

NEWS



Issue 58 | June 2007



LAN CABLES AND SECURITY ISSUES FUTURE PROOFING AGAINST EMERGING THREATS

STATISTICS

CONTENT

COVER STORY:

LAN CABLES AND SECURITY ISSUES

(pages 3-11)

I.C.F

P.O.BOX 26
Graben 30
A-1014 Wien
Austria

Phone +43-1-532 96 40

Fax +43-1-532 97 69

Web www.icf.at

Contact renate@icf.at

The ICF Newsletter is published several times each year by the **International Cablemakers Federation**.

The ICF accepts no responsibility for the accuracy or the content of materials provided by third parties as identified.

ICF NEWS

NEW MEMBER

We are very pleased to welcome Marmon Wire & Cable LLC (USA) as a new member of ICF. More information about our new member can be found at www.marmon.com

ICF CONGRESS 2007



The invitations to the Rome Congress at the Hotel St. Regis from 2 to 6 October have been sent out to all members by email and we would like to encourage you to register by 3 July. After this date we will have to release hotel rooms for which demand is not foreseen in order to avoid extra charges.

Rome, as you are well aware, is one of the most visited capitals in Europe. Hotel prices of course reflect this "attractiveness" which is the reason that we have had to increase the registration fee this year.

We are certain however that you will enjoy the Congress Business Sessions developed by the Standing Commission led by Greg Lampert, the Spouses Program and the Excursion on Friday with the highlight of a private visit to the Vatican Museums with the Sistine Chapel.

Thomas Neesen
Secretary-General

LAN CABLES AND SECURITY ISSUES

FUTURE PROOFING AGAINST EMERGING THREATS

Provided by CRU

INTRODUCTION

Higher Priority for IT Security

This review focuses on recent developments in the LAN (local area network) cable market. More widespread use of new application technologies is placing greater strain on the IT (information technology) resources of enterprises, so that pressure to upgrade existing networks increases. Security is becoming an even higher priority for IT managers. In this context, "security" refers to issues such as maintaining the integrity of a business's core operations in the event of a major incident and protecting systems against penetration by external hackers.

Overview

Firstly, this review looks at general developments in the IT sector, including the increasing importance of data centres and co-location facilities. Then it considers how these developments are affecting the market for structured wiring systems, and the impact on the competing solutions offered by different suppliers. Finally, there is a discussion of cables offering added security in a very specific way: cables that have enhanced fire survival characteristics.

TRENDS IN IT SECTOR

Recovery in IT Investment

One of the key factors that determine the level of demand for LAN cables is IT

investment activity, especially amongst medium and large business enterprises. Over the last eighteen months a variety of factors, driven ultimately by pressure to retain customers and to improve profits, have led to a resumption in IT investment amongst medium and large business enterprises. The collapse of the dot.com bubble in 2000 and 2001 had a major adverse impact on activity in the premises (datacom) sector, though the fall was not as dramatic as in telecoms. There has been recovery since then in most markets, though the pace of the improvement has been generally quite slow.

New Technologies Adopted

There is now a higher profile for technology as a means through which enterprises can attain better levels of internal productivity, generate cost savings and deliver better customer service. Thus there has been an increase in the use of technologies that have existed for several years, but which are now finding more widespread acceptance. These applications and protocols include CRM (Customer Relationship Management) systems, VoIP (Voice over Internet Protocol), Video-conferencing, Multimedia and Wireless.

Clear Benefits Needed

One clear trend in all geographic regions is that, compared to the boom in the late 1990s, there is now a much more measured approach to IT investment, with companies even keener than before to ensure that there will be a clear and tangible benefit to their operations as a result of capital expenditure. But, as with all IT related upgrades, investment in one

