CRYPTOMAGAZINE

HAGELIN-CRYPTOS
CRYPTO AG

Magazine for the customers of Crypto AG, Switzerland 2 ▪ 2012

AIR FORCE

DATA SECURITY IN THE AIR

Dear Reader
How differently people would travel today, in the air and elsewhere, were it not for the first successful motorised flight by the Wright Brothers on 17 December 1903. But even before this historic moment a number of other pioneers had attempted to make man's dream of flight a reality. Wilbur and Orville Wright would never have dared imagine the current state of the art in civilian and military aviation back in 1903, not in their wildest dreams.

This is reason enough to devote the current issue to a sweeping look at the subject of aviation. Crypto AG notes with pride that we too can ideally integrate our pioneering products and solutions into the infrastructure of anything from modern command and control information systems to fighter jets. Our motto in these efforts: it is reassuring to know that secure communication is always guaranteed no matter how fast you travel and what mission you are on.

I hope you enjoy reading this latest issue of CryptoMagazine.

Giuliano Otth

President and Chief Executive Officer

PUBLICATION DETAILS

Published three times a year **Print run** 6,700 (German, English, French, Spanish, Russian, Arabic) **Publisher** Crypto AG, P.O. Box 460, CH-6301 Zug, www.crypto.ch **Editor-in-chief** Béatrice Heusser, Crypto AG, Tel. +41 41 749 77 22, Fax +41 41 741 22 72, E-mail beatrice.heusser@crypto.ch **Design/Typesetting** illugraphic, Sonnhalde 3, CH-6332 Hagendorn, www.illugraphic.ch **Translation** Apostroph AG, Töpferstrasse 5, P.O. Box, CH-6000 Luzern 6, www.apostroph.ch **Printing** Druckerei Ennetsee AG, Bösch 35, CH-6331 Hünenberg **Reproduction** Free of charge with the consent of the editorial office. Courtesy copies requested. Copyright by Crypto AG **Illustrations** Crypto AG: p. 2, 8, 9, 14, 15, 18, 19, 20 · Eugen Bürgler: cover, p. 24 · illugraphic: p. 5, 6, 13, 22 · Patrouille Suisse: p. 10, 11, 15 · Robert Metcalfe: p. 22 · Swiss Air Force: p. 3, 5, 8, 12, 13 · Shutterstock: p. 3, 4, 6, 7, 12, 17, 18, 19, 20, 21, 23 · Steve Mann/Shutterstock.com: p. 2

Air force as part of the combined task force

PRECISION WORK IN THE SKY MANAGED SECURELY FROM THE GROUND

Modern air forces today are engaged more than ever in the business of split-second tasks. Everything depends on maximum coordination between effectors in the sky and sensors and operational command and control on the ground. The resulting flood of data can be sent in real time with special transmission protocols and concentrated into an operational picture. The success of each and every mission would be in jeopardy without this protection.

by Jahn Koch, Customer Segment Manager Defence

Combat Air Patrol (CAP) is a service rendered high above Davos, Switzerland, the venue of the World Economic Forum. Imagine an F/A-18 of the Swiss Air Force equipped with live ammunition taking off on a training flight to take over surveillance duties at a predefined time in the indicated no-fly zone above the conference area. It is accompanied and covered by a second jet known as its wingman. Flying a special loop in the operational area allows both planes to illuminate the region fully with onboard radar by patrolling along paths running opposite to each other. They are supported on the ground by tactical aircraft radar that illuminates the heavily compartmentalised terrain below them. This method covers even the narrow valleys invisible to the permanently installed FLORAKO radar system. Antiaircraft positions are placed at other suitable spots in the terrain where they can cover the no-fly zone with fire in case of emergency.

From routine flight to emergency

A non-identified aircraft suddenly appears just above the cloud cover. It has penetrated the no-fly zone and is starting to cross it without authorisation. The fighter jet pilot received this information in response to his inquiry with the Tactical Fighter Controller (TFC) at the Air Operation Centre (AOC) after approaching the aircraft and making radio contact with the TFC. To give information about the authorisation of the object in question, the AOC relies on the fighter jet pilot to provide a description that is as precise as possible. Apart from aircraft registration, the most helpful information is aircraft type, wing shape, colour and any noticeable weaponry. This data has to be conveyed over radio at this point. The reported information yields a clear-cut answer from Air Traffic Control in this case: the aircraft is not authorised to enter the no-fly zone. This is an emergency, a "hot mission"! The fighter jet flying out in front now acts as moderator, attempting with various manoeuvres and on various radio frequencies to contact the intruder and to get it to leave the no-fly zone or to make an escorted landing accompanied by the two air force jets. If these appeals to cooperation bear no fruit, the aircraft can be shot down in a worst case scenario. Either the wingman off to the side and behind the moderator does this or the antiaircraft units on the ground. They have been put on the alert in the meantime and their radar is also tracking the target. The Air Operation Centre follows the dramatic events precisely as they unfold, drawing on the concentrated information it receives from the radar on board the fighter jet, from the FLORAKO system and from the antiaircraft radar systems. If the intruder tries to escape exposure to the effectors or localisation by the sensors by diving into a cloud bank and fleeing into one of the narrow box-like valleys, it remains visible to the tactical aircraft radar and can continue to be tracked. The operational picture consolidated by the AOC is not reserved solely for the TFC. It is sent back in full to the pilots in the fighter jet, for example, and displayed on their interactive helmet visor so they retain a complete overview of the situation.

In the cockpit of an F/A-18.

Data link as a lifeline for the effectors

The scenario above actually occurred in 2012. It is one of several incidents of this type where everyone involved ended up getting off lightly but where the private pilot who entered the no-fly zone unintentionally or out of neglect had to face hefty judicial consequences. Apart from safeguarding no-fly zones in exceptional situations such as to protect a conference as in this example, the Swiss Air Force conducts constant air patrolling and enforces the safety and order of Europe's most heavily frequented airspace. Even for this vital service in times of peace, the air force needs an infrastructure that ensures the interplay of all sensors and effectors and is absolutely reliable about making the necessary information available at all times. The common recognised air picture (RAP) is the air force equivalent of the common relevant operational picture (CROP) and is the point around which all operations at and around Mach speed revolve. It is obtained by concentrating all sensor data and serves as the basis for all operational decisions during a mission. For this reason, the RAP has to be available in real time at all times for everyone involved. Permanently installed sensors and the regular AOCs for ordinary and extraordinary situations usually exchange their information over permanent high-speed fibre-optic and wire connections in the national fixed-line network, a hardened militarised operational network that is highly autonomous from civilian networks. The mobile positions of the antiaircraft defence and tactical air radar are connected to the AOC via a temporary link into the fixed-line network, preferably microwave links. The fighter jets for their part have analogue aeronautical radio service for voice communication for connecting to the fixed-line network. For data transmission, however, they rely on powerful customised military protocols, data links based on standards such as the NATO-STANAG 5516.

