Betriebssoftware der Kommunikationsprozessoren hinzu.

Wir beschränken uns hier auf die Erläuterung von Maßnahmen zur Erhöhung der Sicherheit der Betriebssoftware der Kommunikationsprozessoren.

Der zugehörige Problemkreis hat ebenso auch Bedeutung für Hosts mit sicherheitsrelevanter Verarbeitung.

Probleme der Verschlüsselung bzw. Sicherung gegen Übertragungsfehler werden z. B. in [14; 15; 16; 28; 29] behandelt.

Ansatzpunkte für Bedrohungen beim Zugang/Zugriff zum System sind:

- Interfaces (Die Schnittstellen werden falsch benutzt),
- Protokolle (die Regeln der Prokolle werden nicht eingehalten) und
- Funktionseinheiten (die Funktion wird nicht korrekt erfüllt).

An den Bedrohungsansatzpunkten müssen auch die Maßnahmen zur Bedrohungsbekämpfung ansetzen.

Dies geschieht:

- Durch Bereitstellung sicherer Funktionseinheiten (Verifikation),
- durch sichere Algorithmen für die Behandlung von Kommunikationsprotokollen (Verifikation) und durch
- Isolierung von Systemteilen/Systemkomponenten, Schichten und Funktionseinheiten.

Nachfolgend wird gezeigt, daß einige der dem Softwarebereich zugeordneten Sicherheitsbedrohungen erfolgversprechend abgewehrt bzw. eingegrenzt werden können. Entsprechende Lösungsansätze sind vorhanden und werden skizziert, jedoch ist bei weitem noch nicht für jedes Problem ein fertiges Rezept vorhanden.

2.3 Lösungswege zur Erzielung der geforderten Datensicherheit

Wir beschränken uns auf die Darstellung der Maßnahmen, die der Datensicherheit in Systemen mit Rechnern gelten und lassen den Problemkreis „Schutz vor böswilliger Behinderung (denial of service)“ außer Betracht.

Es gilt als unbestritten, daß viele der für die Garantie der Datensicherheit eingeführten Maßnahmen auch die böswillige Behinderung des Systembetriebs erschweren. Jedoch ist bisher keine geschlossene Vorgehensweise bekannt, diese Bedrohung grundsätzlich auszuschließen, vielmehr stützt man sich auf den in Abschnitt 2.1 genannten Fächer von Einzelmaßnahmen.

Die hier beschriebene Methodik wurde im militärischen Bereich entwickelt. Die Darstellung der Vorgehensweise und der zugehörigen Ziele, Hilfsmittel und Möglichkeiten sowie der dabei gewonnenen Erfahrungen stützt sich auf offene Literatur, die praktisch ausschließlich aus US-amerikanischen Quellen stammt.

Lösung: Zugangskontrolle
- effiziente Überwachung des Zugangs
  - zum Rechnersystem überhaupt
  - zu den Daten des Rechnersystems

2.3.1 Sicherheitspolitik zur Regelung des Umganges mit Programmen und Daten

Ausgehend von den existierenden Regelungen für den Umgang von Menschen mit schutzwürdigen Dokumenten läßt sich auch für den Umgang mit Rechnern (als Verwalter der Dokumente) eine Sicherheitspolitik ableiten. Danach muß der gesamte Datenbestand klassifiziert werden, wobei die *Klassifikationsstufe* eine Aussage über seine Empfindlichkeit bezüglich der Offenlegung gegenüber einem feindlichen Agenten ausdrückt. Das führt auf vier Klassifikationsstufen (kurz Stufen):

In fallender Reihenfolge heißen sie „streng geheim“, „geheim“, „vertraulich“ und „offen“.

Zusätzlich gibt es innerhalb jeder Stufe Abteilungen (compartments), um den Informationsbestand einer Gruppe von Benutzern gegenüber einer anderen Gruppe abgrenzbar zu machen (z. B. atomic, cosmic, crypto, intelligence, NATO). Die Zugangsberechtigung für eine Abteilung schließt meist die Berechtigung für eine andere aus.

Darauf aufbauend läßt sich eine *Sicherheitspolitik* formulieren, welche die Zugangsrechte zu schutzwürdigen Informationen regelt und den Anforderungen der Datensicherheit genügt [4; 6]. Sie führt ein unvollständiges Ordnungsschema ein, nach dem der Benutzer mit höherer persönlicher Berechtigung Zugang zu entweder gleichhoch oder tiefer eingestufter Information hat. Vorausgesetzt, der Zugang ist als notwendig begründbar (need-to-know-Prinzip). Persönliche Berechtigungen werden entsprechend den Stufen vergeben. Jeder Zugreifer muß nicht nur für die Stufe, sondern gegebenenfalls auch für die Abteilung berechtigt sein. Zwei Hauptvertreter von Sicherheitspolitiken sind die gesetzlich geregelte formale und die willkürlich nach Gutdünken festgelegte Poltik.

