Zeitschrift: Bulletin des Schweizerischen Elektrotechnischen Vereins, des Verbandes Schweizerischer Elektrizitätsunternehmen = Bulletin de l'Association Suisse des Electriciens, de l'Association des Entreprises électriques suisses

Band: 87 (1996)

Heft: 3

Artikel: Das Informatik-Notfallkonzept als Element der Notfallplanung : Teil 1 : wieso brauchen Unternehmen ein Informatik-Notfallkonzept?

Autor: Umiker, Bruno / Peer, Alfred / Truttmann, Paul A.

DOI: https://doi.org/10.5169/seals-902298

Die Abhängigkeit der Unternehmen von der Informatik hat bedrohliche Dimensionen angenommen. Bei Ausfall dieser Dienstleistung durch einen Schaden oder gar eine Katastrophe grösseren Ausmasses steht der Betrieb über längere Zeit still und eventuell geht gar nichts mehr. Dies kann bis zum Konkurs führen. Die Informatik-Notfallplanung macht möglich, diesem Risiko zu begegnen und ein Massnahmenpaket zu erarbeiten, das nach kurzer Zeit greift. So bleiben dem Unternehmen die lebensnotwendigen Informatikdienstleistungen erhalten.

Das Informatik-Notfallkonzept als Element der Notfallplanung

Teil 1: Wieso brauchen Unternehmen ein Informatik-Notfallkonzept?

■ Bruno Umiker, Alfred Peer, Paul A. Truttmann

Die Abhängigkeit auch Ihres Unternehmens von der Informatik hat in den vergangenen Jahren stetig zugenommen und wird weiter wachsen. Einst lag der Schwerpunkt der EDV in der Administration (Finanz- und Rechnungswesen, Personaladministration, Lagerbuchhaltung), wobei die Datenverarbeitung ausschliesslich im Batchbetrieb erfolgte. Durch die rasante Entwicklung in der Computertechnologie wurden neue Anwendungsgebiete erschlossen und gleichzeitig neue Verarbeitungsformen ermöglicht.

Das Vordringen der EDV aus den klassischen Anwendungsbereichen der Administration (operationelle Informationssysteme) in die Unterstützung der Planungsprozesse im Betrieb und in der Fertigung (dispositive Informationssysteme, wie PPS, Materialdisposition, später CAD, CAE, CAQ zu CIM) bedeutet einen wesentlichen Schritt der Anwender in die Abhängigkeit von der Verfügbarkeit der EDV-Dienstleistungen. Der gleichzeitige Wandel der EDV zur Informatik (Ausweitung der Datenverarbeitung über die Elemente Text, Bild [Grafik] und Sprache), die zunehmende Verschmelzung mit der Kommunikations- und Nachrichtentechnik (Dialogverarbeitung, Datenfernverarbeitung, Netzwerke, ISDN usw.) erhöht diese Abhängigkeiten weiter. Der Einzug der Personalcomputer in die Büros und Werkstätten, ihre sukzessive Einbindung in Netzwerke sowie die Ausweitung der Applikationen in strategischen Bereichen (Führungs-, Planungs-, Marketinginformationssysteme u. dgl.) verschärfen die Abhängigkeitssituation noch mehr.

In den meisten Unternehmen ist dadurch die Kritikalität* einer Störung oder gar Katastrophe im Informatikbereich enorm angewachsen. Damit in einem solchen Störfall die Unternehmung nicht in bedrohliche Situationen gerät, sondern adäquat reagieren kann, ist ein entsprechendes Informatik-Notfallkonzept auszuarbeiten. Es muss alle notwendigen Interventionsplanungsmassnahmen sowie alle präventiven und planbaren, situativen Vorkehrungen enthalten, damit schliesslich ein Katastrophenfall bewältigt werden kann. Damit soll verhindert werden, dass eines Tages über Ihr Unternehmen solches oder ähnliches in der Tagespresse zu lesen ist:

«Ein sehr erfolgreicher, international tätiger Industriekonzern hatte bei der Planung seines neuen Rechenzentrums gewisse periphere Risiken massiv unterschätzt. Eine Feuersbrunst in der angrenzenden Schreinerei der Firma führte deswegen zur vollständigen Zerstörung von Hard- und Software sowie der im gleichen Gebäude gelagerten Sicherungs-

Adresse der Autoren:
Bruno Umiker, dipl. El.-Ing. ETH, lic.phil.,
Alfred Peer, Wirtschaftsinformatiker, und
Paul A. Truttmann, Dr. sc. nat. ETH, lic. phil.,
Walter Umiker+Co. AG, 8029 Zürich.