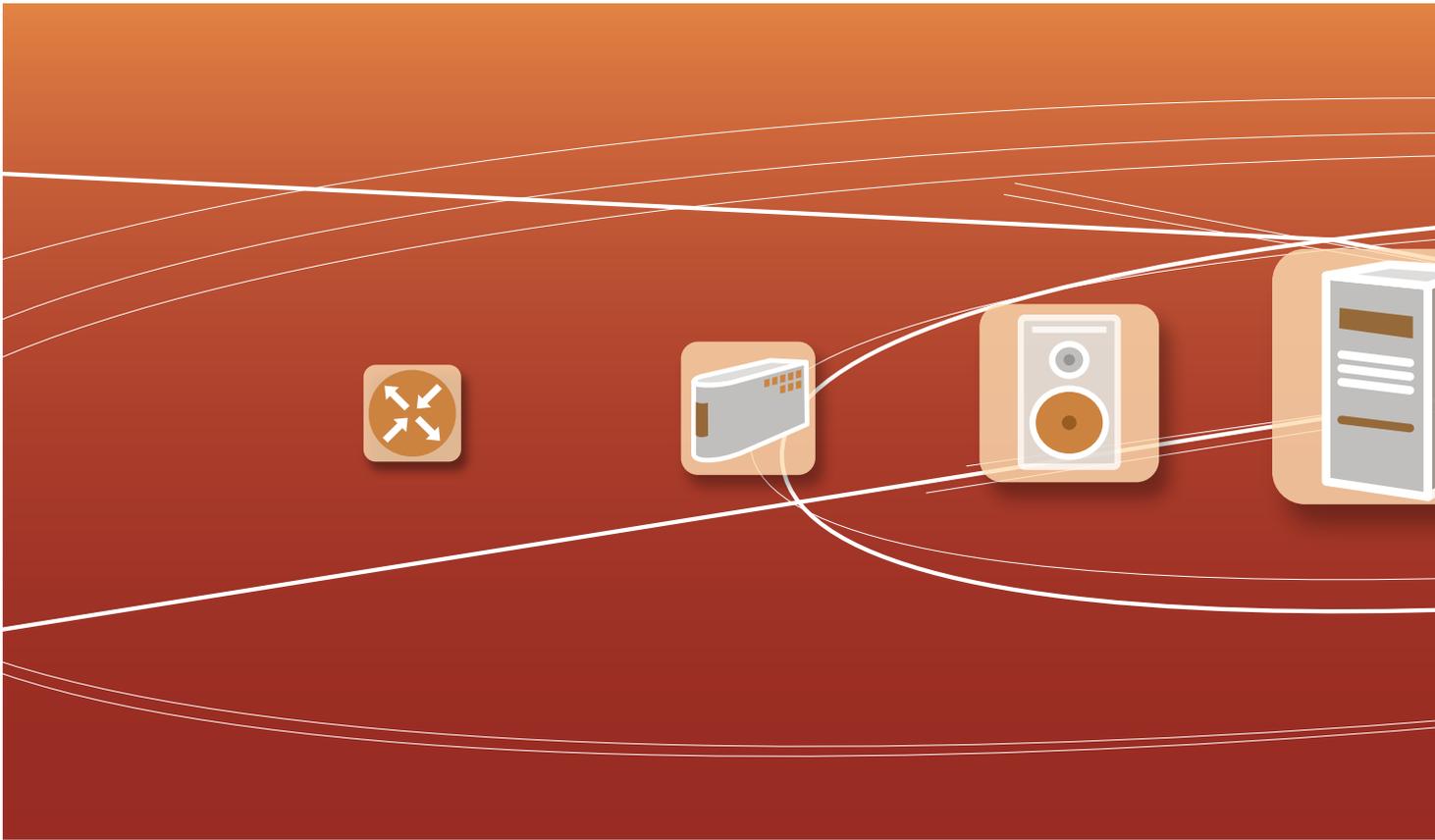
bottleneck area is likely to require subsequent upgrades in related areas, thereby further straining already tight budgets.

Trends Point To More Mobile Workers

Working practices in many countries have also been gradually changing, resulting in many more employees either working remotely from their main office location on a permanent basis, or travelling regularly across different countries, with little time spent at any one location. In moves to cut costs, it is becoming more effective to establish more but smaller branch or satellite offices, with each branch gaining more autonomy in IT terms. This means that the individual employee invariably has more applications attached to their desktop computer. It also means that the IT manager is likely to face greater complexity through having more diverse operations to service.

Online Transactions Grow

As has been frequently reported, there has been strong growth in online business, as more customers are encouraged to purchase goods and services online, reducing transaction costs. While this growth in online business may have been slower than was suggested by some of the early hype, the trend is unmistakable. For many companies the online business is additional to their established business, not a replacement for it (so adding yet more complexity for the over-stretched IT manager!), but in some cases it can mean a fundamental shift in the business model. Online transactions have affected not only businesses addressing consumer markets,



but also the business-to-business sector, as, for example, suppliers compete for contracts from their customers via on-line auctions.

Importance of Network Grows

These continuing changes in the fundamental operations of a business clearly have an impact on the business’s internal communications network. There has been a significant increase on the amount of two-way data traffic being transported between an enterprise headquarters, its sister offices and ultimately its customers. This additional volume has created pressure on the level of performance delivered by the network. This is especially true for businesses, such as call centres, that are required to operate 24 hours per day, 7 days per week. Expectations in turn have been raised over access to the network, with high speed and consistent quality of service now crucial elements. There is no tolerance for network downtime, given the potential amount of revenue lost as a direct result of even a few hours’ failure.

Network Security Vital

These moves towards greater efficiency and operational transparency within the business have also led to more confidential and sensitive information needing to be being shared over the network. This clearly has implications for network security, while incidents such as theft of laptop PCs have been increasing. Hence, at this most basic individual level, guaranteed security has arguably never been so vital.