Sicherheitspolitik, legt Zugangsregeln zu Code und Daten fest.

Komponenten:

1) Durch Vorgaben festgelegte Datenschutzpolitik (mandatory, non discretionary policy)
   - Information ist eingestuft (classification)
   - Benutzer haben Berechtigung (clearance)
   - Berechtigung muß höher/gleich Einstufung sein
   - Hierachische Festlegung der Zugriffsregeln
2) Nicht formell festgelegte Datenschutzpolitik (discretionary policy)
   - Zugang von Benutzern zu Daten nur bei nachweislicher Notwendigkeit (need-to-know)
   - Gitterartig strukturierte (lattice) Sicherheits-Abteilungen
   - Üblich in kommerziellen Rechensystemen

Zur Zeit diskutiert man noch überall auf der Welt, welche Regeln bei einer Sicherheitspolitik im Einzelnen beachtet werden sollten. In den USA hat sich das Verteidigungsministerium (department of defense, DOD) bereits auf eine Politik festgelegt [1], (vergl. Kasten 1).

Sie legt die Schutzmaßnahmen für die Speicherung und Verarbeitung bzw. Benutzung von Informationen durch Rechenanlagen fest und deckt den gesamten Sicherheitsbereich ab (vgl. die Aufzählung in Abschn. 2.1).

Diese Politik ist in einem Handbuch mit einer Aufzählung der notwendigen Einzelmaßnahmen detailliert worden [2].

Das folgende *Beispiel* erläutert die Anwendung einer Sicherheitspolitik:

Die Berechtigung eines Benutzers und seines Terminals wird, falls nicht anders vom Benutzer verlangt, auf das von ihm gestartete Programm übertragen. Während dieses Programm abläuft, kann es sein, daß die Einstufung von Daten des Programms automatisch durch das System geändert wird, um dadurch zu ermöglichen, daß anders (höher) eingestufte Dateien vom Programm benutzt werden können. Die Einstufung des Programms kann dabei höher werden als die des vom Benutzer verwendeten Terminals.

Z. B. darf ein für „streng geheim" berechtigter Benutzer von einem aufgrund der physikalischen Schutzmaßnahmen für „geheim" berechtigten Terminal aus ein „streng geheim" eingestuftes Programm laufen lassen, wenn keine „streng geheimen" Ein- oder Ausgaben über dieses Terminal laufen. Die Ausgabe des Programms könnte z. B. über einen „streng geheim" eingestuften Drucker erfolgen. Dieses Beispiel ist typisch für vom Terminal aus gestartete Stapelprogramme. Wesentlich ist nur, daß die Berechtigung des Benutzers die absolute Obergrenze für die Zugriffsrechte seines Programmes ist, es sei denn, das Programm ist (nach einem speziellen Entwicklungs- und Testweg) auch für die Bearbeitung höher eingestufter Daten zugelassen (wobei es jedoch dem Benutzer nur Daten seiner Berechtigung zugänglich macht).

Neben dem Kern eines Betriebssystems als zentrale Sicherheitsinstanz mit Zugang zu *allen* Daten – unabhängig von ihrer Einstufung – gibt es also u. U. weitere Programme, die höhereingestufte Daten speichern oder gar verarbeiten können, als es der Berechtigung des sie aufrufenden Benutzers entspricht. Sie sind bezüglich der Systemsicherheit ebenso wichtig wie der Kern selbst.

Berücksichtigt man die mögliche Trennung der Berechtigungen bzw. Einstufungen von Benutzern, Programmen und Ein-/Ausgabe-(E/A)-Geräten, dann kann man folgende Zugangsregeln aufstellen [25]:

Berechtigung	Einstufung		
	Eingabe	Programm	Ausgabe
Benutzer	≥	≥*)	≥
E/A-Gerät	≥	unabhängig	≥

*) Ausnahme: Speziell zugelassene E/A-freie Programme.

Die Matrix ist zu Lesen: Benutzer-(Geräte-)Berechtigung muß größergleich der Einstufung der Eingabedaten (Programm-, Ausgabe-Daten) sein.

Im Prinzip können Benutzer, Terminal, Programmcode, Programmdaten, Datei, Ein- und Ausgabe-Daten je eine eigene Berechtigung bzw. Einstufung haben.