* Kritikalität: Summe aller nicht einfach messbaren Konsequenzen aus einem Störfall wie Verlust an Image oder schöpferischer Kraft, seelische Störungen oder politische Instabilität, allgemeine betriebliche Konsequenzen, personelle Konsequenzen, Machtverlust.

Risiko- und Bedrohungsszenarien

- Brandschäden, Rauchschäden, Blitzschlag, Explosionen, Elementarereignisse (Hochwasser, Überschwemmungen, Sturm, Erdrutsche usw.), Erdbeben, Vibrationen, Immissionen, korrosive Dämpfe, abstürzende Luftfahrzeuge, Wasserschäden
- externe kriminelle Handlungen wie Diebstahl, Beraubung, Sabotage, Spionage, Blockade, Bombendrohung, Sprengstoffanschläge, Krawalle, Plünderungen
- Unfälle mit physikalischer Zerstörung der EDV-/IDV-/Netz-Infrastruktur
- interne Ereignisse
- technisches Versagen/Störungen an Maschinen, Hardware, Software, Infrastruktur, Telekommunikation
- menschliches Versagen, Kompetenz- und Ausbildungsmängel, organisatorische Mängel, Fehlbedienung, fahrlässige Zerstörung
- interne kriminelle Handlungen (mutwillige Zerstörung, Sabotage, Spionage, Diebstahl, Beraubung, Datenmanipulation)
- Datenverlust, Verlust der Programm- bzw. Datenintegrität und Datenkonsistenz, Computerviren, Patent-, Urheber- und Nutzungsrechtsverletzungen usw.

Tabelle I

dateien. Da zudem ein Notfallkonzept fehlte, standen schlagartig sämtliche Informatikdienstleistungen über längere Zeit nicht mehr zur Verfügung.»

Welche Ereignisse können zu Informatik-Katastrophen führen?

Es ist nicht nur der «typische Standardfall» der Brandkatastrophe, welche zu einem länger dauernden Ausfall der Informatikdienstleistungen führen kann. So zerstörte beispielsweise eine Sturmflut in Hamburg ein grosses Rechenzentrum vollständig. Diese Arten von Ereignissen (Hochwasser, Überschwemmungen, Sturm, Erdrutsche usw.) gehören zu den Risikopotentialen mit den höchsten Zuwachs- und Schadensraten, wie die jüngsten Beispiele von Hochwasserkatastrophen im Rheinland und im Alpenraum drastisch vor Augen führen.

Eine Reihe weiterer ernstzunehmender Risiken bedroht die heute meist lebenswichtigen und unverzichtbaren Informationsverarbeitungsfunktionen der Unternehmen. Sie sind in Tabelle I zusammengefasst aufgelistet.

Welche Schäden können entstehen?

Am Beispiel eines Katastrophenfeuers sei aufgezeigt, welche wesentlichen Teile der Informatik und betroffener peripherer Bereiche zerstört werden können:

- das Rechenzentrum (Computerraum) mit seiner gesamten Hardware, Software, Infrastruktur samt den Kommunikationseinrichtungen
- sämtliche aktuell auf den Systemen vorhandenen Softwarekomponenten und Anwendungsprogramme
- sämtliche aktuell auf den Systemen gespeicherten Stamm-, Bewegungs- und historischen Daten
- sämtliche innerhalb des Katastrophenbereichs befindlichen, noch nicht verarbeiteten Urbelege sowie Informationen und Daten in Papierform
- sämtliche Arbeitsplätze inkl. Terminals, Personalcomputer und Arbeitsplatzdrucker
- sämtliche Organisationssachmittel wie Belegleser, Mikroverfilmungsanlagen, Poststrassen, Frankierautomaten, Telefonapparate und Telefax usw.
- die Telefonzentrale, Sprach- und Datenleitungen

Welches sind die Folgen, wenn keine Vorkehrungen getroffen sind?