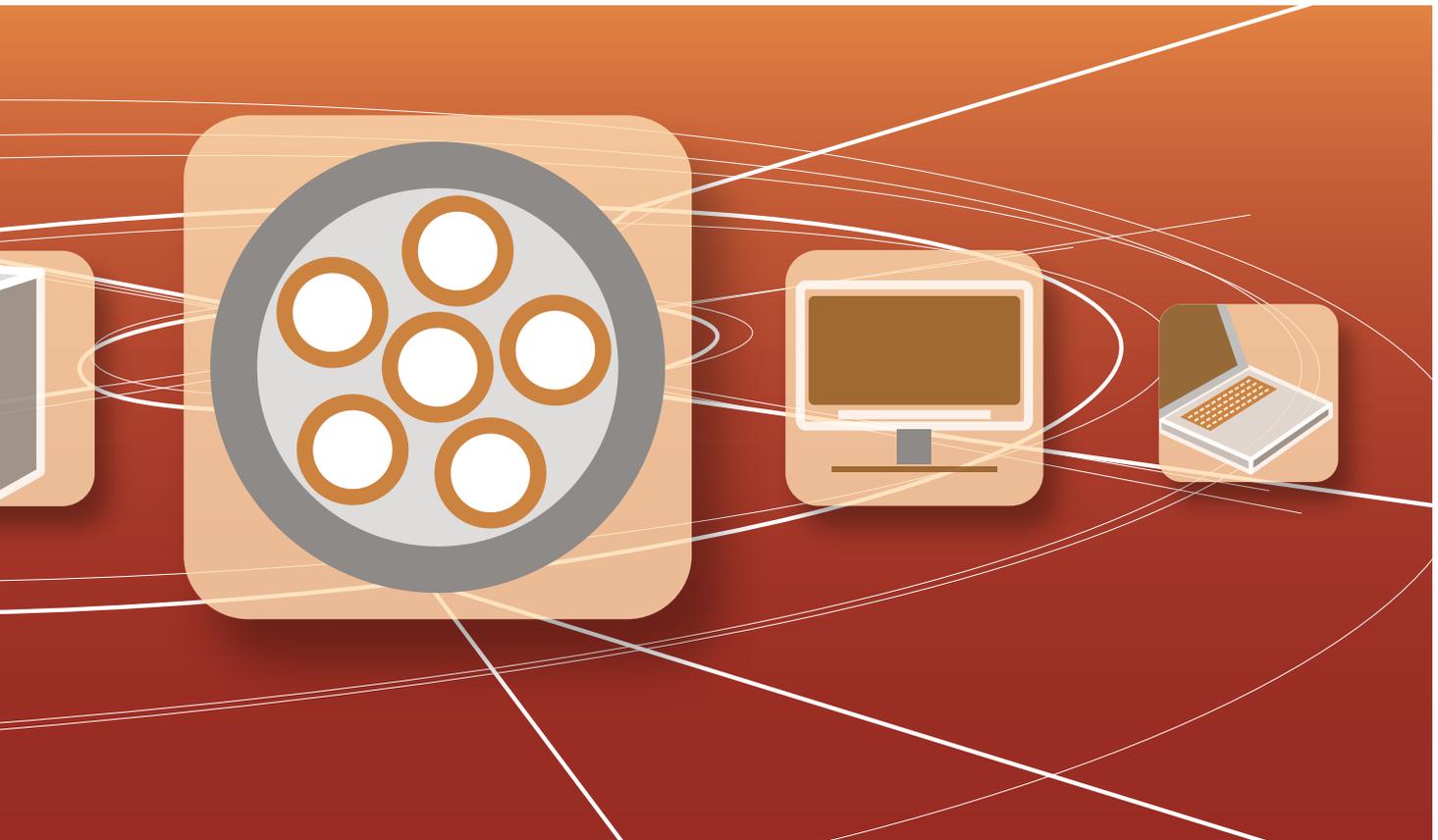
Wireless Technology Poses Problems

Whilst IT managers may feel reasonably comfortable in meeting the challenges thrown up by their wired networks, they do not have so much confidence with regard to wireless facilities. The benefits through enabling employees to operate via wireless connections have forced the management of these systems back onto the agenda. Companies that initially opted to ignore wireless technology have nevertheless been forced to incorporate it into their network planning, as employees

were simply using their own wireless devices regardless. A major problem for all IT managers is how to protect their systems against potential hackers that simply roam areas to identify free wireless access zones and use these liberally.

Wireless Adds To Security Pressures

In such instances, IT managers do not have ultimate control over where access zones are located, but have to deal with ensuing interferences over their enterprise networks. How best to resolve the issues of quality of service and security will remain with the wireless industry for some time to come. On this basis alone, it does not seem likely (as has been suggested by some commentators) that wireless networks will anytime in the near future erode the dominance of the wired network within the enterprise space. Simply attempting to manage wireless access as a complementary feature of the overall network is proving problematic enough.



Data Handling Needs Increase

The IT industry consensus on how to best manage the enterprise network has fluctuated over the years. The current thinking is that a centralised, rather than decentralised, approach is best. On the day-to-day side, IT managers have been tasked with aligning IT resources with current business priorities, whilst maintaining flexibility to cope with future needs. In very basic terms, the datacom network is now being thought of as the “fourth utility”, to enable unused capacity to be redeployed to where it’s best needed at the workstation level.

New Hardware Being Deployed

Server utilisation rates in many instances typically run as low as between 10% and 20%. This is attributed to the fact that when equipment purchases have been made in the past, management has not bought only the capacity relevant to their immediate needs, and has tended to over-provision on a “just-in-case” basis. IT managers have been deploying practices that increase not only the flow of data traffic, but also its

storage and internal use, to tie in with current and future potential threats to security. Such practices include the use of network grids, SANS (storage area networks) and new hardware, including servers and blades. The impact of the use of this type of hardware lies at the heart of all current network-related discussions.

Compliance Forcing Enterprises To Change

The preference for a centralized approach bucks the trend of decentralization emerging at the desktop, offering distributed applications. This change in stance is partly related to compliance and regulatory issues surrounding the storage of all incoming and outgoing data. Whilst most enterprises would question the need for this level of scrutiny, the spate of high profile corporate fraud cases that have recently come to light have led to legislation. This is most relevant to North America, but it has set a precedent for other parts of the world.

GROWING ROLE FOR DATA CENTRES

Data Centre Occupies Pivotal Role

The concept of the data centre as important to IT management enjoyed a surge in popularity during the dot.com era, only to subsequently crash in the wake of the downturn. During this period, the data centre evolved from functioning as a basic secure server room, to more of a mission-critical base. The pressure facing many enterprises has seen the data centre enjoy a renaissance over the last two years, mainly in North America and Europe. Although expectations about the role of the data centre have increased in recent years, in many cases data centre design has not altered to reflect either the leap in technology that the industry has been making, or to cope with added demands placed on disaster recovery management, which has become a

much higher priority for businesses in the light of major incidents like 9/11.