Retaining the confidentiality and integrity of operational information

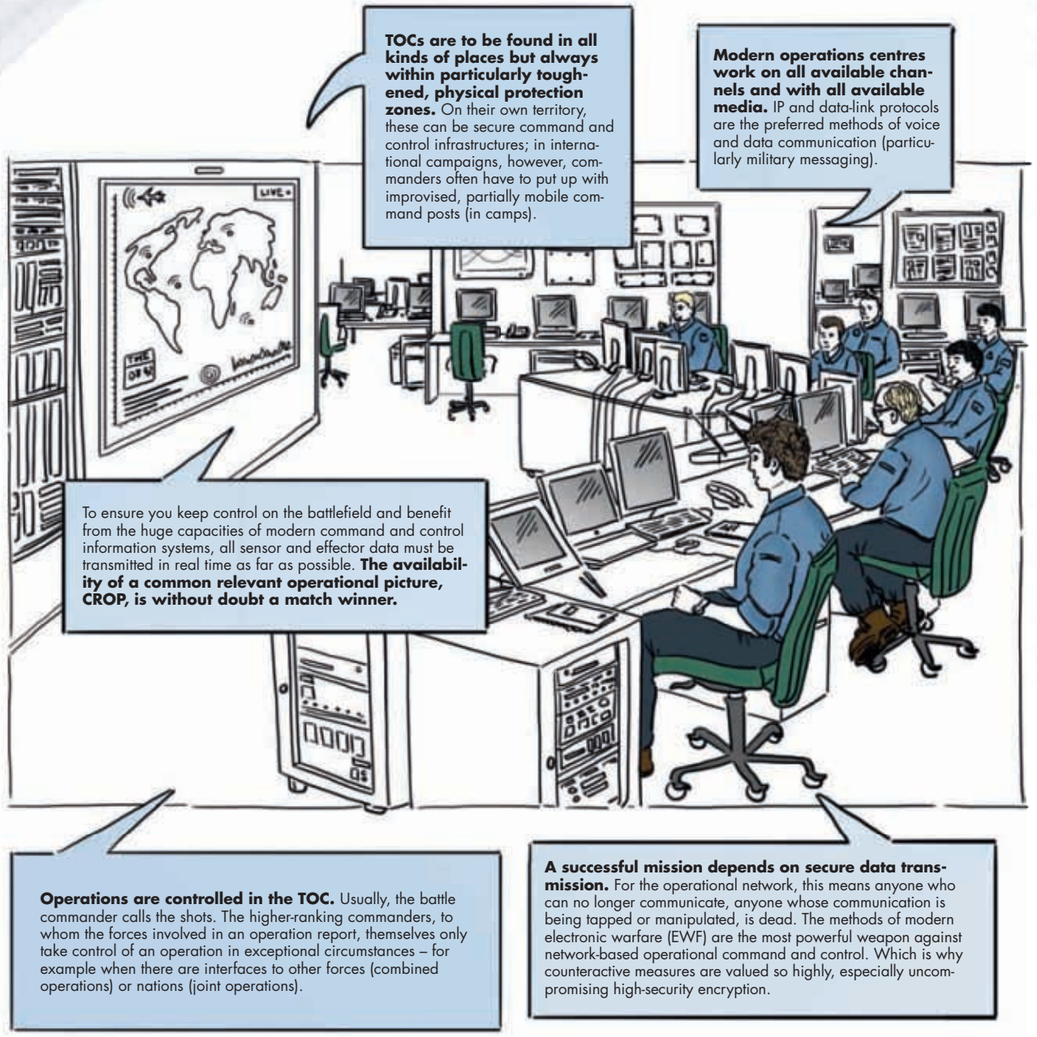
The reason that data and radio communication requires maximum cryptologic protection is virtually self-explanatory. Although government secrets are rarely divulged in tactical information shared during an air operation, operational decisions about, say, the life and death of the crew of an uncooperative plane that has penetrated a restricted-flight or no-fly zone are anything but trivial. One hates to contemplate a situation where outsiders would be hypothetically capable of feeding the wrong instructions to fighter pilots manning the gun controls and simulate, say, a command to shoot down a stray plane. It would be equally fatal if the pilots' aeronautical radio service and the radio communications of the antiaircraft positions could be influenced by the AOC of amateurs or could be tapped – even if it were only by technically experienced members of the media hoping to create an exciting story by publishing a taped conversation. The situation becomes all the more serious for combat missions in defence operations where the opponent wages electronic warfare and tries everything that could physically disrupt the exchange of information of numerous players in an air force combat unit or compromise the content of that information. Electronic warfare should be understood not only in the strictly classical sense. This fact is obvious from the guerrilla fighters in Iraq and Afghanistan in 2009, for example, who succeeded in tapping the non-encrypted video feeds of American aerial surveillance drones with commercially available software bought on the Internet. Only maximum cryptologic protection can effectively remedy the situation and ensure that the confidentiality and integrity of the transmitted operational data are retained.

Combined/joint: how much exchange should there be?

The combined task force of sensors, effectors and a command and control centre is by no means confined just to the air force. It is equally common today in land and naval forces. Modern combat operations no longer entail just combat with combined arms but campaigns involving combined operations, including joint logistics and command and control support. Protection considerations in the past led to many armed forces procuring different means of communication even within the same countries and protecting them with separate encryption systems. These approaches now have to be revised because of the widespread introduction of multifunctional battle networks and the diverse possibilities presented by ever newer command and control information systems. When national armed forces are grouped together to create effective mission task forces within international alliances, the need for a common basis for communication with standard protection for all players becomes all the more urgent. This arrangement alone ensures all-encompassing safety as part of joint operations, also against friendly fire, i.e. unintentional attacks by alliance partners.

THE TACTICAL OPERATIONS CENTRE (TOC) AT A GLANCE

Everything converges in the TOC. Sensors deliver a flood of reconnaissance data that is compressed into a common relevant operational picture, CROP. This is the basis for all operational decisions by the operational commander. Effectors have the same CROP. This means they can follow and implement the intentions of the commanding officer live at all times. Any changes in the course of operation are reflected immediately in the CROP – the situation develops.



Network-based operational command and control

MISSION ACCOMPLISHED IN A NETWORK THAT FITS CURRENT OPERATIONS

Joint operations involving modern weapon and sensor systems can be conducted all the way up to the front in real time thanks to complex command and control information systems. The prerequisite is that the underlying data network must have a logical, correct structure and be highly available and secure. However, these aspects are precisely where improvements are needed.

by Jahn Koch, Customer Segment Manager Defence

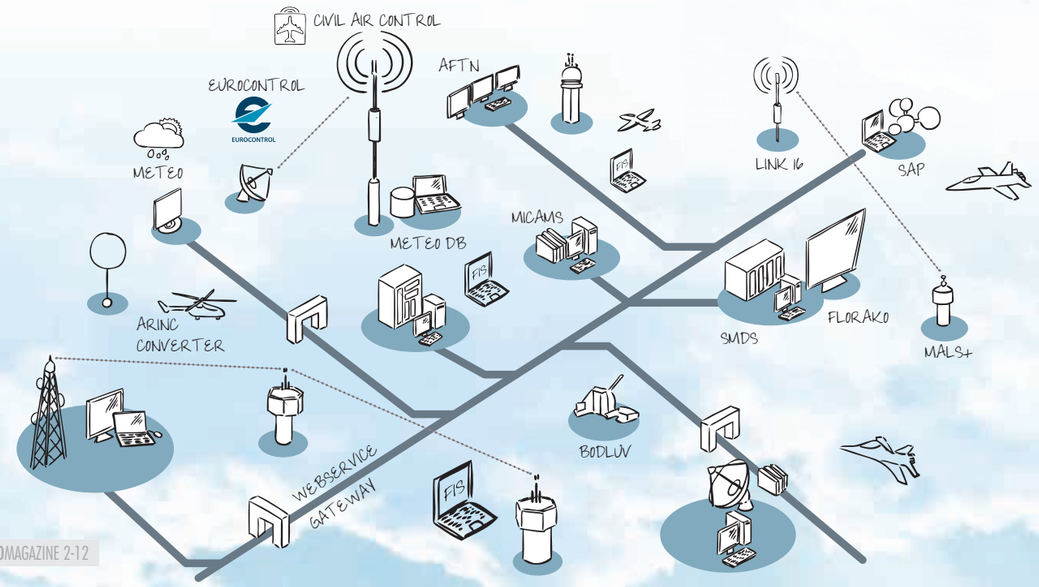
Command and control information systems have been undergoing an extraordinary evolution for years now. They allow large quantities of sensor data to be gathered and compiled in ways that are ever more comprehensive, detailed and, most importantly, reliable and to be converted into a precise operational picture. In addition, there is highly advanced software available today that can give human decision-makers options for action generally within mere seconds using independent concentration and analysis processes. The objective is always to weave together all relevant tactical information to form a common relevant operational picture (CROP) in the medium term whether the data being processed pertains for example to the fuel level of a helicopter, infrared pictures from a reconnaissance drone as a video feed or the health of an infantry platoon advancing on the critical flank in urban terrain. The information is used as a basis for assigning specific tasks to effectors on the ground, in the water and in the air (also in outer space in the foreseeable future) to reach a sub-goal or the final goal of the operation.

