AUBE '01

12TH INTERNATIONAL CONFERENCE ON AUTOMATIC FIRE DETECTION

March 25 - 28, 2001
National Institute Of Standards and Technology
Gaithersburg, Maryland U.S.A.

PROCEEDINGS

Editors: Kellie Beall, William Grosshandler and Heinz Luck

NIST
National Institute of Standards and Technology
Technology Administration, U.S. Department of Commerce

Georg Schmitz, Dr. Peter Witschital
Siemens Gebäudesicherheit GmbH & Co. OHG, Munich, Germany

Internet Technology: New Perspectives for Alarm Systems

Internet technology is making rapid progress with a high pace of innovation and very short innovation cycles. Today, an ‚internet year' is to be considered less than 90 days[1]. Prices of standard hardware and software components are dropping constantly and fast. This is the reason why it becomes more and more attractive to benefit from this technological progress and to make use of standard Internet technology for products and applications which had to rely on ‚traditional' branch-specific technological solutions by now.

1. Learning from other business segments

A good example is the telecommunications industry. Communication systems based on traditional switching technology are now facing strong competition by new systems using new standardized protocols like Voice-over-IP (e.g., the ITU H.323 standard defines how to send voice packages via the Internet using the Internet Protocol (IP)) and Internet technology in general. The new systems reduce infrastructure costs by using the same technology for voice and data communication.

Furthermore they take advantage from Internet technology's steep innovation curve and resulting price/performance advantages. For example, Fast Ethernet boards declined in price by as much as 50 percent in the past year, while the price of legacy PBXs (private branch exchanges) declined by only 7 percent approximately (according to Cisco Systems Inc.; Internet Communications Software Group – Driving the Market for Converged Applications and Services (White Paper); July 2000).

As a consequence, established manufacturers of communication systems lost market share to new manufacturers coming from the IT business segment.

[1] In fact various numbers are mentioned with respect to how long an 'internet year' is. However, the innovation cycles are very short in any case.

2. What does this mean for building automation and alarm systems?

The crude fact is: There is a challenge coming from IT business and if we do not face it, we will get in trouble. But let's look at it positively: It's not merely a challenge, it offers new chances. Internet technology opens new perspectives not only for building automation (HVAC) systems but for alarm systems with higher demand on reliability as well.

There are mainly two aspects of using Internet technology for alarm systems: Internet technology for system communication and Internet technology for providing new services.

3. Internet technology for system communication

First, the technology can be used for internal communication between system components. This will become attractive for two reasons. On the one hand, the cost of Internet technology hardware components will drop dramatically because of mass scale production, e.g., a processor chip with an Internet Protocol stack on board will probably cost less than five dollars in the near future. On the other hand, standard software implementations of all the relevant protocols are available on the market and, furthermore, numerous software packages are offered, based on the Internet Protocol suite and implementing interesting services of all kinds, e.g. encryption, authentication etc. There is no need to make this software, one can buy it off-the-shelf instead, saving lots of development effort.

In order to understand the situation properly it will help to have a look at the OSI 7-layer communication model (see Table 1).

If two devices want to communicate with each other a common protocol is needed in order to make sure that they understand each other, i.e. 'they have to speak the same language'. The messages to be exchanged have usually application specific content and the protocol to be used is a protocol belonging to the application layer of the layered OSI communication model. In order to transport the message from one device to the other, services provided by lower level protocols are used.

	Layer	Function of the layer
7	Application Layer	User level applications (e.g. WWW (HTTP), FileTransfer (FTP))
6	Presentation Layer	Adaptation of formats (empty for Internet technology)
5	Session Layer	Synchronization, administration (almost empty for Internet technology)
4	Transport Layer	Peer-to-peer communication (e.g. TCP (Transport Control Protocol), UDP (Universal Datagram Protocol))
3	Network Layer	Routing and switching (e.g. IP (Internet Protocol))
2	Data Link Layer	Access method to the physical media (e.g. Ethernet, Token Ring)
1	Physical Layer	Physical media and transport of bits (e.g. Coax, Twisted Pair)

Table 1: OSI 7-layer communication model

What does it mean if we say we want to use Internet technology for system communication? First of all, it means that the Internet Protocol (IP, Layer 3) and probably TCP or UDP (Layer 4) shall be used. This decision allows us to use a lot of software components based on TCP/IP or UDP/IP available off-the-shelf on the market, as it was already described above.