Internal or External Data Centres

There are two principal types of data centre: (a) the Corporate Data Centre, which is located in-house and managed by the company's own internal staff; and (b) the Internet Data Centre, typically owned and managed by an external third party, such as an Internet Service Provider. An enterprise may choose to rent data centre space from such an external provider, so as not to have to get involved with management and maintenance of the facilities. This practice is referred to as co-location. Both types of data centres are required to operate within a very strictly controlled environment, keeping temperature and humidity within a limited range, whilst being equipped to respond to hazardous weather conditions, power cuts or breaches of security. The high power output of the electronic equipment concentrated in a data centre means that efficient cooling systems are essential to maintain a consistent temperature.

Location of Data Centres

Security considerations have had an impact on the location of data centres. Thus banks, with major head office locations in financial centres such as the City of London, where there is perceived to be a small but significant threat of a major incident that could disrupt communications and risk loss of vital data, may need to establish a corporate data centre in an alternative location where the threat is considered to be lower.

Consolidation of Data Centres

As was mentioned earlier, many enterprises are choosing to follow a centralised route. This is forcing many of them to reassess and ultimately consolidate their fragmented data centre stock, which invariably leads to establishing a series of larger, but dedicated, operational buildings. The model data centre will ideally house high-speed, "always

on" networking systems of very high reliability. The high-speed concept has meant that even equipment purchased only four years ago can be considered as legacy, and perhaps not completely up to the task required.

Greater Alignment Between Active and Passive LANs

In terms of IT budgets, the highest proportion has traditionally been invested in the active part of the network, which houses the electronic equipment such as routers, hubs and switches. In very basic terms, these are often referred to as the traffic wardens on the data network. In contrast, the passive network or datacom highway, of which LAN cables are a part, has typically not been given anywhere near the level of recognition it merits. Whilst a personal computer will on average be upgraded every 5 to 7 years, and an active switch every 7 years, the structured wiring system (comprising LAN data cables and connectivity) is replaced on average only every 15 years. In overall network budget terms, cabling has typically represented between 5% and 7% of the total.

Enhanced Networks Required

The resurgence in interest in all things related to the data centre is benefiting suppliers of LAN cables, as the changes to the network made at the active level need to have equivalent support at the passive level. The proportion of the IT budget relating to the data centre can account for at least 50%, now affording the role of LAN cables a much higher profile. In comparative value terms, they continue to represent a small share over active products, but they are being factored into the overall solution, rather than being an afterthought. In view of anticipated growth in demand for higher network speeds, it is strongly believed that applications developed for the data centre environment will eventually migrate to the desktop. Structured cabling products will provide this support.

IMPLICATIONS FOR CABLING

LAN Cables Within the Enterprise

LAN cables are used in premise or enterprise networks, either within buildings or between buildings in a campus-style layout. They are also often referred to as "datacom cables" or "data cables", though strictly speaking these terms could include some other types of cable not used in LANs. LAN cables are typically installed in conjunction with interconnecting hardware, to deliver a structured wiring system. There are two main LAN cable media in current use: copper twisted pair and multimode fibre optic. Coaxial cable was used in some early LANs but has been superseded by twisted pair cables.

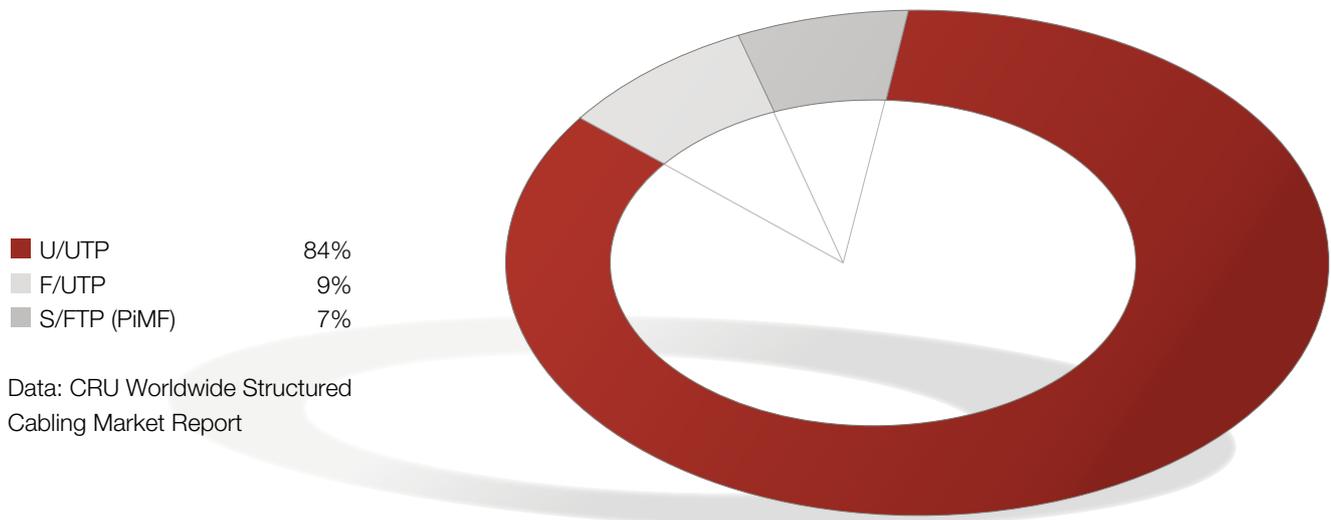
Horizontal and Vertical

Copper twisted pair cables are used mainly to deliver data from a distribution frame (patch panel) to the outlet (desktop), referred to as the horizontal segment of the network. Fibre optic cables are generally used in preference to copper cables within the vertical building backbone (also referred to as the riser or backbone) for medium/large networks or in environments where high bandwidth is required. These riser cables are used between floors, linking distribution frames on each floor. At the termination of the horizontal cable patch cords are used to connect the wall or floor outlet to each individual workstation.