Hat ein Unternehmen versäumt, die erforderlichen Vorkehrungen zu treffen, um einen vollständigen Ausfall der Informatikdienstleistungen als Folge von Katastrophenereignissen zu verhindern, muss es mit gravierenden Konsequenzen (Tabelle II) rechnen. Das Fatale dabei dürfte sein, dass die Folgeschäden diejenigen des eigentlichen Katastrophenereignisses bei weitem übersteigen werden. Dies ist um so wahrscheinlicher, je höher der Grad an computerunterstützter Informationsverarbeitung in einem Produktions-, Handels- oder Dienstleistungsunternehmen ist. Das gleiche Los kann private oder öffentliche Institutionen treffen.

Die Produktion von Waren und Dienstleistungen wird massiv gestört. Warenwirtschaft, Disposition und Qualitätssicherung können nicht mehr gewährleistet werden. Die Forschungs- und Entwicklungsarbeiten stehen still. Die gewohnten Mittel zur Führung und Steuerung des Unternehmens fehlen, die innerbetriebliche Kommunikation und Koordination wird erschwert. Die Produktions- und Distributionslogistik und damit die Versorgung des Marktes sind nicht mehr sichergestellt und unterziehen dadurch die Kundenbeziehungen einer enormen Zerreissprobe. Lieferungen und Leistungen können nicht mehr fakturiert werden, was zudem die Firma in Liquiditätsengpässe stürzen kann. Fehlen entsprechende Reserven, kreist bald der Pleitegeier über dem verkohlten Fabrikgemäuer . . .

Das Fatale dabei dürfte sein, dass die Folgeschäden diejenigen des eigentlichen Katastrophenereignisses bei weitem übersteigen werden.

Dieses Bedrohungspotential für das Gesamtunternehmen ist vielfach nicht einsichtig. Viele, gerade grössere und mittelständische Firmen neigen zur Ansicht, einen Informatikkatastrophenfall ohne schwerwiegende Auswirkungen über längere Zeit «überbrücken» zu können. Gestützt wird dieser schwerwiegende Irrtum vielfach mit dem Hinweis, man habe ja früher oder vor noch nicht allzu langer Zeit auch ohne oder nur mit sehr geringer EDV-Unterstützung alle wichtigen Funktionen abwickeln können. «Es müsste doch in einem Katastrophenfall möglich sein, mit zwar behelfsmässigen, aber sehr einfachen Mitteln die wichtigsten Aufgaben und Arbeiten zu erledigen . . .»

Selbst in Unternehmen, welche in Risk-Management-Belangen sehr umsichtig und professionell agieren, gibt es vielfach

Folgeschäden aus Informatik-Katastrophenfällen

- Störung von Produktion, Warenwirtschaft, Disposition und Qualitätssicherung
- Stillstand der Forschungs- und Entwicklungsarbeiten
- Marktversorgungsprobleme (Produktions- und Distributionslogistik)
- Liquiditätsengpässe infolge fehlender Fakturierung der erbrachten Lieferungen und Leistungen
- Störung der innerbetrieblichen Kommunikation und Koordination
- weitere, schwer vorhersehbare Störungen und Schäden