This is the theoretical aspiration of today's armies in the national (combined forces) and international (joint forces) environment of large alliances. The reality right now is still more modest in many places. There is a worldwide trend towards network-centric warfare, however. This approach allows the progressive merger of formerly separate branches of the service to forge highly effective task and response forces.

Operational networks: highly available and broadband if possible

At present, network-centric operational command and control posts (also known as war rooms) need one small data centre with a corresponding local network environment for their work from brigade size onwards plus a contemporary command and control information system. The subordinate units and platforms usually have to make do with more meagre data capacities. The smaller the unit and the larger the geographic distance to operational command and control, the more modest the channels for constant information exchange usually are. This is particularly true if the operation takes place on foreign territory, where it is impossible to connect the front with one's own existing fixed-line network infrastructures. The same applies to airspace and the high seas.

The more services and functions are required at an existing low throughput rate and the more information that is fed back in return to operational command and control, the better it is.

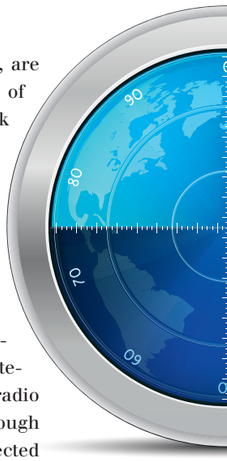


The general availability of a connection is indispensable if one has to accept less bandwidth than desired and can use only the most urgently needed interactive services over long-range channels (such as low-bit-rate HF messaging and analogue radio telephony). As a rule, smaller units are connected to operational command and control over highly mobile radio networks. Temporarily "dismounted" staffs of larger units and combat groups are frequently connected over partially mobile microwave link networks. If the operation takes place in one's own territory, one can often resort to existing backbone networks. From an operational standpoint, they are particularly suitable for connecting high-performance systems such as tactical radar stations and fire control systems. The rule of thumb for modern communication and command and control resources at the front (access level) is this: the more services and functions are required at an existing low throughput rate and the more information that is fed back in return to operational command and control, the better it is.

Lurking dangers of electronic warfare

Operational networks are highly mobile at the tactical level (at the edge) of combat units. Whenever possible, they connect seamlessly to the operational level with their own resources, generally employing radio integration. They are secure to the extent that they move in a way that keeps them sealed off from other networks and have only a small number of defined transitional points into larger networks of the same military operator. Effective cryptologic protection and additional electronic hardening measures such as frequency hopping, for example, are required as well as a transmission capacity adjustable to tactical needs (field strength superiority versus detectability). Otherwise, they are at the mercy of blows from opponents waging electronic warfare (EWF). It is relatively easy to locate transmissions with physical means, to disrupt them or to put them in to disarray. Or the transmitted contents can be captured and compromised – with fatal consequences for one's own troops and mission success.

Radio equipment commonly used today has standardised cryptographic protection (generally software-based). This fact does not enhance security, however, because the products of different manufacturers are not fully compatible with each other. The situation is further exacerbated by political regulations on exporting and handling encryptions in various regions of the world. The same risk exposure exists analogously wherever an opponent can gain access to one's transmission media, i.e. also to fibre-optic and wire connections. Operational networks at the lower tactical level, for their part, are rarely exposed to the frequently evoked danger of cyber attacks as long as they have no other network transition points than the ones provided for. The associated principle is as follows: "Protected and only to the next highest operational level".



Connected to the top command over the data highway

Certain powerful sensors, weapon systems and platforms that generate a high data volume must be connected directly to the core, i.e. to the broadband strategic command and control network. Like the radio integration points, they are generally connected through temporary microwave links or are directly connected electronically or optically as part of the permanent military infrastructure (especially in the case of permanently installed sensors such as radar stations). If the operational network also has permanent command and control network infrastructures – often referred to as the backbone – the war rooms are also connected to them. This is the case throughout most developed countries. If there is no permanent fixed-line network, the partially mobile "dismounted" level of the operational network (often microwave in this case) forms the top and most powerful conclusion of the operational network.

The people with operational responsibilities and battle commanders are connected through the backbone to their superiors in the strategic and political command of an army or multinational combat force. This top command does not control the course of the operation directly but instead by specifying targets and goals. As part of the military administration, the top command typically operates on its own conventional fixed-line network structures. However, these structures are usually independent sub-networks separated from the civilian portion of the network and protected with additional hardening and logical zone transitions. Cyber attacks can sometimes inflict severe damage to this part of the combined network, commonly called the standby network, without protection guaranteed to be at the highest security level. The standby network is therefore amongst the critical infrastructures of every nation regardless of its civilian or military users.

Swiss Air Force

RELIABLE COMMUNICATION IS CRUCIAL TO A MISSION

As Commander of the Swiss Air Force, Lieutenant General Markus Gygax heads up a high-tech organisation with a diversity of real-time tasks. Along with its conventional duties of national defence, the Swiss Air Force is the only air patrol operating in Switzerland. Its mission is to ensure the official enforcement of order and safety in Swiss airspace, the most heavily frequented in all of Europe with 3,000 flight operations a day.

Jahn Koch conducted the interview

Lieutenant General, the Swiss Air Force has a broad range of tasks to perform in ordinary and extraordinary circumstances. What role do you feel a well-functioning command and control and information network plays in this regard and how big a priority is it to protect the information processed in this network?

Markus Gygax: Reliable communication systems are enormously important for us. Like all comparable high-tech organisations, the Swiss Air Force relies on the full availability of operationally relevant information. The main reason is that our tasks are time critical to a high degree and our aircraft in the air must respond within seconds when they are in operation. This response requires the ground systems and effectors in the sky to have exact knowledge about each other at all times. In our case, there is the added factor of an equally full coordination with civilian air traffic in the most heavily frequented airspace in Europe. You can compare the relative importance of our communication systems with that of mobile phones for modern society.

What risks are there that the exchange of information from sensors and effectors can be influenced from the outside and what consequences could this have?

The heavy dependence on high-tech systems naturally makes the air force vulnerable in this regard. As part of the administration, we also consider cyber attacks a genuine threat, a fact recently underscored again by the repeated attacks on the Federal Department of Foreign Affairs (FDFA). They pertain primarily to feeder networks and network areas adjoining the actual military operational network. Attacks of this kind are bothersome because they always occur at inappropriate times and disrupt daily work. The operational network itself is not as endangered by cyber terrorists because of its hardening and separation, but it is jeopardised by the classic possibilities of electronic warfare (EWF). We have regular training sessions on these electronic warfare attacks, determine existing weaknesses and remedy them. Keeping our systems absolutely up to date at all times is crucial to mission success. That is why we make such great efforts to update them constantly to the latest state of the art. These efforts start with acquisition. When Switzerland acquired the FLORAKO radar system in 2004, we had the most modern and powerful airspace surveillance capabilities in Europe.

The command and control information system for the air forces (CCIS-AF) comprises a number of individual components such as the FLORAKO. What operational possibilities does it give to your commanders and what additional ones are set to come in the near future?