Electromagnetic Screening of Cables

The basic function of electromagnetic screening is to contain the transmitted signal within the screen and to limit interference from external sources of electromagnetic radiation. (The terms "screen" and "shield" are used interchangeably in the cable industry.) Electromagnetic screening of cables can be provided by wrapping foil (thin metallic tape, copper or aluminium) around the cable, or by braiding (copper or aluminium wires, sometimes tin-plated or silver-plated).

GLOBAL DEMAND FOR LAN TWISTED PAIR CABLES BY CABLE TYPE 2007



These screening methods can be used separately or in combination, i.e. foil plus braid.

Twisted Pair LAN Cable Types: UTP, FTP & SFTP

The most commonly used design of LAN cable contains four twisted pair conductors. There are three principal varieties of twisted pair cable construction, traditionally known as UTP, FTP and SFTP. Within these basic designations the “U”, “F” and “S” indicate the design of each type of balanced twisted pair cable, from the most basic unshielded version (UTP), moving on to the foiled or partially screened version (FTP), and ultimately to the top-of-the-range fully shielded version (SFTP). To ensure optimum performance, if UTP cable is used, it would be matched with UTP components to make up the structured wiring system, and likewise FTP and SFTP cables must be matched with the appropriate components.

LAN Cable Types

In view of the number of alternative combinations of screening methods there was some scope for confusion, so the traditional designations for LAN cables, though they continue to be widely used, have been reworked,

to provide a more specific framework for system installers and IT managers. The newer designations for LAN cable construction are: U/UTP, F/UTP, SF/UTP and S/FTP. The first letter in each designation indicates the type of outer shield used, “U” for unshielded, “F” for foil, “S” for braid and “SF” for foil + braid. The second letter (after the “/”) indicates the type of shielding used on each pair. Thus the newly designated SF/UTP refers to a braided shield with a foil surrounding a UTP cable, but with no shield around the individual pairs. In contrast, the new S/FTP refers to a braided outer shield, with a foil shield on each individual twisted pair. S/FTP was referred to traditionally as SFTP or PiMF- Pairs in Metal Foil.

U/UTP Traditionally Dominant

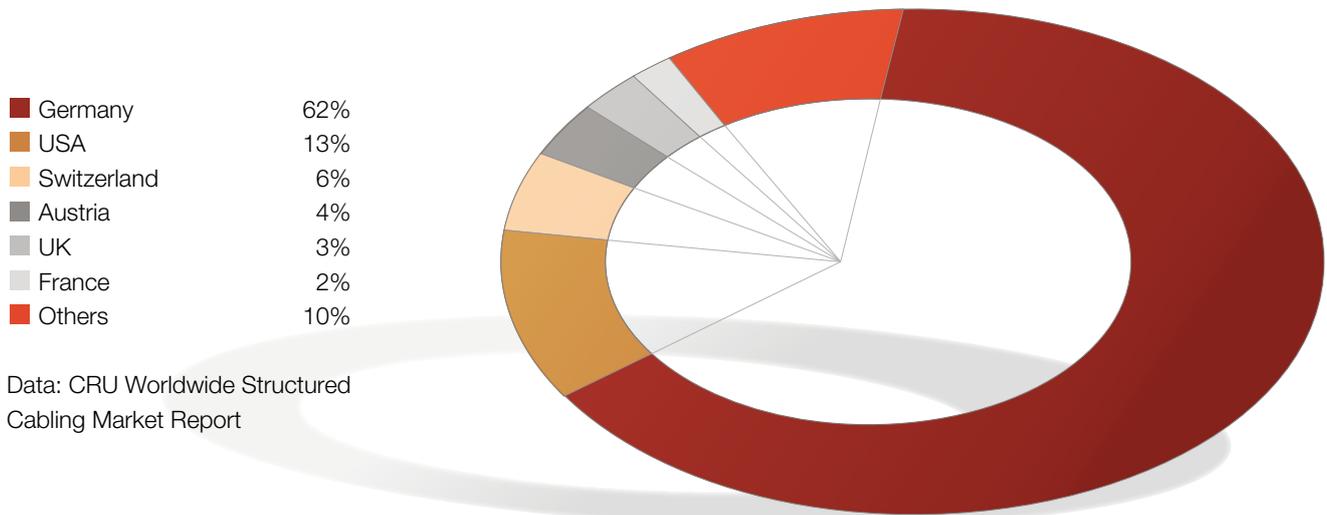
The global LAN cable market has traditionally been carved up in terms of copper cable demand in a reasonably clear-cut way, reflecting how the market in different regions or countries originally developed. This was fashioned by the particular technology that was offered by the major suppliers that first established the structured wiring system market in these countries. Until recently, these trends have largely remained unchanged, with choices

made by customers in the early years usually replicated in later upgrades to higher bandwidth, although not always with the same supplier. Markets that have traditionally used unshielded systems have tended to retain this preference, while markets that have adopted screened solutions have stayed that way. As illustrated in the chart, the dominant product type within the global copper twisted pair cable market is U/UTP.

