Ingenieurbüro Kaufmann

Christof Kaufmann

Diplom-Ingenieur	**Graduate Engineer**
Maschinenbau	**Mechanical Engineering**

kaufmann@ibkaufmann.com

IT Memo

In most situations **in the company** (access to files, calculations, emails, other documents, accounting systems, DMS, CMS, ERP, SAP-use, etc.) there is a client-server structure. This term does not include, for example, special workstations for software development, hardware-related programming workstations, CAD/CAM solutions, machine and system controls and the like, although with the latter the question is whether the manufacturer has already provided the programming workstation appropriately which might be mandatory for the machine. But in principle it is also possible here to develop a machine control program on the PC and then load it onto the machine. This is particularly the case with simulation programs for controls.

Even today, **operating systems for computers** do not generally come from Microsoft, but very often and there are reasons for that: Apple never really designed its systems for use in networks. For example, there are no Apple servers. The situation is similar with LINUX as a UNIX derivative. Although both products can be made “network compatible” through certain measures, both as servers and as clients, this is more to be understood as an emergency aid in individual cases. This is not a solution in the true sense for professional use in a company. There is no experience with solutions such as SUN Workstation from USA. These are completely separate systems for specific tasks.

Server operating systems today come mainly from **Microsoft** and (generally a little less well known) still from **IBM**.

Microsoft Upgrades for Servers: Microsoft has also developed the bad habit of releasing new operating system versions at ever shorter intervals for servers as well, which forces contract customers in particular to have to renew practically the entire server landscape at ever shorter intervals. This is made more difficult by the fact that an easy-to-use general version-upgrade is usually not available, although this is formally claimed. If you run it, you will find that you have an empty machine that has been reset to an initial state, which does not correspond to the expected meaning. In addition, not every new version released is a win! The Server 2008R2 operating system was a good and stable platform, this also applies to Server 2019. The versions in between (Server 2012 and Server 2016) had some weaknesses and must be viewed as immature. Basically, these were development versions on the way to Server 2019, but they were sold early.

Microsoft Updates for Servers: With the flood of updates released, the problem is that these updates can be downloaded automatically, but are not installed automatically. This setting does not exist; manual intervention is required. In addition, a restart is usually necessary, but this often results in utilities not starting, even though they are set to start automatically. The reason for this is that when the server starts after the update, it still has a good portion of the update to process and simply “forgets” that a few services still need to be started. Manual intervention must also be carried out here. For small networks with 10 servers the problem is small. In large networks with >100 servers, the problem is uncomfortably large. There is a network-wide Update Deployment to assist, but that's not much help, because the updates to the target machines are then deployed but still not installed and the problem with services possibly not starting remains.

A customer whose basic machines in the server landscape still have older operating systems such as Server 2003 or Server 2008R2 and only uses a Server 2019 where it is really needed for functional reasons does not have these problems. For example, it is completely unnecessary to replace a domain controller based on Server 2008R2 with a Server 2019 just because Microsoft would like it that way. The concept of necessity must also be questioned otherwise: in principle, Microsoft is not officially backwards compatible. However, the experiment shows in many cases that, for example, programs that were developed for Server 2008R2 (e.g. Microsoft Office 2010) also run perfectly on Server 2019 and, conversely, a program that, according to the manufacturer, is released “from Server 2019 upwards” runs without any problems on Server 2008R2. But it can actually happen that software that ran on 2008R2 has to be reprogrammed under Server 2019 because Microsoft has changed too much. Which of course has a certain intention.

First of all, **Microsoft networks** are relatively easy to manage as long as it is a LAN with fewer than 254 units (computers, printers, etc.), which can be represented with a “single-tier” IP4 network. If there are more than 254 units, the network must be segmented and transfers and forwardings are defined. Microsoft networks work relatively unproblematically with up to 500 simultaneous logins. In addition, for example in an airline with 5,000 simultaneous logins, difficulties arise that require special measures.