3.1 TCP/IP is not enough

However, this decision alone does not guarantee that two devices understand each other. Therefore, a common protocol on the application layer is needed. There are many possibilities to choose from. As there is the general tendency away from proprietary protocols to open standardized protocols (for obvious reasons), BACnet is one of the candidates for the common language among the devices. A little bit deviating from the OSI model, BACnet defines its own network layer protocol and uses UDP/IP as one of its possible data link layers.

When a common application layer protocol has been found, the other open question is what to use below IP as data link and physical layer. In order to profit as much as

possible from widespread technology, Ethernet is the best choice. Ethernet is an established, worldwide standard supported by IEEE and ISO. It has been broadly used in office environments and is penetrating the industrial environment as well. The high number of users ensures the downward price of its components. The long-term exposure to Ethernet technology has produced an expansive knowledge base and unparalleled resources. However, for industrial usage Ethernet has some drawbacks which are sedulously stressed by its critics. But these drawbacks can be avoided or overcome today.

3.2 Ethernet and real-time behavior

Ethernet as used in an office environment uses a media access method known as CSMA/CD (carrier sense multiple access with collision detection) that cannot guarantee a deterministic behavior of the network. This can be overcome by using an appropriate network topology with so-called Switched Ethernet technology. The switches make sure that every device connected to the network can operate full-duplex with a guaranteed bandwidth. Thus, the network supports real-time communication with guaranteed response times. In addition, there are several options how to assign priority levels to messages. The fact, that it is possible to build networks with guaranteed response times based on Ethernet technology has been proved many times in industrial automation applications today. One should keep in mind that the requirements with regard to real-time behavior are usually much higher in industrial automation than in alarm systems. Furthermore, it is for sure that the real-time behavior of the Internet (including Ethernet technology) will be further improved because there is high demand for transporting real-time video information via the Internet.

The bandwidth of standard Ethernet is 10 Mbit/s which is quite high compared with other bus systems used for alarm systems today. If that should not be enough, Fast Ethernet is available today with a bandwidth of 100 Mbit/s and Gigabit Ethernet (1 Gigabit/s) is emerging. The IEEE standardization group has even started work to define 10 Gigabit/s Ethernet.

3.3 Ethernet and reliability

Reliability is not only an issue for alarm systems but for industrial automation as well. It is not acceptable that single faults may cause a complete stand-still of a production line easily resulting in million dollar losses. For that reason the issue of making an Ethernet-based control network reliable has also been solved already in industrial automation. There are several solutions for making an industrial Ethernet redundant and fault-tolerant, some of them can even cope with double faults in the system.

More and more often customers ask whether it is possible that existing company-owned TCP/IP network infra-structure can be used for the alarm system as well, in order to save efforts for installation of a separate network. The answer is: yes and no.

As mentioned before, a standard office LAN (local area network) based on Ethernet is not suited for time-critical applications. The network topology would have to be adjusted. For several reasons, it may be the better solution to install a separate security network for safety-critical and time-critical applications which may be connected to the office network via a TCP/IP-Gateway (the terms router or bridge may also be used, although all of them have different functions). The big advantage of using Internet technology for both the security network and the office network is that information which is not time-critical can easily travel across the border between the sub-networks. From a PC in the office network it is then possible to get always up-to-date information about the status of the alarm system. In automation technology this concept is know as the sensor-to-boardroom integration. All plant devices act as servers providing information to anyone anywhere.

3.4 Ethernet and robustness

Some critics of Ethernet for industrial use argue that the connectors (in an office environment cheap RJ45 connectors are used) are not suited for an industrial environment. But this problem has been solved already, too. Several alternative Ethernet connectors are available for rugged environments.

3.5 Internet technology has an influence on the system architecture

As prices drop, the level on which Internet technology can be used profitably drops. While Ethernet and IP communication is used on the management system level (management layer) already today, it starts to be profitable on the control panel level (control layer) now. Even some IP-based sensors are available today, but currently this not yet profitable for low-cost sensors. However, we see no reason why Internet technology should not move down to the sensor level (device layer) in some years time.

Using Internet technology will of course also have an impact on the overall system architecture of an alarm system. Today a simple alarm system installation usually consists of a control panel with hundreds or even thousands of sensors connected to it. If you think of a multi-functional alarm system for fire detection, intrusion detection, and maybe access control, it is necessary to install lots of cables in the building for the different sensors to be connected with the control panel(s). From our point of view an architecture for a new system that makes use of Internet technology would be a more decentralized architecture with the sensors connected to smaller system units spread over the building and connected via Internet technology. This could probably help to reduce installation and maintenance costs of the system.