International Standards Allow Flexibility

Guidance set down by international standards bodies (the main relevant ones are TIA/EIA, ISO/IEC and CENELEC) does not promote one product type over another, but standards do lay down strict criteria with regard to the performance of cables within the network. Standard compliance is determined by the effects that cable and components within the passive network will have on signals at various frequencies. Compliant systems should limit the degree of unwanted signal distortion and noise introduced by the cabling system itself. Key performance criteria on which the industry focuses attention include reducing insertion loss (attenuation) and alien crosstalk. The

COUNTRY SHARE OF TOTAL S/FTP (PIMF) LAN CABLE DEMAND 2007



Data: CRU Worldwide Structured Cabling Market Report

latter term refers to interference from external sources of noise: shielding is one means of reducing this problem.

Restricted Pockets of Demand for Shielded Cabling

Shielded LAN cables and premises wiring systems have traditionally been more popular within some parts of Northern Europe than elsewhere. Demand for fully shielded systems (especially S/FTP or PIMF) has been highest in Germany and Austria. In France users have traditionally favoured partially screened cables (especially F/UTP) to fully screened versions and a broadly similar trend has evolved in Scandinavia. In our chart, the US appears as the second largest S/FTP market, but this is a result of the very large total absolute size of the US LAN cable market: penetration of PIMF in volume terms in the US market is only 1%.

No Strong Conflict Over Shielding

The popularity of U/UTP in most parts of the world can be attributed partly to its lower cost of manufacture, which ultimately benefits the end-user through lower initial cost. Many of the world's leading LAN cable producers are North American in origin, and some of these

have exclusively favoured U/UTP. The rivalry between the U/UTP and S/FTP camps over the years has been relatively light, in the sense that neither party really strayed onto each other's territory. That is not to say that demand for S/FTP cable has not existed in traditional U/UTP countries, but it has been either sporadic, or restricted to very specific environments. Some cable groups operating in a variety of markets have offered both shielded and unshielded solutions, aiming to meet local market preference.

Higher Performance Opens Up Debate

However, the heightened demand for optimal performance and security management within data centres has triggered a wider debate that has seen S/FTP solutions come into head-to-head competition with U/UTP solutions. The consensus on guaranteeing optimal performance within both active and passive networks is currently settled on 10 Gigabit Ethernet as its framework. In terms of standards, performance criteria are being set out in relation to 10GBASE-T. In reference to both unshielded and shielded copper media, the initial corresponding LAN cable specifications were Class E

(otherwise referred to as Category 6, defining balanced cabling characteristics over a maximum bandwidth of 250 MHz) and Class F (otherwise referred to as Category 7, defining balanced cabling characteristics over a maximum bandwidth of 600 MHz).

Screened Cables More Secure

Improved security is one benefit that screened cables can generate. In theory, the EM fields emitted by unshielded cables could be detected by suitable equipment and network traffic monitored. Even if the risk is very small, really high security networks may choose to use screened cables or, eliminating any risk of external eavesdropping, use fibre optic cable throughout. In practice, only a few network installations, such as sensitive military operations, have used fibre optic cable for security reasons.

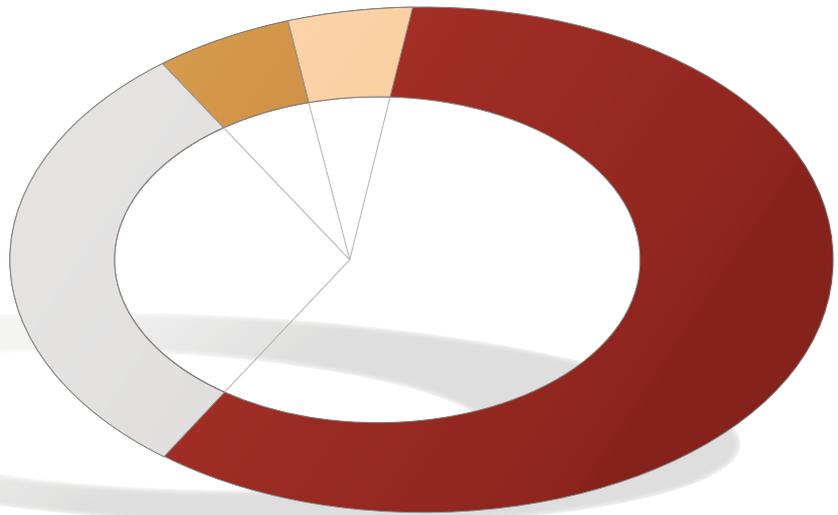
Forcing Change in Supplier Pace

As is typical of the IT sector as a whole, suppliers often seek to differentiate themselves by marketing products that they claim will perform at levels beyond those specified by the industry standards bodies. The suppliers of structured cabling are no different from the rest of the IT industry in this respect. By 2006 many U/UTP and F/UTP LAN cable pro-

GLOBAL DEMAND FOR LAN TWISTED PAIR CABLES BY CATEGORY 2007

■ Cat. 6/Class E	56%
■ Cat. 5E/Class D	33%
■ Cat. 7/Class F	6%
■ Cat. 6A/Class EA	5%

Data: CRU Worldwide Structured Cabling Market Report



ducers had already launched enhanced versions of their existing Category 6 / Class E designs. This invariably meant that they were launching products at Category 6A / Class EA level, in anticipation of the final standards ratification. The standards body in the US, the TIA, has not yet actually ratified its version of this standard. It is anticipated that this will emerge later in 2007, but the performance parameters are already widely known. Suppliers of PiMF cables have been quick to point out that their products (Category 7 / Class F, offering up to 600 MHz) were already compatible with the emerging standard, and hence no upgraded version would be necessary.