Tabelle II

Ablaufphasen zu Katastrophenereignis (ausserhalb der Arbeitszeit)	
Vor Eintritt des Katastrophenereignisses	Die Datenverarbeitung geht ihren gewohnten Gang (Normalbetrieb). Niemand ahnt die über das Unternehmen hereinbrechende Katastrophe. Letzte Datensicherung (Saves) (10) Täglich (in der Regel nachts nach Abschluss der Tagesarbeiten) erfolgt mindestens eine vollständige Datensicherung auf allen Computersystemen. Somit kann davon ausgegangen werden, dass eine vollständig ausgelagerte Datensicherung höchstens 24 Stunden alt ist. Ungesicherte Daten (11) • Die nach der letzten Datensicherung bis zum Eintritt des Katastrophenereignisses vollzogenen Daten- und Programmänderungen sind nicht gesichert und gehen somit verloren. Sie müssen nach wiederaufgebauter Funktionsfähigkeit des Rechenzentrums oder des EDV-Betriebs im Backup-Rechenzentrum zuerst nachgearbeitet werden.
Während des Katastrophenereignisses	Das Katastrophenereignis (20) tritt irgendwann ein und beginnt sich in der Regel langsam zu entwickeln und dann auszuweiten. Nach einer gewissen, nicht zum voraus definierbaren Zeit wird dann das Ereignis entdeckt. Ereignisentdeckung (30) • Das Entdecken des Ereignisses kann entweder durch zufällige oder geplante menschliche Beobachtung oder durch eine vorhandene automatische Alarmierungsanlage erfolgen. • Im Falle eines Brandes kann die Ereignisentdeckung sehr spät, im Extremfall erst nach Eintritt des Feuersprungs erfolgen, falls keine Brandmeldeanlage vorhanden ist. Dies könnte bewirken, dass die Löschkräfte viel zu spät alarmiert werden, wodurch das Risiko einer Grosskatastrophe zunimmt.
Externe Interventionen	In der Regel, besonders ausserhalb der Arbeitszeit bzw. nachts, treten zuerst externe Interventionskräfte in Aktion: • Alarmierung der externen Interventionskräfte (31) • Automatisch entdeckte Brände werden direkt durch die Brandmeldeanlage an externe Interventionskräfte (Feuerwehr) gemeldet. • Durch Beobachtung entdeckte Schadenereignisse müssen durch telefonische Alarmierung an die Interventionskräfte gemeldet werden. Reaktionszeit der Interventionskräfte (32) • Nach manueller telefonischer oder automatischer Alarmmeldung rücken die Interventionskräfte sofort aus. Bis zum Eintreffen am Schadenplatz benötigen sie je nach Entfernung, Tageszeit und Verkehrslage unterschiedlich lange Zeit. Währenddessen kann sich das Schadenereignis weiter entwickeln, üblicherweise, ohne dass wesentliche Massnahmen dagegen ergriffen werden können. Lagebeurteilung und Interventionsentscheide (33) • Nach dem Eintreffen der Interventionskräfte macht der Schadenplatzkommandant zuerst eine sofortige Lagebeurteilung und erteilt daraufhin den Ersteinsatzbefehl. Intervention (34) • Die Interventionskräfte beginnen mit ihren Rettungs- und Löscharbeiten. Die Intervention dauert so lange, bis das Schadenereignis unter Kontrolle gebracht ist. Danach kann mit den Untersuchungs- und später mit den Aufräumarbeiten begonnen werden. Dies kann Stunden bis mehrere Tage dauern.
Unternehmensinterne Interventionen	In der Regel, besonders ausserhalb der Arbeitszeit bzw. nachts, müssen die internen Verantwortlichen zuerst alarmiert und aufgeboten werden: Telealarm an die Alarmierungsgruppe (40) • Automatisch entdeckte Brände werden direkt durch die Brandmeldeanlage an die im Alarmierungshandbuch bezeichneten Alarmverantwortlichen in der entsprechenden Reihenfolge gemeldet. • Bei durch Beobachtung entdeckten Schadenereignissen erfolgt die Benachrichtigung der unternehmensinternen Alarmverantwortlichen durch die externen Interventionsinstanzen (Feuerwehr, Polizei) zu gegebener Zeit. Reaktionszeit der Alarmierungsgruppe (41) • Die via Telealarm oder die externen Interventionsinstanzen alarmierte Person begibt sich so schnell wie möglich vor Ort und erkundigt sich über den Alarmierungsgrund. Lagebeurteilung und Alarmierung des Krisenstabes Informatik (42) • Je nach vorherrschender Situation entscheidet die alarmierte Person in eigener Kompetenz und Verantwortung über die unmittelbar zu treffenden Massnahmen, entsprechend den Richtlinien und Anweisungen im Interventionshandbuch, im speziellen darüber, ob der Krisenstab Informatik aufgeboten werden muss. Reaktionszeit Krisenstab Informatik bzw. Gesamtkrisenstab (43) • Bei einem Grossereignis muss neben dem Krisenstab Informatik eventuell der erweiterte Krisenstab des Unternehmens benachrichtigt bzw. aufgeboten werden Erste Lagebeurteilung durch Mitglieder des Krisenstabes (50) • Es kann im Extremfall längere Zeit dauern, bis der Krisenstab entscheidungsfähig ist. Die zuerst am Schadenplatz anwesenden Mitglieder des Krisenstabes nehmen ihrerseits eine erste Beurteilung der Lage vor und leiten gegebenenfalls erste Massnahmen ein. Erste Sitzung des Krisenstabes (51) • Sobald der Krisenstab für die Informatikbelange in entscheidungsfähiger Zusammensetzung vorhanden ist, wird er, entsprechend der analysierten Situation (52) und allfälliger Vorgaben des übergeordneten Krisenstabes, über die erforderlichen Massnahmen entscheiden (53).