Cloud and servers in the cloud are a fad that appeals primarily with seemingly cheap prices. As expected, they should of course fill the providers' coffers. If you take a closer look, you will notice: the customer's administrator cannot manage these servers without restrictions, there are unsupported features in connection with any own software and the customer cannot connect these servers to be a network. As a result, even a smaller company that perhaps only needs 5 servers simply doesn't get anywhere with it. Apart from that, the company data is outside the company = security aspect. It is something different to store backups in a cloud. Since a “cloud” is nothing more than a sales term for a webdav-supported SSL remote drive, the customer can just as easily do this with their own resources. He doesn't need a provider for this.

Virtualization of servers (and also workstations) is already very beneficial for today's customers, especially in terms of cost savings: 15 Microsoft servers (or other) can easily run as "virtual machines" on a single hardware platform equipped with 350 GB of RAM. (“VMs”). Shortly after year 2000, virtualization technology was first developed by Vmware, mainly as a test scenario for operating system development. With the HyperV product, Microsoft has – as so often – followed. Both products are mature and recommended. When it comes to the RAM requirements of a single VM, younger administrators in particular tend to greatly exaggerate, which then leads to an apparent RAM shortage. Experienced people start with a small value, then look at the machine in operation and adjust it so that the RAM reported as free during operation corresponds to approx. 40% of the allocated RAM. That's completely enough. And so you then realize that, for example, instead of 64 GB of RAM, 8 or 10 GB are completely sufficient.

IT security is a very complex and extensive topic, which can therefore only be partially addressed here. And it is the case that the needs due to possible threats in a small private business must be assessed very differently than in banking and stock exchanges or in the area of large companies or critical infrastructure (power plants, control centers, armaments, military, police and rescue services). A basic distinction is made between the danger from outside and the danger from within, although the latter can also simply include the ignorance or gunfire of employees. Basically: a network that cannot be seen from the outside cannot be attacked from the outside! In IT, a distinction is made between the “good” and “bad” sides. While the good administrator is responsible for the good side, i.e. for the functioning of the network and the infrastructure as a whole and is an expert for this, the “bad IT person” is an expert for the other side: he has researched the techniques of intrusion, reading, stealing or destroying and is an expert there. A customer is well advised if his capable system administrator contacts an expert on the evil side, such as the Hamburg Computer Chaos Club in Germany, and has his system checked from outside. Of course, in practice, carelessly opened emails are the most common cause of threats and actual damage, but there are also documented attacks that occur via a vulnerability in the driver program for a hard drive controller. Such a danger can only be discovered by a specialist. (if at all! But thank God the latter hurdle also applies to the attacker!)

Remote access to the company network via VPN has established itself as an overall secure solution. Establishing a VPN connection with an encryption depth of 1024 bits can still be considered sufficiently secure against attacks in most cases. But of course more is always the better. We would recommend a solution that only allows connections between defined hardware, for example the company's firewall, and certain computers. The always unique MAC address of the accessing computer is used for identification. This avoids man-in-the-middle scenarios.

VPN for international connections is something different and runs through providers with their own server network in the relevant country. For frequently traveling business people, journalists and simple tourists, in some countries it is only possible to establish a connection to their home country using such provider-supported VPN connections. One can argue about the sense, nonsense and, above all, the justification for restrictions that are usually imposed by the state. Or you can simply solve the problem. Even a German traveler cannot enjoy the German sports show abroad as a public offer from the German ARD without such a VPN. Logging into (email) accounts abroad without such a VPN can also be difficult or pose a security problem.