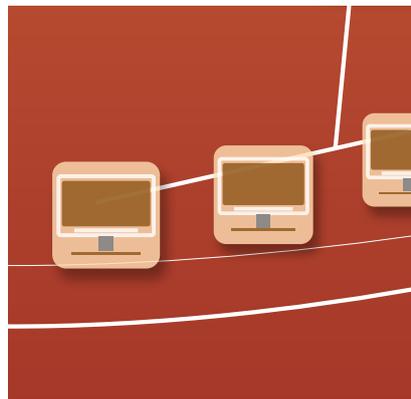
Design Makeover for Cables

One key criticism faced by suppliers of U/UTP cable is that, in their quest to provide the level of performance required for overloaded networks, their enhanced cables have ended up being even bulkier than S/FTP cables, a factor that has been used negatively by the competition over the years. In data centres large numbers of cables may be bundled together in cable trays. To ensure that their products remain attractive to data centre managers struggling to cope with cramming even more products into limited space, sev-

eral suppliers have come up with SFF (Small Form Factor) cables. This has led to significant reductions in the overall diameters of high bandwidth U/UTP cables.

Initial Muted Reaction From Customers

The structured wiring systems user base has not yet followed the emerging trends in the IT sector. Part of the delay in greater migration to Category 6A has not only been the time it has taken for standards bodies to finalise their guidelines, but also the lack of relevant active equipment. This is already changing, with several equipment suppliers launching server adapters and switch modules specifically for 10Giga-



bit Ethernet in January 2007. They have conceded that the best approach is to offer attractive pricing to enable the market to move towards mass uptake in as little time as possible, which will ultimately benefit all suppliers competing in this space. This may not initially be sufficient encouragement to gain mass-market appeal. Many customers are still undecided as to whether they actually need to consider 10Gigabit Ethernet, and may prefer to stick at 1Gigabit Ethernet. Using advice from the industry standards bodies, Category 6 / Class E is deemed adequate to meet these needs. Indeed, the ripple effect from the first phase of the 10Gigabit Ethernet debate has been a significant upgrade amongst customers to Category 6.

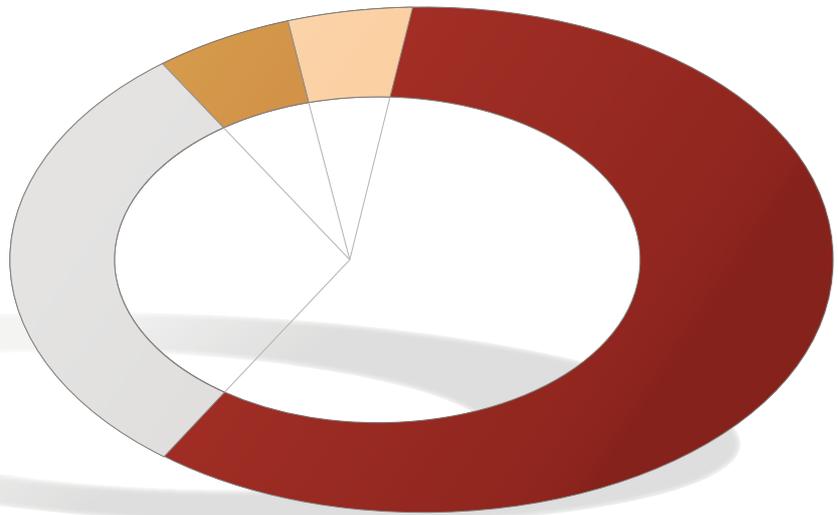
U/UTP Oriented Suppliers Concede Value of Shielding

Several suppliers, even though they have traditionally offered only U/UTP structured wiring systems, have launched S/FTP products since Q4 2006. Whilst they may continue to place greater emphasis on their U/UTP business, such moves are a reflection of the importance of the debate currently underway. The process guiding this strategy of introducing shielded products may be one of future-proof-

SHARE OF FIBRE IN DATA CENTRE AND SAN ENVIRONMENT

■ Multimode 50µ/OM3	55%
■ Singlemode	25%
■ Multimode 62.5µ/OM1	15%
■ Multimode 50µ/OM2	5%

Data: CRU Worldwide Structured Cabling Market Report



ing through trying to anticipate developments that may occur in a few years time. Thoughts are already turning to the next generation performance level, with references emerging to deployment of 100Gigabit Ethernet, by 2010!

Enhanced Shielding Also Imminent

Suppliers of shielded structured wiring systems are also trying to raise the bar in terms of system performance. They are working in association with standards bodies to establish and ratify a standard for Category 7A. Although the so-called Cat 7A standard is, as yet, some way off full IEEE ratification, it will undoubtedly start to appear more frequently in marketing campaigns. As we understand, the standard will endorse performance at between 900 and 1200 MHz for higher end applications, including Video-on-Demand and multimedia.

Fibre Joins Data Centre Race Also

Fibre optic LAN cables have equally emerged as a strong contender in the context of 10 Gigabit Ethernet and the data centre environment. In countries in which investment in data centres is strong, CRU estimates that demand for such cables represents around

15% of total fibre optic cable demand within the enterprise market sector. Uptake has been strongest within very large data centres, where data traffic has to travel over longer than average distances. This includes data centres owned and managed by Internet Service Providers. In these instances the ability to promote a co-location facility as being fully kitted out with fibre is viewed as a guarantee to attract customers anxious for proof of ultimate network security, in as much as that can be guaranteed.