The CCIS-AF is already performing indispensable services today, operating in all task areas of the air force, i.e. in defence missions, air patrolling, search-and-rescue operations and in air transport for the armed forces and the authorities. It is highly reliable and of course must remain so in the future. Commanders need to bring about further advances in how the CCIS-AF depicts and handles operational processes. In addition, there is a desire for more extensive networking that would dock mobile command posts to the CCIS over a satellite link, for example, amongst other things. As with so many projects, the limiting factor is the budget but the big advantage of these systems is that they grow continuously over a lengthy period of time and can be expanded time and again in moderate stages. There is not this option with an aircraft because you cannot get anywhere with just an engine and landing gear.

There is heavy dependence on computer-assisted command and control resources. Is this another source of danger?

We are fully aware of the existing risks especially because of the great responsibility we share for the safety and security of civilian aviation. The most important measure for the operational network besides protection and hardening is to give it a redundant design. Take the two radar stations for civilian air traffic control, for example. They are both at low to medium altitudes above sea level and would not allow reconnaissance of the airspace in southern Switzerland because of the intervening Alps. Above them are the recognised air pictures from our radar stations, which are located in the High Alps and illuminate our airspace completely and in overlapping areas. All the parties involved are linked together in secure networks, ensuring a comprehensive recognised air picture (RAP). Incidentally, the same can be said of our combat pilots. Thanks to a data link they possess all the information from their own sensors and from ground-launched sensors right in the cockpit.

If you as Commander of the Swiss Air Force had three wishes regarding the acquisition of new systems, what would be on your wish list?

My priorities would be as follows: a new fighter jet, a new antiaircraft system with a powerful tactical radar system of the kind we are now pursuing under the project name BODLUV2020 and a new drone system that interfaces with the data link. The antiaircraft system has to be directly controllable from the air force operations centre. The drone, for its part, should be able to supply us with high-resolution live video feeds. The question of what weaponry a drone system of this kind should have is not an issue for a small country like Switzerland. However, its reconnaissance capabilities are all the more significant for the overall Swiss security system, i.e. also for the police, border guards and rescue organisations.

On the subject of aircraft acquisition: What do you, as Commander of the Swiss Air Force, think of the current status of the Tiger spare parts project (TTE) that has led to such heated public debates in Switzerland?

We must acquire new aircraft to fulfil our duty to provide air patrolling. There were indiscretions and misinformation after the completion of the aircraft evaluations and in advance of the Federal Council's decision on which type of aircraft to purchase. These incidents are irritating. They took some of the discussions out of context and caused confusion amongst politicians and the public alike. The fact is the Gripen is the right aircraft to meet the needs of Switzerland and those of Sweden for that matter although our two nations do differ in many ways. The next milestone is the 2012/13 Arms Programme. It will contain the Gripen and has to be voted on by parliament. That is when we will know whether a referendum will be needed, probably in 2014. No agreements can be signed prior to that. If the acquisition proceeds as planned, it will be 2018 at the earliest before we can count on having the new aircraft. They would then become operational between 2020 and 2025 in new aviation squadrons. Incidentally, this is perfectly normal. Countries neighbouring Switzerland also decide on acquisitions first and then implement them successively thereafter.

Thank you, Lieutenant General Markus Gygax, for this interview and for your interesting insights.

LIEUTENANT GENERAL MARKUS GYGAX, COMMANDER OF THE SWISS AIR FORCE

Markus Gygax was born on 30 April 1950. After a commercial apprenticeship and the completion of pilot training in 1971, he joined the surveillance wing, where he was a member of Patrouille Suisse from 1974 to 1983.

Markus Gygax continued on in the Swiss Air Force in a variety of leadership positions and task areas. Most recently he was Chief of Air Force Operations and Deputy Commander of the Swiss Air Force from 2004 to 2008. He has been its Commander since 1 March 2009.

In his career as a pilot, Lieutenant General Markus Gygax has clocked over 4,900 flight hours.

The Swiss aerobatics team Patrouille Suisse on the ascent

CLEAR COMMUNICATION DURING A FLIGHT IS ESSENTIAL

It is a picture that could have come from a film like Top Gun or Flyboys. Six bold heroes of the air force are striding towards the viewers – in the background is a red and white Northrop F-5E Tiger: pure dynamism and adrenaline. The six men are members of the Swiss aerobatics team Patrouille Suisse and appear as described above on the team's website. They are the main attraction of Swiss aviation. As a team, they depend on clear, straightforward communication. *Casha Frigo Schmidiger conducted the interview*

The Patrouille Suisse can look back on a nearly 50-year history as an aerobatics team. It was founded in 1964 as the official aerobatic jet squadron of the Swiss Armed Forces domestically and abroad. It furnishes proof of the capabilities and precision of the Swiss Air Force nearly daily with its many performances at air shows and its public training sessions. The members of the Patrouille Suisse are all hand-picked Swiss career military pilots or air traffic controllers from skyguide, the organisation for civilian and military air traffic control in Switzerland. The demonstrations of the six aircraft are designed to be 18 minutes long and are monitored by commanders from the ground. Safety is the top priority.

Daniel Hösli is a lieutenant colonel in the Swiss Armed Forces and has been the Commander of the Patrouille Suisse since 1 January 2001. Trained as an F/A-18 pilot for the Swiss Armed Forces, he has been a career military soldier since 1981 and was a member of the aerobatics team himself for ten years, from 1987 to 1997. His impressive record of achievement at the end of last year consisted of 5,050 flight hours in the following aircraft: F/A-18 Hornet, F-5, Tiger, Hunter, Vampire, PC-7, PC-6 and PC-3.

The Commander of the Patrouille Suisse, Lieutenant Colonel Daniel Hösli, shared even deeper insights into the fascinating activities of his team in the following interview.

Lieutenant Colonel Hösli, the Patrouille Suisse is a calling card and flagship for the Swiss Air Force and is highly respected far beyond the borders of Switzerland. What are its main tasks?

Daniel Hösli: The Patrouille Suisse has mainly three responsibilities: to recruit suitable young talent, produce proof of performance capabilities and serve as an ambassador for the Swiss Armed Forces domestically and for Switzerland abroad. Incidentally, the PC-7 TEAM, which flies the training aircraft of Pilatus Flugzeugwerke, has these same responsibilities.

How closely do you work with other units of the Swiss Air Force?

We cooperate very closely. All pilots in the Patrouille Suisse are career military pilots for the multi-purpose F/A-18 fighter plane of the Swiss Armed Forces, so networking with other air force units is automatic.

How do you achieve safety during demonstrations?

We achieve it by using our best trained pilots for the shows. They are accustomed to working hard and with full concentration. There is also always a fall-back option in the sense that there is a man on standby for each pilot. A thorough briefing precedes each operation. This practice ensures that all pilots have the same valid information. Clear communication during a flight is essential!

Spectacular formation in front of the North Face of the Eiger.

Like Crypto AG, the Patrouille Suisse has to rely on maximum precision. How do you keep ensuring this precision?

We conduct a thorough debriefing with video analysis after each operation. Our stated goal is to keep improving ourselves and to optimise our precision and reliability.

One of your goals with your flight demonstrations is to stir enthusiasm amongst young people for the air force. How successful are you in these endeavours? What is the relative importance of the armed forces for young adults in your estimation?

If we can believe the latest surveys by renowned institutes, the relative importance of the armed forces for young people is on the rise again as is the recognition they give to the armed forces. Many young adults who seriously analyse our work acknowledge that the air force makes a valuable contribution to Swiss security in the third dimension.

The Patrouille Suisse even has a major role in a feature movie produced by Swiss television called "Anjas Engel" (Anja's Angel). What reactions did you receive on this project?

I received a large number of highly positive reactions. The fact that the Patrouille Suisse plays a lead in a successful Swiss movie shows how popular the team is.

Do aerobatics squadrons also have the function of demonstrating superiority in the air?

In a certain sense, yes. As I mentioned earlier, one object is to demonstrate the capabilities of the Swiss Air Force and to convince everyone that it is not worthwhile to enter into a conflict with Switzerland.