2.3.2 Beispiele von im Aufbau/Betrieb befindlichen sicheren Systemen

Die Forderungen moderner Führungssysteme nach vollautomatisierter Haltung, Verarbeitung und Nutzung von militärisch eingestuften Daten, die – ohne aktive Kontrolle jedes Einzelfalls durch Sicherheitspersonal – über entfernt aufgestellte Terminals nicht nur gelesen, sondern auch aktiv verändert werden dürfen, erzwingt einen Systementwurf, der nach bestem wissenschaftlichen und technischen Stand die Integrität aller Datenbestände garantiert.

Gleichzeitig muß dieser Entwurf sicherstellen, daß der Nutzer am Terminal im Rahmen seiner Pflichten und Rechte freizügig und möglichst effizient arbeiten kann.

Ein Beispiel für die Realisierung eines sicheren Datenübertragungs-Netzes, das alle Anforderungen an sichere Kommunikation erfüllen will, ist das 1980 in Probebetrieb gegangene AUTODIN II-Netz*), ein mit Datagrammen arbeitendes Paketvermittlungsnetz (PV-Netz) des US-Verteidigungs-Ministeriums (Department of Defense, DOD) [10].

Es unterscheidet 16 Sicherheitsstufen und 512 Abteilungen. Andere Netze, in denen z. T. nur Einzelmaßnahmen für sichere Kommunikation realisiert wurden, sind SACDIN (Strategic Air Command Digital Network), WWMCCS (world wide military command and control service) sowie WIN (WWMCCS Intercomputer Network).

2.4 Ende-zu-Ende-Verschlüsselung (EZE-V)

Datenkommunikation findet immer zwischen zwei Partnern statt, und es ist plausibel, daß sie für sicherheitsempfindliche Daten eine Verschlüsselung, beginnend beim Absender und endend beim Empfänger, fordern. Entsprechend dem US-Standard FED-STD-1026 (Draft 2) sind fünf Sicherheitsziele zu beachten, die alle die Kompatibilität der Kommunikationspartner voraussetzen (deshalb ist ein EZE-V-Standard nötig):

1) Verhütung der Enthüllung von Klartext-Nachrichten, Erkennung der betrügerischen,
2) Veränderung einer Nachricht,
3) Einfügung einer Nachricht,
4) Zerstörung einer Nachricht,
5) Erkennung der Wiederholung einer früher gültigen Nachricht.

Es wird ein EZE-Standard angestrebt, der diese 5 Bedrohungen beseitigt und doch den Verkehr der Endgeräte verschiedener Hersteller untereinander zuläßt.

Die Datenkommunikation zwischen Partnern folgt in jedem Einzelfall einem bestimmten Regelwerk (Satz von Protokollen), das Steuersignale, Formate, Meldungslängen, Optionen usw. festlegt und damit Syntax und Semantik des Kommunikationsablaufs bestimmt.

Um die speziellen Anforderungen der Ende-zu-Ende-Verschlüsselung in dieses Regelwerk zu integrieren, müssen dort vorhandene Funktionen erweitert werden. Diese Funktionen lassen sich logisch gliedern.

Bild 4 zeigt das Architekturmodell der ISO für die Verbindungen von Daten-End-Einrichtung (DEE) über offene Kommunikationsnetze [32].

Die Beziehungen zwischen den verschiedenen Partnern des hierarchischen Systems werden durch Protokolle geregelt; dabei werden horizontale und vertikale Beziehungen unterschieden und entsprechend unterschiedliche Benennungen verwendet.

Ebenenprotokoll (peer-to-peer protocol): Satz von Regeln zum Austausch von schichtspezifischen Steuerdaten so-

*) Seit April 1982 wird statt dessen das Defense Data Network (DDN) aufgebaut, das auf ARPA-Net Technologie beruht [38].

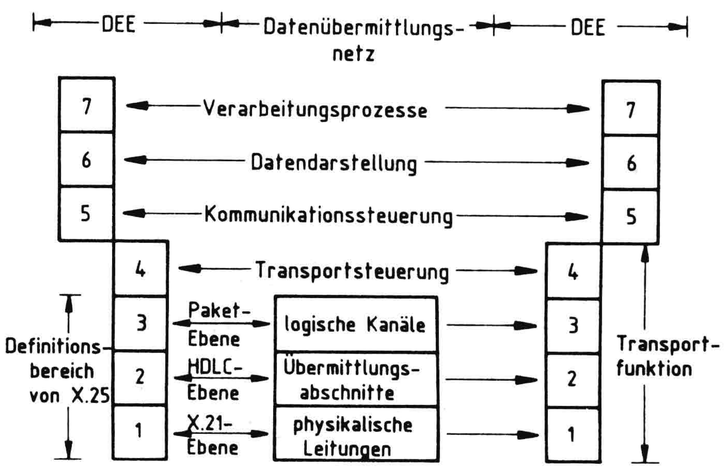


Bild 4. Schematische Darstellung der hierarchischen Struktur von Datenübermittlungsprotokollen nach dem Architekturmodell für „offene Kommunikationssysteme" der ISO.