Tabelle III

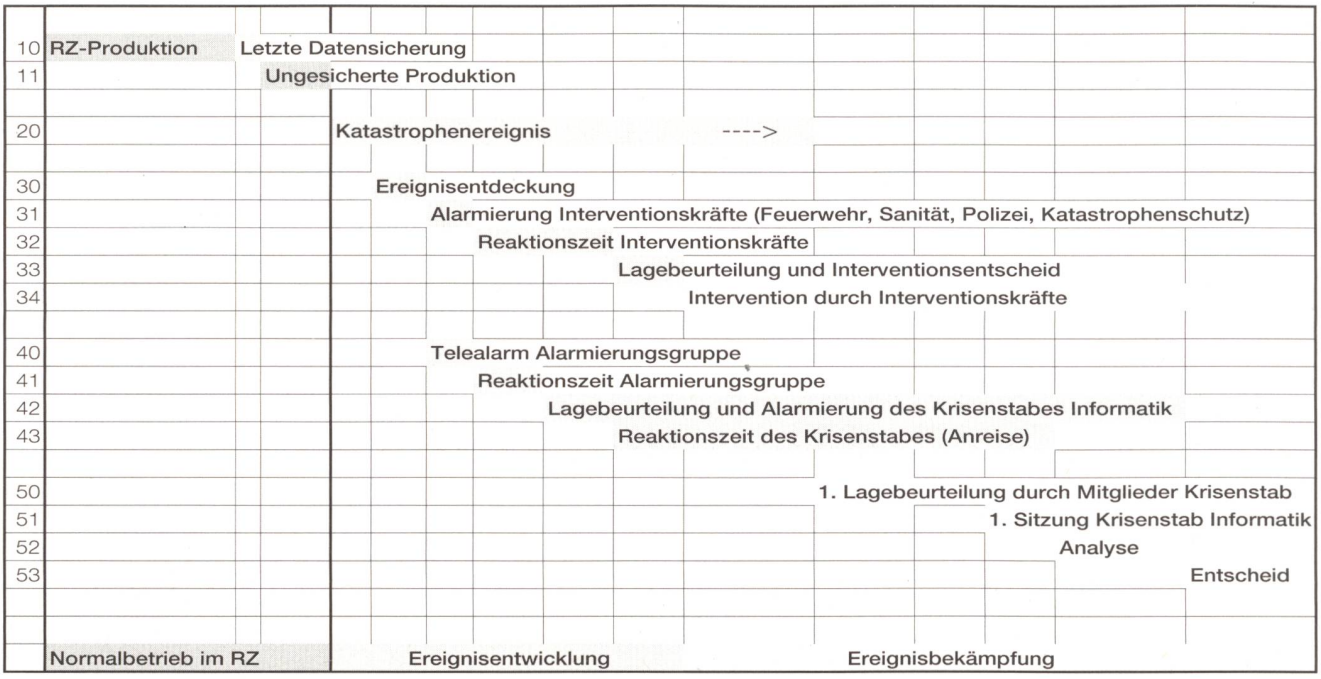


Bild 1 Phasen und Ablauf der Katastrophenbewältigung

Ausschnitt A: Alarmierung und Interventionsplan (siehe oben)
Ausschnitt B: Umbau des Notfallplans und Wiederaufbau der Informatik (folgt im zweiten Teil)
Bemerkung: Das Diagramm von Bild 1 ist zu gross, um als Ganzes dargestellt zu werden. Es wird deshalb in zwei Ausschnitten publiziert, die dort positioniert sind, wo die entsprechenden Vorgänge im Text behandelt werden.

Meinungen, wonach auf einen vollständigen EDV-Ausfall situativ reagiert werden könne, ohne dabei Gefahr zu laufen, die Steuerung und Kontrolle der lebenswichtigen Unternehmensfunktionen zu verlieren. Insbesondere sei dies ohne aufwendige und teure Vorsorgemassnahmen möglich.

Was passiert nach Eintritt eines Katastrophenfalls?

Die Problematik eines Katastropheneintritts liegt einerseits darin, dass diese meist völlig unerwartet erfolgt, und anderseits die Entwicklung des Ereignisses schlecht vorausgesagt werden kann. Aus diesem Grunde ist bei fehlender Interventionsplanung damit zu rechnen, dass ein erhebliches Chaos entsteht, nicht situationsgerecht reagiert wird und deshalb die erforderlichen Massnahmen nicht zeitgerecht eingeleitet werden können. Um ein solches Chaos zu vermeiden und die unmittelbaren Schäden sowie die längerfristigen Konsequenzen möglichst gering zu halten, ist als primäre Komponente eines Notfallkonzepts ein Alarmierungs- und Interventionsplan bereitzuhalten.