The Patrouille Suisse can look back on a nearly 50-year history. It will be celebrating its golden anniversary two years from now. What are you especially proud of?

What makes me especially proud is that the Patrouille Suisse has been flying accident-free for 48 years and that we can excite hundreds of thousands if not millions of spectators year after year with our demonstrations.

Thank you, Lieutenant Colonel, for this interview and for your interesting insights. ■

www.patrouillesuisse.ch
www.luftfahrt.ch

Unmanned flight systems

VIDEO GAMES WITH COMPREHENSIVE COVER

Even today, many armed forces are relying increasingly on unmanned aerial vehicles known as drones. They perform mainly reconnaissance tasks, using special sensors to collect relevant data about opponents in order to create a common operational picture. The second category of drones is gaining steadily in significance. They are equipped with weapons and initiate attacks. The use of these types of drones is already commonplace. There are more than 10,000 drones worldwide. *by Casha Frigo Schmidiger, Publicist*

Unmanned aerial vehicles (UAV) were initially used primarily for surveillance and reconnaissance operations against opponents. With their further development and spread, they began being used specifically to fight tactical and strategic infrastructure. After all, a drone operated semi-autonomously via a satellite link from a war room in some suburb can be deployed efficiently in the operations area to hunt down and thin out combatants without the person controlling the drone having to come anywhere close to actual combat.

Drones have revolutionised warfare. With the use of these aerial vehicles, the consequences of a war for one's own troops can be dramatically reduced. This fact lowers the threshold for initiating a war. What people often ignore in the euphoria of being able to prevent collateral damage to their own troops is that soldiers come under increased psychological strain. They may be present at the scene of events only virtually but they see the consequences of their action and the damage they inflict much more clearly than if they just dropped a bomb on enemy territory. That is why the term "War Porn[1]" is already making the rounds following "War Games".

Of course, far be it for us to cast doubt on the use of unmanned aerial vehicles. Military operations are no longer imaginable without them and they render valuable services in civilian settings as well. For instance, they can provide useful information during natural disasters. In addition, they help to compile data for the Border Guard Corps and police forces.

Big haul from the air

Unmanned aerial vehicles function similarly to model aircraft. The biggest difference is that you can only control the toy as long as you have it in sight whereas you can control a drone from a mobile or fixed control centre. This centre usually has three screens. Two show map details while the third transmits images from the camera mounted on the belly of the drone. The drone itself has two transmission channels: the sensor channel and the control channel.

A modern army today would be unthinkable without unmanned aerial vehicles. These vehicles swarming across the skies are also highly profitable targets for cyber warriors to attack because of the collected data they contain.

The US Army, for example, had to learn this lesson the painful way. Three years ago word got out that Iranian-Shiite militia units in Iraq had succeeded in intercepting and recording video data from Predator drones. The data had been transmitted over an unprotected link[2] . In the process, information about US troop movements and bases, among other things, fell into the hands of enemy combatants. One fact that attracted special attention was that Iraqi troops used SkyGrabber for this purpose, software that sells on the Internet for a bargain price of less than a hundred dollars. SkyGrabber mainly provides an easy way to tap unprotected satellite transmissions of all kinds.

Protection squared

As this example shows, the protection of drone payloads urgently requires greater attention as does the protection of control data.

The transmitted data (COMSEC) and the transmission channel used for communication (TRANSEC) must both be rendered secure to achieve efficient protection. Digital encryption renders COMSEC (voice and data) secure. Air force units are making increasing use of the Internet Protocol (IP) for their communication. For this reason, the IP VPN application was added as an extension to the MultiCom Radio Encryption Unit HC-2650 from Crypto AG. It allows secure communication to be conducted through a secure VPN tunnel. This new application is compatible with all other units of the IP VPN family from Crypto AG. IP can be used for the parallel transmission of different applications such as voice, video and further data that would otherwise only be manageable with separate interfaces, channels and appropriate COMSEC units.

But encryption alone is of no use as protection against jammer transmitters, i.e. units that obstruct the transmission path and interfere with drone control. Other technologies are needed. Frequency hopping has won out as a means of protecting TRANSEC. Instead of broadcasting at a constant frequency, the radio unit hops within the stipulated frequency range as much as several hundred times a second. The transmitter sends just a very short information packet at a certain frequency before switching to a new one. The object is not to proceed actively against the jammer transmitter but rather to evade it by taking electronic protection measures (EPM). If one frequency is disrupted, the only information packet affected is the one sent at that frequency. The disrupted packet can usually be reconstructed. The loss of a small number of information packets is tolerable and renders the process quite robust in dealing with external influences.

SECOS (Secure EPM Communications System): successful long-standing partnership

The SECOS waveform allows quick frequency hopping combined with highly effective encryption and was developed as part of a long-standing collaboration with the German company Rohde & Schwarz. Various radios for tactical and stationary operations and for carrier-capable operation for air force units use secure radio communication with SECOS, thereby ensuring the interoperability of the services amongst each other in the VHF/UHF

frequency range. SECOS systems are installed in various aeroplane and helicopter models and in airborne warning and control systems (AWACS) made by different well-known manufacturers. They are likewise in use on board military frigates and in military air defence and are an excellent means of protecting unmanned aviation. SECOS is currently deployed successfully in countries on all continents.

Sources:
[1] Spiegel, 11 March 2012
[2] Computerworld, 17 December 2009

Company anniversary of Crypto AG

SIXTY YEARS OF MOVING FORWARD TOGETHER

Delight in innovation and consistency in values! For six decades, Crypto AG has relied on these two mainstays of its business philosophy to enable demanding customers to handle the most sensitive information reliably and securely. With this attitude, the company was instrumental in helping to shape a fascinating chapter in the history of information security.

by Rudolf Meier, Publicist

The year was 1952. Europe was still suffering from the after-effects of the war. Two huge political blocks faced off in mutual mistrust. A quick economic upturn was the only way to ease tensions. Diplomacy was truly global at this point and had taken on a peacekeeping function …

This same year the legendary Swedish encryption pioneer Boris Hagelin founded his company Crypto AG in the central Swiss town of Zug for the purpose of developing and producing encryption equipment. His timing was quite favourable, as time would tell. Politics was highly dynamic. No one wanted anymore war but tremendous efforts were needed to secure peace, particularly with regard to exchanging the right information at the right time. Countless information and communication channels were set up with an ever changing array of new technologies. But one principle continued to apply: diplomacy was impossible without secrecy! The same rule applied for all countries so all governments had to rely on tap-proof channels. Crypto AG had almost worldwide success in this market to provide protection against tapping.

Crypto AG became a company with a major focus on research and development because computers had become so widespread and global networking gave rise to a whole range of new information risks. Security always has to stay at least one step ahead of the threat. Soon the mechanical encryption units were replaced with digitalised, processor-controlled counterparts. Countless new applications were added as time went on. Crypto AG became a trendsetter, over decades, and remains one today. And many of the initial customers from the 1950s have remained loyal to the company just as long. Is this success attributable solely to technical expertise?

Ultimately always the same values

Security is probably a measurable quantity, at least in part. Without trust, however, it has no longevity in actual application. Behind every piece of equipment, every electronic process, there are reliable people who take responsibility for it. And in the case of information security, time is an additional vital factor. Under certain circumstances, data may have to be kept protected for an extremely long time (e.g. matters of state security). In other words, a mistake could become noticeable much later and inflict great damage.

When it comes to solutions for information security, customers and suppliers enter into a type of defined symbiosis with high expectations. Crypto AG can lay several crucial weights on its side of the scales. The company has never been engaged in an area other than the creation of information security, the purpose for which it was founded. It has remained independent in every respect, including not belonging to an international corporation. It is not committed to block thinking politically, ultimately because it is domiciled in neutral Switzerland. In keeping its security promise, Crypto AG has always applied the criterion of "no scaling". In other words, only the greatest possible (yet still practicable) scope was our guide. One could also interpret this attitude as stubbornness in a certain sense, which naturally excluded several categories of customers, for instance most private customers. Products from Crypto AG are also hardly suitable for the mass market because top information security always has to be implemented individually and specifically.