wie von Nutzdaten im Auftrag der nächsthöheren Schicht. Die hierarchische Stellung des Protokolls wird durch einen einengenden Zusatz spezifiziert. Im ISO-Referenzmodell wird zur Kennzeichnung allgemein der Vorsatz (N)- verwendet, zum Beispiel heißt es dort (N)-layer oder (N)-protocol.

Schnittstellenprotokoll (interface protocol: Satz von Regeln zum Austausch von Steuerdaten und Nutzdaten zwischen benachbarten Schichten. Im ISO-Modell hat dieser Begriff keine unmittelbare Entsprechung.

In einem konkreten Rechnerverbundsystem gemäß dem ISO-Referenzmodell existieren also mindestens 7 Schichtprotokolle und 6 Schnittstellenprotokolle. Die Anzahl der Protokolle kann aber auch größer sein, wenn innerhalb einer Schicht bzw. im Verkehr benachbarter Schichten alternative Protokolle zur Verfügung stehen, von denen je nach Aufgabenstellung eines angewendet wird.

Nach den Bildern 5 und 6 unterscheidet man Leitungs-, Kanal-, Transport- und EZE-V. Leitungs- bzw. Kanal-V werden eingesetzt, wenn physikalische Leitungen bzw. Multiplexleitungen zwischen Punkt-zu-Punkt oder Mehrpunktverbindungen eingesetzt werden. Die Leitungen können privat oder Bestandteil öffentlicher Netze sein.

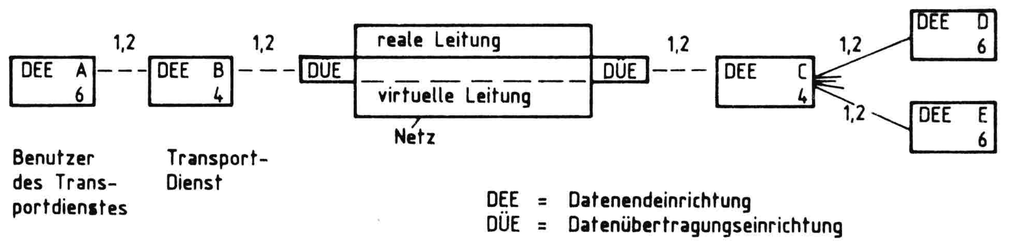


Bild 5. Verteiltes System. Die Zahlen geben an, in welcher ISO-Modell-Ebene jeweils bei der betreffenden Komponente bzw. Leitung verschlüsselt wird.

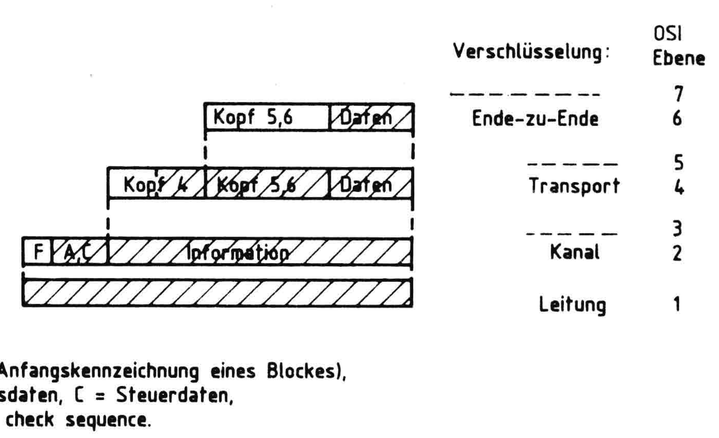


Bild 6. Aufsatzpunkte für Verschlüsselung im OSI (open system interconnection) Architekturmodell der ISO. Schraffierte Daten werden in der entsprechenden Ebene verschlüsselt.

Transport-V wird zum Schutz virtueller Verbindungen in Paketvermittlungsnetzen (X.25) zwischen den Datenendeinrichtungen eingesetzt, wobei viele Leitungsabschnitte enthalten sein können.