The progress in wireless technology may be another influence on future system architecture. Again, using Internet technology has the advantage that e.g. Wireless LAN technology or next generation mobile communication technology, like UMTS (Universal Mobile Telecommunication System), can easily be integrated into the future alarm system architecture because it is for sure that these new technologies will support the transport of IP packages and Internet technology in general.

4. Internet technology for providing new services

Besides system communication, the other important aspect of Internet technology is the provision of opportunities to add value for the customer by offering really new services. In the following, we can just try to give a few examples.

4.1 Remote control and remote service via web technology

First of all, web technology (using the standardized application layer protocol HTTP (HyperText Transfer Protocol)) allows to access the alarm system anytime from anywhere. Of course, access shall be restricted to authorized personnel. No problem, just take an authentication software package, perhaps some encryption package or what ever you need off the Internet technology shelf. In the alarm system an embedded web server is needed. Again, hard- and software are available on the market in various sizes at various prices. On the client side the big advantage is that every device supporting standard web browser technology can be used for access, whether a PC, a PDA (Personal Digital Assistant), a wireless 'web pad' or – soon – a UMTS mobile phone.

Remote Access by web technology enables you to offer remote control and remote services to your customers, perhaps the service being your USP (unique selling point) giving you an advantage over your competitor. For your service organization remote access offers a huge cost reduction potential. Of course, remote service can also be implemented without web technology. But with web technology you can buy most of the components needed on the market and there is no need to implement and maintain a proprietary solution.

By using Internet technology it is also quite easy to integrate audio- and video-information into an alarm system. There are standards, e.g. the H.323 standard we already mentioned before, which define how to transmit multimedia information over IP-based networks. Not to forget the messaging services which come for free with Internet technology, like Electronic Mail. Alarm or system fault messages can be forwarded by E-Mail, Fax or SMS (Short Message Service for sending and receiving short test messages with a mobile phone). All this offers many opportunities how to offer added value to the customers.

4.2 Software download and application service providing

Another simple application layer protocol is FTP, the File Transfer Protocol. Based on this protocol, it will easily be possible to download software or data from remote into the system in order to update the system software. If the alarm system is connected with

the Internet (whether the public Internet or a VPN (Virtual Private Network) of the system vendor or any service provider) it becomes possible to offer services to the customer which do not have to be installed on the alarm system. Instead, they are located on a so-called application server owned by the alarm system vendor or a service provider. Such ASPs (application server providers) are just emerging rapidly in the office world. An ASP offers software which can be used via the Internet, but does not have to be installed on the customers computer. The customer can choose to pay a monthly flat-rate for the license to use the software or to pay per use. For an alarm system the customer may want to run a diagnostic program from time to time providing some information about the status of the sensors and detectors. Because he runs the program only if needed, he may prefer to run it from the application server and to pay for it by use. An alarm system installer may prefer not to install a planning and provisioning tool on his own computer but to use the tool from the application server, where he always gets the most recent version supporting all new system features. For the system vendor or service provider it is much more convenient to update the version of the application program on his own application server than to update hundreds of application programs which are installed on the systems of the customers.

4.3 New possibilities for improved risk calculation and priority analysis

Due to the closer integration of the alarm system's control network with the office network and the transparency between those networks it will be much easier than before to combine information related to the alarm system with information available from the customer's office network. In case of fire alarm, for example, information about the material stored in a warehouse could be taken into account, in order to perform a more detailed risk calculation and priority analysis. This information could help in the decision whether a building has to be evacuated immediately, or in the decision about the best strategy for fire fighting.

Of course, it would be great if the fire fighters could get more detailed information about the situation on-site, before they arrive there. Our vision is, that the fire fighters have access to detailed information from the alarm system via a mobile Internet terminal in their trucks (e.g. using mobile Internet access via UMTS). They can get

every information they need to fight the fire effectively, whether there are specific risks, how to get most quickly to the center of the fire etc. Even transmission of life video images from the site is possible. This vision is not far away.

5. Summary

We have to be aware that if the alarm system manufacturers will not take the opportunities offered by Internet technology for offering new services to the customers, some vendors of IT technology will start to offer more and more safety and security related services. There is a clear trend from delivering only technology to delivering applications and services.

The customers, of course, like systems which are based on open standards and standardized interfaces because this helps to protect the customers' investments, to manage complexity and to reduce risks of change. The use of standard hardware and software components and the new system architecture of multifunctional integrated alarm systems supported by Internet technology will significantly reduce installation and maintenance costs of the systems.

The experiences made with using Internet technology in industrial automation have produced reliable, robust solutions with real-time behavior which are equally suited for use in alarm system applications.

Internet technology opens new perspectives for alarm system manufacturers.