Bild 1 gibt einen Gesamtüberblick über die Phasen und den zeitlichen Ablauf vor Eintritt des Katastrophenereignisses bis zum Abschluss der Intervention. Dargestellt ist bewusst der schwierigere Fall eines Ereignisablaufs ausserhalb der Arbeitszeit. Während der Arbeitszeit erfolgt die Alarmierung zuerst intern, gefolgt von einer Rekognoszierung und Lagebeurteilung, danach die Alarmierung der externen Interventionskräfte und parallel dazu die Evakuierung des Personals. Im Prinzip laufen die Phasen wie in Tabelle III ab.

Was braucht es, um einen Informatik-Katastrophenfall zu bewältigen?

Diese Frage kann in keinem Unternehmen aus dem Stegreif beantwortet werden! Nur wenn man im Unternehmen das Risikopotential und die Verfügbarkeitsanforderungen an die Informatik (in zeitlicher, qualitativer und quantitativer Hinsicht) genau kennt, kann man festlegen, ob und welche Notfallmassnahmen notwendig sind, um einen Informatik-Katastrophenfall zu bewältigen und somit die generelle Zielsetzung sicherzustellen. Diese essentiellen Festlegungen können und sollten nicht einfach «aus den Fingern gesogen» oder «aus der Wundertüte organisatorischer Tricks gezaubert» werden, sondern müssen systematisch analysiert und mit der gebotenen Sorgfalt getroffen werden. Mit anderen Worten: Es braucht dazu ein Informatik-Notfallplanungsprojekt. Wie dieses aussehen könnte, wird im Teil 2 dieses Beitrags dargelegt werden.