EZE-V schützt den Nachrichtenaustausch zwischen Anwendungen in verschiedenen Prozessoren: Z. B. sind in Bild 5 DEE A ein Host, DEE B sein Host-Interfaceprozessor, DEE C ein Terminal-Interfaceprozessor und DEE D bzw. E abgesetzte Terminals. Die Verschlüsselung in Ebene 6 schützt dagegen, daß der Host bzw. Terminal-Interfaceprozessor Daten (un)beabsichtigt vertauscht und damit die Datensicherheit verletzt.

Aus Bild 6 ist zu sehen, wie auf der Sendeseite mit zunehmender Aufbereitung für die Übertragung von Daten, ausgehend von der Ebene 7 (Anwendungsebene), Adreß- und Steuerinformationen in den Ebenen 6 bis 2 zugefügt werden und welche Daten jeweils verschlüsselt werden dürfen. Die verbliebenen offenen Daten werden jeweils von der benachbarten Ebene benötigt, um arbeiten zu können. Beispielsweise erkennt Ebene 2 Blöcke der HDLC-Prozedur an den flags F.

Auf der Empfängerseite werden die verschlüsselten Daten schrittweise aufgedeckt, bis schließlich in Ebene 7 wieder Klartext vorliegt. Man beachte, daß in den Ebenen 1 und 2 abschnittweise verschlüsselt wird. nämlich Punkt-zu-Punkt, vgl. Bild 5. Die Verschlüsselung in Ebene 1 verwendet man, um traffic flow security zu garantieren, d. h., zu verhindern, daß aus z. B. der Zahl der feststellbaren HDLC-Blöcke Rückschlüsse auf den derzeitigen Nachrichtenfluß gezogen werden.

Um in den entsprechenden Schichtprotokollen die Ver- bzw. Entschlüsselung vornehmen zu können, benötigt man zusätzliche Steuerkommandos und -antworten zu den für die Kommunikation ohne Verschlüsselung notwendigen Kommandos, d. h., die Schichtprotokolle müssen erweitert werden. Nach [27] zielen Arbeiten zur Normung eines Standards zur Verschlüsselung in der Transportebene 4 darauf ab, Verschlüsselungseinrichtungen verschiedener Hersteller kompatibel arbeitsfähig zu machen. Beispielsweise müssen festgelegt werden:

- Die Stationstypen (Primary, Secondary, Combined Station).
- Die Art der Verbindung (Punkt-zu-Punkt, Mehrpunkt).
- Die Betriebsphasen (ruhend, Kommando, Daten-Transfer).
- Schlüsselverteilungsmodus, Authentisierungsverfahren, Verifikation von beanspruchten Rechten eines Teilnehmers mit Hilfe eigener Berechtigungs-Verzeichnisse.
- Auswahl des Verschlüsselungsmodus.
- Weitere sicherheitsrelevante Aktivitäten.

EZE-Verschlüsselung befaßt sich wegen seiner Anwendungsnähe mehr mit „Information" als mit „Kommunikation", jedoch bestehen in der Vorgehensweise große Ähnlichkeiten zwischen Transport- und EZE-Verschlüsselung. Man erwartet, daß sehr ähnliche Standards für beide Bereiche entwickelt werden.

(wird fortgesetzt)

DIE BEITRÄGE DIESES HEFTES WURDEN GESCHRIEBEN VON

Dr.-Ing. *Bernhard Walke* (42). Diplom in Elektrischer Nachrichtentechnik, TH Stuttgart 1965. Anschließend Mitarbeiter, später Abteilungsleiter bei AEG-TELEFUNKEN in Ulm. Zunächst im Forschungsinstitut bis 1981, später im Geschäftsbereich Hochfrequenztechnik. Promotion 1975, Uni Stuttgart. Seit Oktober 1983 o. Prof. für Datenverarbeitungstechnik im FB Elektrotechnik der Fernuniversität Hagen. Zahlreiche wiss. Veröffentlichungen zur Leistungsanalyse von und über Abfertigungsstrategien in Rechensystemen, darunter das Buch „Realzeitrechner-Modelle", Oldenbourg: 1978. Arbeitsgebiete: Warteschlangenmodelle (Analyse und Simulation), Protokolle der Datenübertragung, Organisation des Ablaufs in verteilten Systemen, Sicherheit bei Datenkommunikation. Mitglied in GI und NTG. 1979-81 Sprecher, heute Mitglied des Leitungsgermiums der GI/NTG Interessengruppe „Messung, Modellierung und Bewertung von Rechensystemen".