Microsoft RDP protocol for terminal server sessions was previously considered secure because it includes its own encryption. However, this information is now obsolete. The encryption key is too weak and the RDP protocol has too many holes due to its functionality that can be used to attack the target machine. The RDP protocol, which is extremely practical for work, should only be used for purposes within a LAN. There, however, it provides excellent services: even in networks with many employees, it replaces the work of carrying out installation measures on all workstation computers individually. The administrator can limit himself to maintaining the terminal servers. The mapping of the local printer usually works without driver installations. For the need for several hundred simultaneous RDP sessions, Mi-

crosoft has so-called RDP farming, which load balances between several terminal servers in order to avoid performance drops on individual servers. Today, a terminal server is nothing more than a normal server on which the so-called RDP services are activated by licensing a certain number of sessions. Powerful applications such as CAD or video production, especially with strong graphics requirements, will still be run on an appropriately equipped physikal workstation and not in a terminal server session. There are also suitable RDP clients for MAC computers from Apple to access a Microsoft terminal server.

Firewall is a term that is used in different meanings. On the one hand, there is the **computer firewall**, with which the computer/server protects itself and applies rules for incoming and outgoing traffic. Much more important is the **network firewall**, which is located between the external network / WAN = Internet = Danger (Red) and the internal network / LAN / (Green) and something in between called DMZ = Demilitarized Zone (Yellow) and, depending on the equipment, others network segments. A good network firewall allows all data traffic to be monitored and controlled. Rules determine which requests from one of the segments are forwarded where to, if at all. It issues the certificates necessary for VPN access. One can establish a direct network-to-network connection with other firewalls of the same design. It can also act as a DHCP server and assign dynamic IP addresses. Satisfactorily good firewalls are already available as free software versions. You can definitely buy a very good hardware-based device from a well-known manufacturer for 5,000 Euros.

IP4 and IP6 addresses: While clearly recognizable IP4 addresses based on the pattern 192.168.020.001 are particularly useful for internal use on the company LAN, an IP6 address based on the pattern such as 2dfc:0:0:0:0217:cbff:fe8c:0. proves to be illegible and therefore extremely difficult to use in practice, especially since 100 computers in a network each appear completely different and do not follow any recognizable pattern. The argument for the introduction of IP6 lies in the explosion in the number of necessary IP addresses in the public internet space, caused in particular by cell phones and tablets. Regarding the status quo, however, it should be noted that the IP6 standard has not become established and a quick change is not expected. The main aim of the IP6 standard is to make the computer unique worldwide (similar to the MAC address) and thus always offer both authorities and hostile attackers find a clearly defined target. We consistently simply switch things off like that.

Network speeds have been a big issue since optic fiber (LWL) cables emerged and Fiber To The Home (FTTH) became a buzzword. In order to be able to evaluate this, one first needs to know the following: in the optimal range of short cable routes up to 250m, i.e. in the company LAN, there were jumps from 10 Mbit/s to 100 Mbit/s and then to 1 GBit/s = 1,000 Mbit/s, so according to the numbers, an increase by a factor of 10 each time seems to occure. Real measurements with the stopwatch when transmitting defined data packets did not show a factor of 10 in both cases, but a factor of aprox. 2.5 as a real increase in speed. So if there is a 10 Mbit/s line with copper cable at a location, you should keep your expectations within limits if a provider offers “fast optic fiber” but limits its offer to 100 Mbit/s in the Ts & Cs, but demands five times the price. And a stable 10 Mbit/s line is ultimately worth more than a shaky 100 Mbit/s line with dropouts. Fiber optic cables cannot easily be intercepted on the go using magnetic sensors. Those belonging to the area of critical infrastructure need their own cables anyway. Fiber optic cables can easily reach 1,000 Mbit/s and more. But the data stream also has to be processed or received and at this point in particular it is often observed that the speed of large transfers drops after a few seconds when buffers run full.

