DGT Cyber Protector

The threat of cyberattack

The Cyberwar is an element of today's reality. It aims to inflict the greatest possible damage with the help of the latest technology. It causes intentional disruption of interactive, organized information flow in the cyberspace. It is carried out especially in the relation to the infrastructure of significant importance for the economy and the country defense and is aimed at paralyzing communication and thus decision-making processes in critical situations.

Every IT system has been or will be attacked - the only question is - when?

According to reports of the Ministry of the Interior and Administration, prepared on the basis of the information of the Police Headquarters, the Internal Security Agency, the Customs Service, the Ministry of Digitization and the Ministry of Justice, cyber attacks are increasingly outsourced by foreign governments. It must be assumed that the attacks on ICT systems operating in institutions responsible for country's security are inevitable.

Unique feature of DGT Cyber Protector

Modern ICT solutions are based almost entirely on the IP infrastructure. All forms of protection, such as a firewall or a session border controller protect the IP infrastructure more or less effectively, but never entirely. It is due to the fact that today no one can ensure 100% network security when every now and then new vulnerabilities are being discovered and new forms of attack are being used.

With DGT Cyber Protector we took a different approach. Our long-time experience in critical communications shows that in order to be in control of the situation one factor must be maintained regardless of everything else - the voice communication. The commanding officer can loose access to all functionalities of modern systems, eg. digital maps, digital data, video stream etc. but as long he can communicate with others, he is able to effectively control the situation. This is what DGT Cyber Protector guarantees - the secure voice communication even in the event of a complete IP network paralysis.
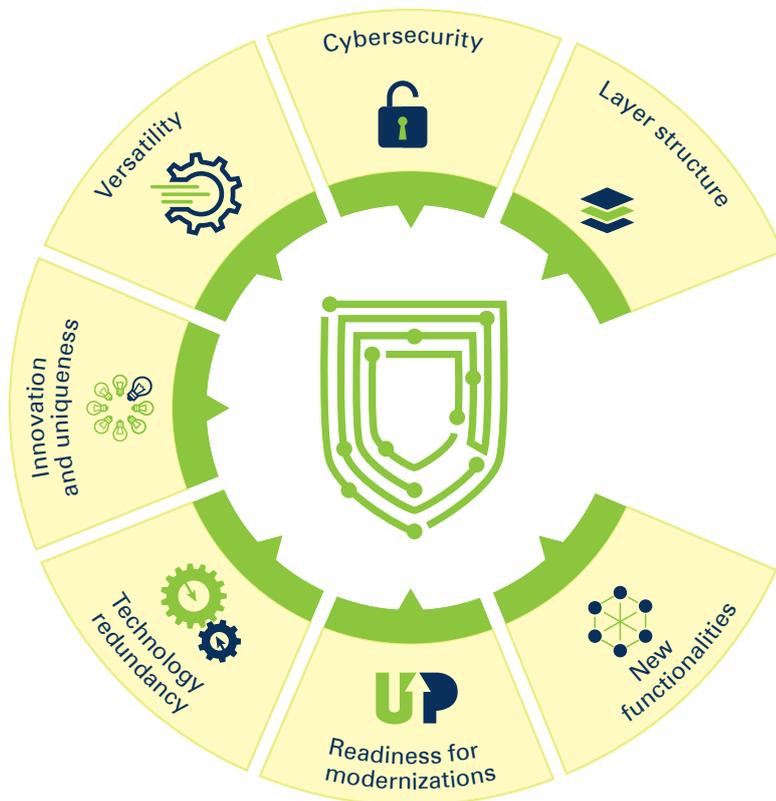
Versatility
Each DGT's system can be upgraded to support the solution DGT Cyber Protector. The modernization has been prepared in a way that the user can keep the majority of the existing infrastructure. Thanks to that the cost of modernization is significantly reduced.

Innovation and uniqueness
Nobody can talk about ensuring total security in terms of new, unknown attacks. They still reveal more gaps in the IP layer. DGT Cyber Protector, in addition to protecting the IP layer, is also equipped with a layer separated from the IP. Blocking or infecting of that layer via cyber attack is impossible.

Cybersecurity
Cyberthreats, although they are growing at a rapid pace, are still neglected by many users. The scale of the threat is so serious that every system (including systems that work in the area of critical infrastructure) can be successfully attacked. DGT Cyber Protector guarantees critical voice communication even in the face of a successful cyber attack.

Layer structure
The IP layer is protected in accordance with best practices. Despite this, it should be assumed that its infection or blocking is possible. Therefore, the DGT Cyber Protector uses a layer separated from others, made in a different technology. This layer can work - guaranteeing critical connectivity - completely autonomously, even after complete disconnection / blocking of the IP layer.

Technology redundancy
DGT systems use IP technology to implement many services and functionalities. Thanks to the appropriate system architecture, available in the DGT Cyber Protektor solution, we can talk about technology redundancy. At the time when IP technology fails, the second technology allows you to maintain the continuity of voice communication.

Readiness for modernizations
DGT Cyber Protector was developed in a way to expand a system that will allow the use of future technologies while maintaining security critical communication.

New functionalities
The DGT Cyber Protektor is also modern,so far unavailable for many users, functionalities in the field of unified communication (UC), e.g. video call, connections via a web browser and many more. It is possible thanks to the reconstruction of system and equipping it with newest hardware and software.