That said, whoever steps over the threshold at Crypto AG can bring the highest expectations with him, also with regard to confidentiality.

Just a short stopover

The company is geared to highly personal customer relations. The lack of major festivities in this anniversary year typifies this orientation. Customers who visit headquarters during the year will benefit from several additional amenities. And a richly illustrated anniversary book has been published to mark the 60-year history of the company. Besides documenting the special qualities of the company, it contains wonderful pictures highlighting the uniqueness of Switzerland as a country.

View of the Matterhorn, the most impressive landmark of Switzerland.

Tradition and modernism stand side by side in Zug.

The fountain in Lake Geneva.

Mathematic and statistical attack methods in cyber war

AGGREGATE DATA AS A NEW SECURITY PROBLEM

Normal everyday business, i.e. daily operation of ICT networks involving data traffic that is (allegedly) not particularly sensitive, is often viewed as unproblematic in terms of security. Nothing could be further from the truth, as scientists have proved quite impressively once again. Given the new attack methods, standby networks have no choice: they need constant protection at emergency level.

by Urs Kürzi, Customer Segment Manager

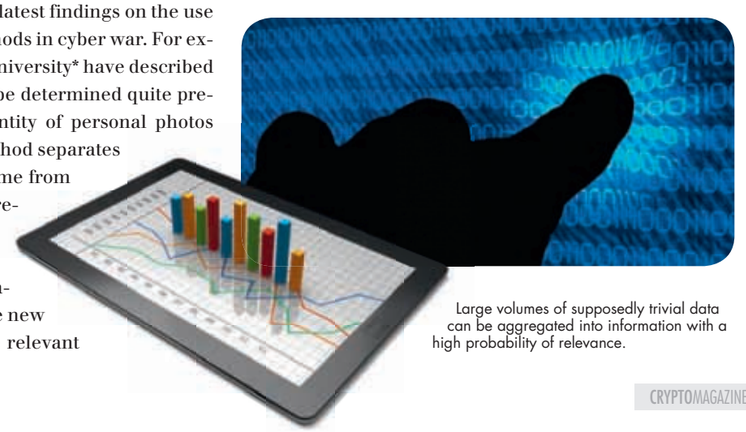
Contemporary ICT infrastructures must accommodate a broad spectrum of political, diplomatic, military, civilian, and business interests and ensure networking in normal everyday business. Operators are often mainly worried about the uninterrupted growth in demands with respect to bandwidth and information management. After all, availability problems are always unpleasant because they are felt immediately. Gaps in security are just the opposite. They are not noticed until damage has already been done, usually irreparable damage. The myth that enormous transmission capacity in itself affords a degree of security is a purely erroneous belief. Not a single byte can hide in the crowd, even with a data throughput of 10 gigabits per second. Each data packet, no matter how quickly it is sent, has a destination address and a source address following precisely defined structures (frames) and can be specifically filtered out regardless of where it is in the network. And to exacerbate the situation: the larger the data quantities, the more promising an attack will be on the data related to normal everyday business circulating in the network!

Intelligent data compression as a potential risk

Data can be tapped while being transmitted. This is a known fact. However, capabilities exist today that many operators and users of ICT infrastructures cannot even imagine. For instance, clever analysis algorithms can be used to extrapolate valuable single pieces of information from streams of huge data sets thought to be of little relevance. These operators and users can only be encouraged to take a closer look at the latest findings on the use of mathematical-statistical methods in cyber war. For example, researchers at Cornell University* have described how a person's hometown can be determined quite precisely drawing on a large quantity of personal photos from different places. Their method separates the photos a person takes at home from the rest of them. With the researchers' mathematical-statistical method, data existing for a person, a place or an organisation can be used to generate new data that is highly likely to be relevant and that might be extremely valuable. Applied to ICT infrastructures, this means that even in the normal everyday business of the standby network the data has to be encrypted first before being exchanged along the transport path. Otherwise, it is all too easy for operational pictures to be ascribed with great probability or "calculated" profiles to be created. The method involved here is both fascinating and dangerous. It shows that data with low classification can suddenly gain strategic value.

The bottom line is that the traditional Tolstoy scenarios have more or less become obsolete. The difference between standby and emergency, civilian and military command and control models is increasingly small regarding the relevance of a consistent security philosophy! The European Union has described security as something that requires continuous attention and that makes constant action necessary. It is nearly impossible nowadays to object seriously to this view.

Source:
* Press text, 22 February 2012, Algorithms can guess hometown from stream of photos



Large volumes of supposedly trivial data can be aggregated into information with a high probability of relevance.

Crypto AG at the DSA in Malaysia and at the FIDAE in Chile

PRESENT ACROSS THE GLOBE

There is no better place than international trade exhibitions to forge new business ties and cultivate existing, sometimes long-standing ones. This truism was confirmed once again by the participation of Crypto AG in the DSA and the FIDAE. In any case, our two on-site representatives returned to Steinhausen enthusiastic about their impressions and the many good personal conversations they had had.

by Josef Borner, Senior Vice President, Head of Strategic Business Development, and Heiner Düringer, Senior Vice President, Head of Marketing and Sales

As we all know, visitors to trade exhibitions arrive with three objectives: 1. Networking, 2. Networking and 3. Networking. The DSA and the FIDAE are both highly typical in this regard. The visitors from around the globe include individuals from the widest variety of business areas and government organisations: defence ministers, military attachés, arms purchasers, staff from government administration agencies and the secret service, technical supervisors, system integrators, officials responsible for e-government services and engineers of all kinds. Of course this list is not complete but it does show the enormous contact potential for conducting exciting, informative and promising personal conversations that subject-specific trade exhibitions offer.

Of course the contacts mostly relate to technical topics. One often sees familiar faces and long-standing customers, however, so there is ample opportunity for personal exchanges, too. In a casual atmosphere over a cup of tea, coffee and Swiss chocolate, people can discuss ongoing projects and conjure up new ones or are perhaps even so far along that they can define concrete details. It is enormously important and exciting for us to find out what needs our customers have at an early stage. Practical needs change in the ICT sector almost more quickly than anywhere else, especially in areas where comprehensive ICT security is paramount. Along with the classic tasks of the secure processing, saving and transfer of sensitive data, new and important sub-aspects constantly arise under the banner of globalisation.

CHILE

The trend towards fully integrated security solutions

System integrators are one visitor segment with which we cultivate extremely close ties. Practically every ICT infrastructure – no matter what the size – is globally connected, resulting in a constant increase in the diversity and complexity of individual areas, topologies, applications and user requirements. An enormous amount of specific technical expertise is needed to achieve a smooth interplay of all the necessary components and functions. Both sides are therefore keenly interested in the exchange of know-how between ICT integrators and our security experts on the latest trends.

Swiss Ambassador Yvonne Baumann officially opening the Swiss Pavilion together with Chilean Defence Minister Andrés Allamand Zavala.

It was striking how often total office integration was the main topic of conversation at both trade exhibitions. If a phone, fax and PC are on a desk today, the obvious tendency is to integrate these user-oriented devices directly into a single network. This task is simple today with IP, but it is important to keep in mind that different network technologies are used to communicate with the widest variety of communication partners throughout the world. Not just fixed-line networks or the Internet, but also mobile networks, radio links and satellite links. If all these options are to be used, they must be brought up to a uniformly high standard of information security. Security implementation is a joint task for system integrator and security supplier because ICT components and terminals from different manufacturers are involved. The ideal situation is to have the interested customer also sitting at the table at the trade exhibition. The earlier the crucial points of a comprehensively secure ICT infrastructure can be recognised and jointly defined (at least in terms of perspective), the quicker a concrete project can later be set up.