Fibre Usage Mainly OM3

Unlike copper, the standard for 10Gigabit Ethernet over fibre has been ratified for some time. Although single mode fibre optic cables are sometimes used within the data centre, multimode cables feature more strongly. In particular OM3 multimode fibre with a 50-micron core and enhanced performance, otherwise referred to as Laser Optimized Multimode Fibre (LOMF), is considered to be the highest performer for this environment, even within the riser. 10Gigabit Ethernet performance out to the desktop is not considered an issue over the interim period, outside highly security sensitive environments such as banking and government.

FIRE SURVIVAL CABLES

Fire Survival and Circuit Integrity

Fire survival cables are cables that are designed to continue to operate for a defined minimum period of time during a fire. They are also known in the North American market as circuit integrity cables, since these are used in circuits that must be able to maintain their integrity during a fire. Many manufacturers refer to these products as "fire resistant" cables. Traditionally, the main application for fire survival cables was in fire alarm systems, as in some countries it is a requirement that such cables must continue to operate for a specified period in the event of a fire. In addition to fire alarm systems, these types of cable may also be used in other safety-critical wiring circuits, such as those powering emergency lighting and sprinkler pumps.

Various Test Standards

In addition to the international standard IEC 60331, there are several different national fire survival cable standards. These national standards are generally more rigorous than IEC 60331. The

CABLE FIRE SURVIVAL TEST STANDARDS

Country	Standard
International	IEC 60331
European	EN 50200
Germany	DIN 4102 Part 12 [E30 E60 E90]
UK	BS 6387 [C W Z]
France	NF C 32-070 CR1
Italy	CEI 20-36
Switzerland	TP 20B/3B 3.4.2
Spain	UNE 20431
USA	UL 2196
Canada	ULC S139
Australia	AS/NZ 3013
Singapore	SS 299-1 [C W Z]

Data: Cable manufacturers' product literature

fire performance tests check that the cable can survive not only fire, but also mechanical shocks and water spray. Some standards involve testing not a just a length of cable, but apply to the cable plus fixings. For example, the North American standard for circuit integrity cables involves particularly robust tests of the cable and its fixing system, including a blast from a high pressure hose after a fire test in a large furnace.

Alternative Designs for Fire Survival Cables

The earliest type of fire survival cable was mineral insulated (MI, also sometimes known as MIMS, MIC or MICC). An MI cable consists of copper conductors surrounded by mineral powder insulation (usually magnesium oxide) contained within an outer metal sheath, usually a copper tube. Though MI cable is a traditional design of fire survival cable, they found favour only in certain countries, such as the UK and China. Alternative fire survival cable designs that use polymeric insulation and tapes (often mica) are now in wider use than MI cables. In the event of a fire the polymeric insulation forms a protective ash so that the cable can continue to operate.

New Applications Emerge

Traditionally fire survival cables were low voltage energy cables, essentially building wire but with enhanced fire resistance. In more recent years other types of cables have become available with fire survival properties, including coaxial cable, twisted pair communication cable and fibre optic cable. Fire survival communication cables are aimed at applications such as more sophisticated alarm systems, emergency telephone lines, CCTV systems and public address systems that have to continue to operate during a fire.

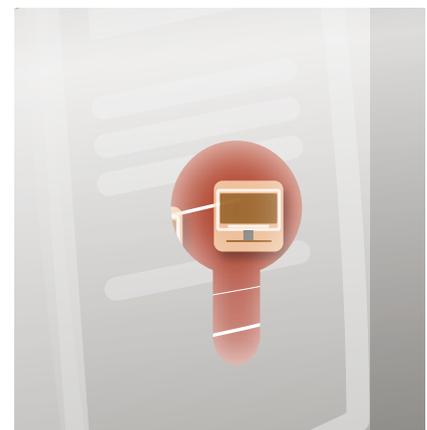
Niche for Fire Survival LAN Cables

Much of the debate over the fire performance of LAN cables in recent years relates not directly to their fire survival characteristics but to concerns over (a) cables being a potential means by which a fire within a building could spread, and (b) the potentially harmful emissions given off by some cables when they are exposed to fire. These issues are very important, but are separate from the fire survival performance of LAN cable, which is not generally a major concern. It seems unlikely that a very large market for LAN cables with enhanced fire survival properties will

emerge. In normal office buildings the LAN network is very important, but, unlike alarm and other emergency systems, it does not have to continue to carry out essential functions during a fire. However, there are niches where fire survival LAN cables could be used. For example, within data centres, in the event of a major fire, some critical cables would need to operate for long enough to allow the transfer of data to a back-up location.

CONCLUSIONS

The increasingly complex make-up of the typical enterprise network has pushed the debate over the importance of highest quality and when to buy "best-of-breed" further up the agenda of many customers. Whether their ultimate choice will rest with unshielded, fully shielded or fibre optic LAN cable at this point is difficult to gauge. Users now have a range of highly performing products from which to make a qualified choice. The challenge for the supplier industry is not to start pushing performance levels above 10Gigabit Ethernet too soon, thereby further confusing and potentially alienating their customer base. Security issues have become a greater consideration in the minds of IT managers and consultants, a trend that is likely to continue. The key concern of IT managers is to maintain network reliability and integrity.





FUTURE PROOFING AGAINST
EMERGING THREATS