SAP is a company that has the reputation of “once SAP, always SAP” and also represents the business strategy that the SAP product does not have to adapt to the customer's processes; rather, the customer has to adapt their processes to SAP. First, the customer receives an offer for a system. What he is not told is that he needs the same system again for the development steps and the subsequent testing, and as a result he pays three times the price. At least that was the case in the past. There were 10 million Euro projects that were reversed because SAP was ultimately unable to meet the customer's requirements. The reason for this can be found in the structure of how SAP develops customer projects. The parent company delivers 3 basic modules, while so-called SAP consultants - which are software houses that specialize in individual modules - deliver the modules that the customer actually needs. If the customer now needs the three basic modules from the parent company and two additional special modules from two different software houses, there is no guarantee that the whole thing will run together - since it comes from three different sources. And SAP itself has a problem releasing updates for its three basic modules because it is not certain whether these will run smoothly together with the modules from the software houses. Research shows that IT costs tripled after implementing SAP. At least some time ago, SAP began, not publicly but in the background, to convert its products from PC-based Microsoft servers to IBM's AS00 / iSeries platform. In this way you would also get rid of the update problem quite elegantly. Smart !

IBM AS400 / iSeries is a solution from the area of so-called medium data technology that was developed a long time ago (60s) and was originally intended for use together with hundreds of simple terminals that were connected to the machine via simple telephone wires. The hallmark of these machines has always been absolute stability and this remains the case to this day. All processes run on the ma-

chine itself; access is now via Windows clients instead of terminals. It is a modular system, the smallest version of which is a simple 19" 3U slot, but in a powerful version it fills an entire room. IBM has continued to develop this series and the basic equipment of the IBM operating system release really offers everything the heart desires, including modern features. The basic equipment includes the IBM database DB2, which, according to current rankings, still is one of the fastest databases in the world along with ORACLE. When fully expanded, the machine can manage 8 TB of RAM (!!). PC-based machines with a maximum of a few hundred GB cannot keep up with this. There are no updates (so no reboots are required) , no viruses or malware for the AS00. IBM guarantees 100% backwards compatibility when a new machine comes out with a new operating system release. Large globally active companies such as TUI or airlines use the AS00 with their login requirements. The only “disadvantage” of this system is that, like any other system, you have to write and maintain programs for it.

Databases come from **ORACLE** or **IBM** for large needs, depending on the hardware platform PC or AS400, for small to medium needs from **Microsoft** as Microsoft SQL Server or for free, very small areas as **MySQL**, popular as an internet database. Systems available today under names such as ERP, CMS or DMS systems or accounting/financial systems are **database applications as a frontend** that access a specially designed **database structure in the backend**, i.e. running on the server.