ASIAN DEFENCE JOURNAL

ADJ Today

Issue #3

DSA 2012

Wednesday, April 18, 2012

The Official Show Daily

Crypto's Voice Encryption System

Security Applications

Key Features

Article on the Voice Encryption System from Crypto AG in the exhibition journal of the DSA Malaysia.

DSA – Defence Services Asia

The DSA took place for the thirteenth time at Putra World Trade Centre in Kuala Lumpur, Malaysia, from 16 to 19 April 2012. The DSA attracts about 850 exhibitors from around the globe, making it the largest military exhibition in Southeast Asia. A Rafale fighter and various armoured vehicles covering the entire gamut of sizes and features were among the many attractions visitors could marvel at on the 40,000 square metre fairground. The trade exhibition was hosted by the Malaysian government and officially opened by its representative His Excellency Minister Dato'Seri Zahid bin Hamidi.

A unique aspect of the DSA, which is staged every two years, is that attendance is by invitation only. This exclusivity ensures that nearly all visitors to the DSA (about 27,000 this year) have great technical expertise. For example, 324 VIP delegations from 41 nations were present. It is self-evident that representatives of the armed forces make up the largest portion of visitors.

The Crypto AG stand was in the Swiss Pavilion and enjoyed a large and steady stream of visitors throughout the trade exhibition. One reason for this popularity may have been the two Alpine horn players, who occasionally filled the air with genuinely Swiss music (attracting clusters of people). Of course, they were dressed in proper style in blue-and-white embroidered edelweiss shirts. It was easy for them to create a pleasant atmosphere for large numbers of visitors, who then rewarded these efforts by staying longer at the stand as guests.

Of course, business did not get short shrift in the process. The products presented included the Mobile Client HC-7835, the unit from the MultiCom Radio Encryption Family HC-2650 and HC-2605 that has proved itself thousands of times in actual practice, and the all-purpose Desktop Unit HC-9300. Of course, all products were integrated in a typical reference scenario. Keen interest was shown in the handy new HC-2605 terminal designed for the most rugged use. More than one visitor said this or words to this effect about the terminal: "a miracle of miniaturisation and so convenient to operate." We were naturally pleased to hear that we are keeping up with the current trend in terms of the shape of our units.

FIDAE – Feria Internacional del Aire y del Espacio

The staging of our appearance at the FIDAE, held in Santiago de Chile from 27 March to 1 April 2012, was no less interesting, exciting and impressive. The FIDAE is a classic aeronautics and space exhibition with a correspondingly impressive atmosphere. Over 530 companies from 40 countries accepted the invitation to the seventeenth FIDAE and presented themselves at the most important Latin American trade exhibition of all. The new Boeing 787 Dreamliner, the Airbus A400M and the Airbus 380 were special highlights. And of course the line-up included spectacular demonstrations by fighter jets. The FIDAE is the fifth largest trade fair of its kind.

Crypto AG participated for the third time. We gave in to our enthusiasm and fascination during our five-day stay at the trade fair. Emotions are one thing, measurable successes are another. We also generated a number of leads and accepted numerous requests for offers.

The first highlight in the Swiss Pavilion was the official opening by Swiss Ambassador Yvonne Baumann together with Chilean Defence Minister Andrés Allamand Zavala.

Josef Borner talking with an interested fairgoer at the DSA.

Our stand had an optimum strategic position, allowing us to witness these festivities first-hand. Our (new) stand was also a pearl in all other ways. It impressed not only us but our visitors and guests as well. The half-high glass panels were an elegant touch. The sitting areas behind them offered an absolutely discreet place for conversations about sensitive topics such as concrete projects. We can report with pride that high-ranking individuals enjoyed staying a few minutes longer at our stand and were taken with our products. In addition, we were able to greet a number of regular customers and other prospective clients from Argentina, Ecuador and Brazil, among other countries.

The starting points were usually our system presentations with functional systems such as secure voice solutions and secure messaging. The crucial aspect is always to give prospective clients a hands-on experience and let them test the systems themselves. Of course the stand was more elaborate and expensive to set up as a result, but that extra effort definitely paid off.

It was the HC-9100, the latest addition to our product line, that attracted the most attention, however. It is probably the tiniest of all complete encryption units in existence and comes in the form of a microSD card. It is a technical miracle that sparks genuine enthusiasm. The simple mode of operation (installed in a Nokia GSM phone) and the quick switchover from plaintext to encrypted mobile communication (and back) are two of its features of great significance for potential users. Another striking plus was that no further functions of the GSM network provider are needed to encrypt the connection. The user remains autonomous thanks to his own individual IP call manager.

Our pleasant conclusion is that our participation even in far-away exhibitions and trade fairs is worthwhile as long as we make the right choice and tailor our approaches to the target audience. Personal networking is still always more valuable than any e-mail or phone call! ■

The structural plan for the Information Society

ETHERNET: AN ON-GOING SUCCESS STORY

Ethernet technology plays a leading role in global networking. With its rapid development since the 1970s, it also offers a lesson about modern industrial history. Those who spend some time learning about the essence of Ethernet could well derive even more advantages from it for their own applications in future.

by Rudolf Meier, Publicist

The global Information Society is not even 20 years old, but we have already been taking it for granted for a long time. You pick up a laptop or a modern smart phone and all of a sudden you have access to billions of pieces of data and information, websites and network services. For many people, this all-present communication has existed for more than half their lives. It is no wonder that revolutions of various kinds are now being sparked on the basis of this technical capability.

The astounding part of this success story is that basically everyone is familiar with the latest user devices and their features but only a handful of people are aware of what complex and literally global network infrastructure has to be available for them behind the scenes. All modern applications up to and including social networks or cloud computing can only function if the global network is uniform, efficient and accessible. So what drives advances more: the cool devices or the networks with their gigantic bandwidth growth?!

Ethernet as a school subject

Anyone with even a small interest in network technology will soon hit upon Ethernet. It is the most widespread protocol today for information and communication networks. Because Ethernet is so dominant, it is already part of the primary school curriculum in several countries. That certainly cannot hurt. After all, it will continue to shape our future for a long time to come. And future here includes both benefits and risks!

At the same time, Ethernet is a lesson on industrial history. From the most modest beginnings, Ethernet went through a bottom-to-top process to grow into a vast, powerful infrastructure to which the entire world is hooked up today. All that people were looking for back then (around 1973) was local wire networking of computers and printers so every device would be compatible with every other one, as with radio networks. Just like radio waves use free space, all participants were to be connected simultaneously. In philosophy "ether" refers to primordial matter and in physics to the space in which radio waves are propagated. Based on this thinking, the American inventors Robert Metcalfe and David Boggs selected the term "ether" and added "net" to it.

In other words, Ethernet was initially a purely LAN technology. Computers and peripheral equipment were spreading at such a phenomenal rate, however, that network technologies also underwent rapid further development.

The basic idea lives on

Ethernet is a packet-based (or packet-transmitted) digital technology; only digital signals (bytes) are sent. The bytes are put in a cyclical standardised sequence for sending so the sender and recipient can operate synchronously. The standardised unit in Ethernet is called a frame (referred to in IP as packet). Frames are functionally divided within themselves because control information is needed along with the payload while the transmission is underway in the network.

This frame construction was quickly refined as development work proceeded and it became the key factor for success. This turn of events was by no means a matter of course, because all additions had to be accepted by manufacturers and standardised by the IEEE, the Institute of Electrical and Electronics Engineers. Additional areas were successfully incorporated into the frames to enable active network components to perform various programmed tasks. For instance, rerouting, checking, selecting and prioritising. A modern Ethernet network today is an intelligent organism.