(Teil 2 folgt in Bulletin Nr. 9/96)

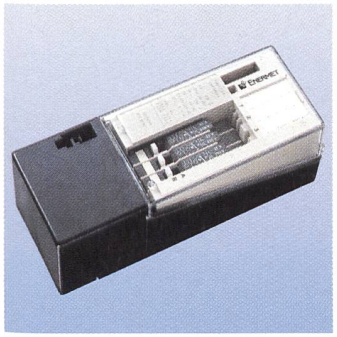
Le concept d'urgence informatique en tant qu'élément de la planification d'urgence

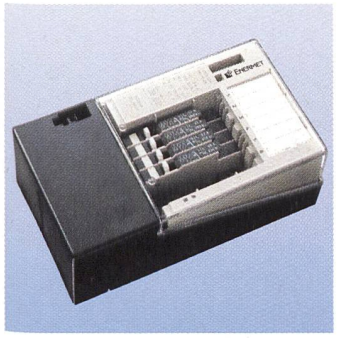
La dépendance des entreprises à l'égard de l'informatique a pris des proportions inquiétantes. Si ce service est défaillant par suite d'un dommage ou même d'une catastrophe plus grave, l'exploitation est bloquée durant un temps prolongé et, peut-être, rien ne va plus. Cela peut mener à la faillite. La planification d'urgence informatique permet de parer à ce risque et d'élaborer un ensemble de mesures rapidement efficaces, afin que l'entreprise conserve en tout temps ses services informatiques vitaux. La seconde partie de cet article paraîtra dans le numéro 9/96.

Energie, wo man sie braucht.

Wir nutzen die Reserven Ihrer Energieversorgung:

Enermet Rundsteuersysteme – seit 50 Jahren erfolgreich.





50 Jahre Erfahrung / 50 years experience

Als reines Schweizer Produkt haben unsere Rundsteuersysteme und -empfänger einen hohen Qualitätsstandard und zeichnen sich durch Langlebigkeit und geringe Störanfälligkeit aus. Die wesentlichsten Eigenschaften unserer System-Lösungen sind:

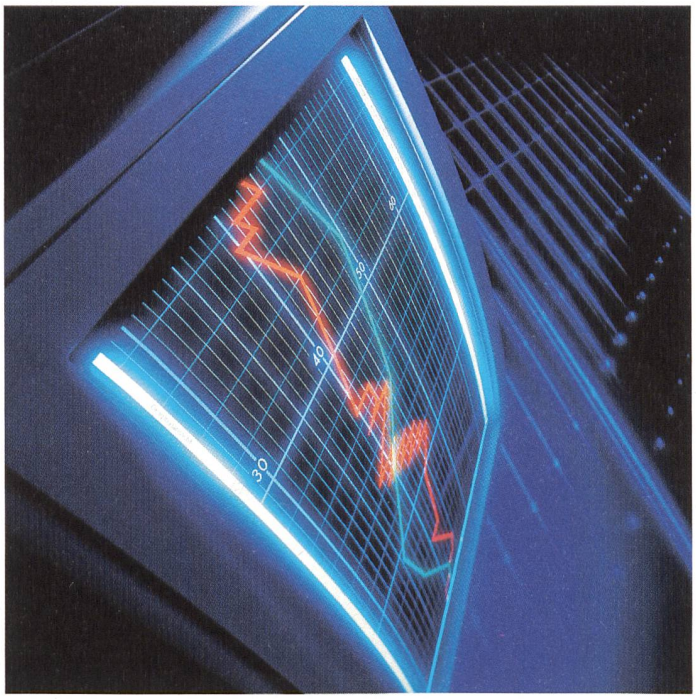
«Extrem benutzerfreundlich, Verwendung neuester Technologien!»

Unsere Kommandogeräte sind äusserst einfach zu bedienen und mit Hilfe des integrierten, adaptiven Lastreglers werden Leistungsspitzen automatisch reduziert.

Bei den Sendeanlagen gelangen modernste Technologien wie IGBT-Transistoren, GPS-Synchronisation, sowie verlustarme Ankopplungselemente zur Anwendung.

Lassen Sie sich von unseren Produkten, unserer Beratung und dem leistungsstarken Service rund um die Uhr überzeugen.

«Wir sind immer in Ihrer Nähe.»



ENERMET

ENERMET AG ■ UNDERMÜLISTRASSE 28 ■ CH-8320 FEHRALTORF
TELEFON 01/954 81 11 ■ FAX 01/954 82 01