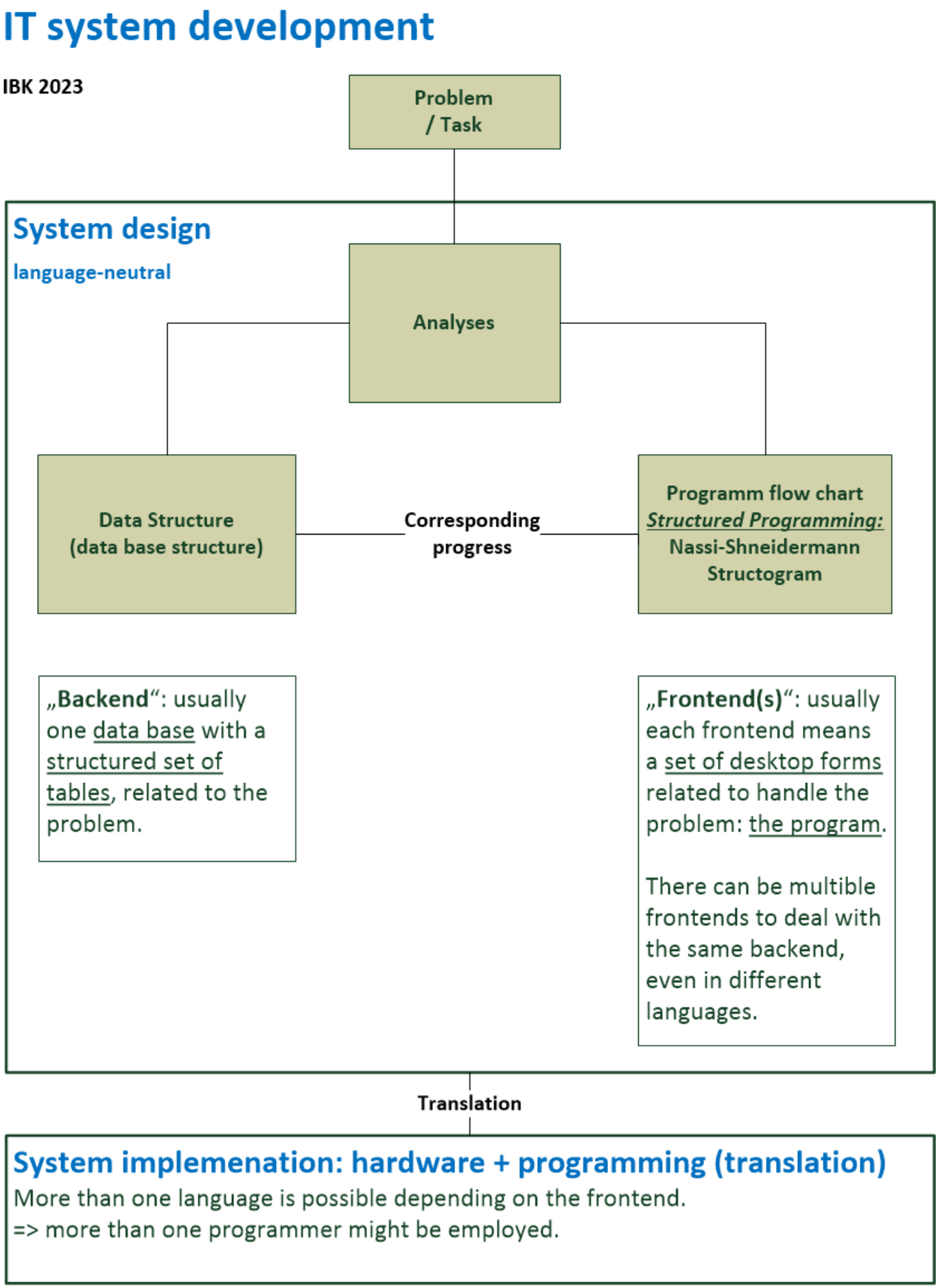
Hardware-related programming, such as that required for **machine controls** and **simulation programs**, is a completely separate topic. The most important thing here is speed: the program must always be faster than the machine can run and the simulation

must take mass inertia into account. Unless the hardware supplier has already provided specifications, the hardware-related programming language **ASSEMBLER** is preferred at this point.

Software development: Every sensible programming follows the methodology of the generally valid structogram developed by **Nassi-Shneidermann** to represent the so-called structured programming: individual modules are recorded in the plan, each of which is run through from top to bottom and always has a defined, stable end state generated. This representation is programming language-neutral and therefore generally valid. It can then be translated into any language. It is certainly possible to implement individual modules in different languages. Approaches known under names such as ***Scrum*** or ***Agile Programming*** are more likely to be understood as teaching methods in order to do exactly what has been described above. In other words: anyone who has really internalized Nassi-Shneidermann and thinks like that no longer has any additional advantages from Scrum etc.

Software with direct access: The Internet is to be understood as a network through which a database can be accessed, for example, just like in a LAN. With our developments, we have shown that it is possible to write lean, fast software without relying on a security-vulnerable WEB browser, which allows a computer from any location to work on the company system without any “third-party resources” in between. Of course tap-proof.

System development in IT: the following image shows the basic procedure for developing an IT system that is supposed to fulfill certain tasks.



The not uncritical idea of SCRUM is to divide the first step of system design for larger projects into a group of several people moderated by a *Scrum Master*.