By way of comparison, the Internet Protocol IP relied on a much more complicated approach, which in exchange opened up many more ways of handling demanding transmission tasks. This trait also suggests why the two programs soon found each other in an optimum combination known as IP over Ethernet.

Data transport: direct or nested?

But how can media content such as e-mail, video or phone be transported with Ethernet technology? The packet principle enables any digital information to be taken along in byte form, in other words regardless of what was digitally coded. This feature allows (at least) two tasks to be performed:

- Direct transport of payload: The frames are loaded with directly usable data (e.g. numbers, text, images) that can be used as such by the recipient.
- Nested protocol data transport: Data packets of another protocol are incorporated in the frames and can contain complex applications. In the case of IP over Ethernet (IPoE), these packets are IP packets, which in turn have payloads but regulate their own use themselves with higher-level program instructions.

In the former case, Ethernet becomes a simple but efficient data transport channel, as used in the form of global backbones. The paths the Ethernet frames take between senders and recipients are controlled solely by the frames (in tandem with intelligent network components such as switches and routers). Thanks to this capability, network providers can offer their customers numerous individual services (whose designations are not always entirely logical or comprehensible …).

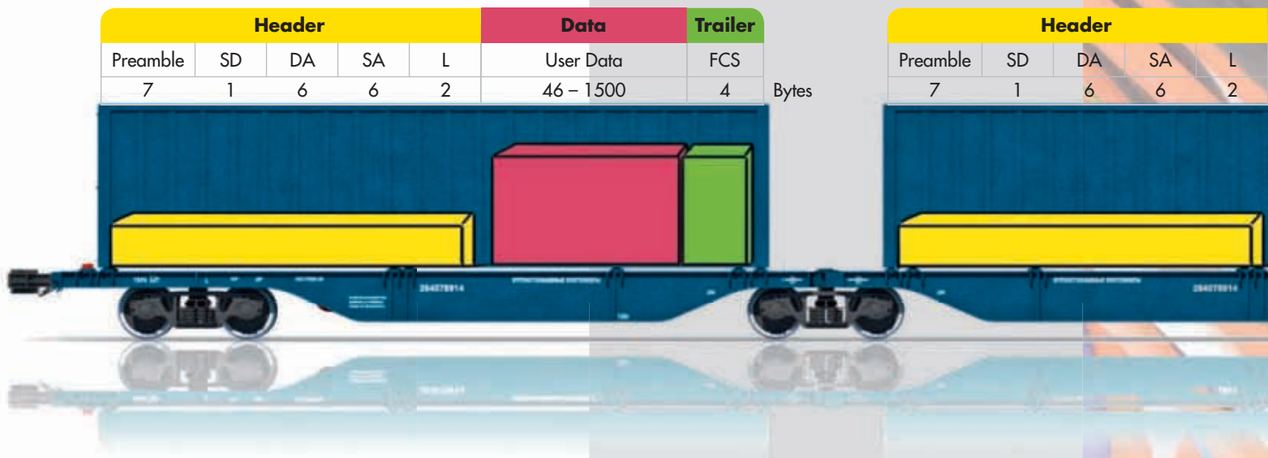
In protocol data transport, the IP information can be applied additionally for highly complex control tasks at higher layers of the OSI model. IP together with Ethernet allows universal use of products and services (applications) and a fine division of data streams all the way to the end users. The apps found in smart phones for example would be impossible without this principle.

From LAN to WAN

The switchover from copper wire as an electric conductor to optical fibres with fibre-optic transmission was one factor that contributed to the rapid development of Ethernet. Low-loss fibres and high-quality laser technologies had to be developed before this could happen, however. A single fibre with a core diameter of 10 µM can transmit much more data than a copper wire. If several fibres are bundled into a single cable, the result is a reasonably priced transmission channel that delivers incredible performance. In earlier times, optical signals had to be refreshed after being transmitted just a few hundred metres. Now they do not need refreshing until after about 100 kilometres. This means even deep-sea optic-fibre cables can now be laid provided they have built-in repeaters.

A PC as a window to the world …

Our office computers are generally still connected to an Ethernet cable. But whole new dimensions of Ethernet also come into play if for example we send an e-mail to a recipient on another continent. What is most amazing is that we are constantly offered greater performance at lower prices. This has to do with the success of Ethernet. The world is flooded with cheaply produced Ethernet components and competition among manufacturers keeps the pace of development fast. We can therefore continue to look forward to new applications and even greater user convenience. ■



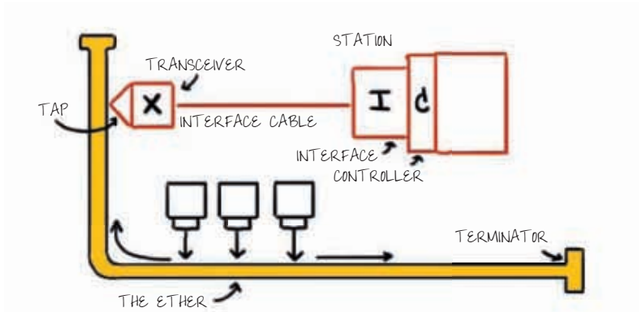
ETHERNET FRAME: SIMPLE PRINCIPLE – ENORMOUS POTENTIAL

Each stream of digital data must be cyclically structured in some way in order to transmit data in a meaningful manner. In Ethernet this structure is created with separate divided units (frames, data packets). Ethernet operates according to the traditional "postal principle": it needs a source address and a destination address (placed in the header), space for payload (data) and additionally a final check (due to the huge data volumes) (trailer) to confirm that everything was transmitted correctly. The position and length of the functional bytes are stipulated (simplified depiction):

- **Preamble:** Announces that a new unit begins
- **SD:** Start frame delimiter/network synchronisation
- **DA:** Destination address
- **SA:** Source address
- **L:** Length or identification of the standardised Ethernet type
- **User data:** The actual payload for transmission – e.g. IP data packets used to send many modern applications all the way to the end users (VoIP, messaging, phone apps, etc.)
- **FCS:** Frame check sequence: the actual final signal in the frame and the calculation check as to whether the correct number of bytes was transmitted.

Supplementary fields can be put in the header to meet numerous other user requirements for complex functions at higher layers of the OSI model. The standards based upon IEEE 802.3 are authoritative in this regard. They also play an important part in encryption measures.

Robert Metcalfe and the fundamental concept of the original Ethernet.



HAGELIN-CRYPTOS
CRYPTO AG

CRYPTO AG – TO REMAIN SOVEREIGN

Crypto AG, Headquarters

Crypto AG
P.O. Box 460
CH-6301 Zug
Switzerland
Tel. +41 41 749 77 22
Fax +41 41 741 22 72
crypto@crypto.ch
www.crypto.ch

Crypto AG, Regional Offices

Abidjan
Crypto AG
01 B.P. 5852
Abidjan 01
Ivory Coast
Tel. +225 22 41 17 71
Fax +225 22 41 17 73

Abu Dhabi
Crypto AG – Abu Dhabi
P.O. Box 41076
Abu Dhabi
United Arab Emirates
Tel. +971 2 64 22 228
Fax +971 2 64 22 118

Buenos Aires
Crypto AG
Maipu 1256 PB «A»
1006 Buenos Aires
Argentina
Tel. +54 11 4312 1812
Fax +54 11 4312 1812

Kuala Lumpur
Crypto AG
Regional Office Pacific Asia
Level 9B Wisma E&C
2, Lorong Dungun Kiri
Damansara Heights
50490 Kuala Lumpur
Malaysia
Tel. +60 3 2080 2150
Fax +60 3 2080 2140

Muscat
Crypto AG
Regional Office
P.O. Box 2911
Seeb PC 111
Sultanate of Oman
Tel. +968 2449 4966
Fax +968 2449 8929

A member of
The Crypto Group