TECHNICAL SOLUTION PROPOSAL **Reference:** **B2014-023**

Title: Safety-critical system with additional safety mechanism

Corporate entity: Diehl BGT Defence GmbH & Co. KG

Introduction

The present invention relates to a safety-critical system comprising at least two physically separate, interconnected units, with at least one additional security mechanism for protection against unlawful access and against manipulation by unauthorised third parties.

Problem

The accessibility and network availability of vulnerable targets, such as safety-critical weapon systems, is increasing. At the same time, an increasing number of security gaps have recently been discovered in introduced weapon systems. Such gaps are usually difficult to remedy retrospectively and require a great deal of effort, especially in terms of time and money. Attacks on increasingly digitalised security-critical systems with or without radio-linked networks can therefore not be ruled out, so that electronic penetration into IT-based infrastructure systems and individual operational systems represents a thoroughly realistic threat. The main focus must therefore be on secure communication between the individual physically separated units of a system. Manipulation or unauthorised access by third parties can cause particularly high damage here. A fundamental need for security precautions for safety-critical, especially military systems is therefore self-explanatory. The security mechanism according to the present invention is intended to reduce the effort required to eliminate existing security vulnerabilities and at the same time increase the overall security of the system. The focus is on secure data exchange between the individual physically separated units of the safety-critical system.

Previous approaches to solutions

One option for protection against cyber attacks is the use of hardware-based encryption devices. Organisational security, in particular physical access to interfaces and controls of a safety-critical system or, in the case of a weapons system, to a tactical operations centre, can be accomplished through physical access controls. Both measures (IT security, organisational) already provide a certain degree of protection.

Another time-consuming and cost-intensive solution to increase the safety of a safety-critical system is to change software in one or more of the physically separated units of the safety-critical system and to integrate new interfaces and/or safety mechanisms there.

Solution/implementation

The technical solution of the invention provides for at least one configurable hardware proxy to be connected upstream at an interface of one of the physically separated units of the safety-critical system. Cleverly, such a proxy is connected upstream of each interface of a physically separated unit. This makes it unnecessary to change the software of the physically separated units. Instead, the proxy, which is integrated in additional hardware, takes over the implementation of the remote station with the additional or new safety mechanism as well as the conversion to the existing interface of the one physically separated unit.

Physically, the at least one proxy is located on one of the physically separated units. The proxy thus separates the new/additional safety mechanism from the existing safety-critical system. The independent hardware component "proxy" makes it possible to promptly implement additional safety mechanisms on one's own hardware and/or new interfaces without having to intervene in the hardware and software of the existing safety-critical system.

The proxy can be designed as a SoC (System on a Chip) with preferably ARM processors and possibly additional FPGA hardware. Such a design of a proxy is characterised by low energy requirements and high performance at the same time and advantageously allows booting from an SD card or a USB stick. For the exchange of software or implementation of a new or additional security mechanism, it is thus sufficient to exchange the SD card or the USB stick, which can also include the proxy software in addition to the operating system of the SoC.

For a simple bridge configuration of a proxy designed as a SoC, two Ethernet interfaces should be available. According to the OSI definition, the bridge connects subnets protocol-wise on layer 2 (LLC, IEEE 802.2) or 2a (MAC layer) of the OSI reference model. Due to this configuration, the SoC or the proxy does not have its own IP address and therefore cannot be attacked via Ethernet in principle. In particular, a configuration as a transparent bridge prevents the proxy from being attacked via the existing infrastructure of the safety-critical system. This is because a transparent bridge learns both which MAC addresses are in which subnet and possible recipients by entering the senders of packets in the individual subnets into an internal forwarding table. Based on this information, the bridge can determine the route to the recipient. The sender addresses are constantly updated in order to detect changes immediately. The advantage of the transparent bridge lies, among other things, in the fact that the presence of the proxy acting as a bridge cannot be functionally detected from the outside, since no functional change of the "overall" system is visible there - as mentioned before - the proxy also has no IP address of its own and thus also offers no attack surface, since it cannot therefore be addressed itself. Although it is theoretically possible to detect the presence of a proxy via secondary secondary effects outside the functionality space of the "overall" system, since the presence of a proxy leads to a slight delay in the runtime of the IP packets. However, this does not impair the functionality of the "overall" system.

"system, since the IP protocol does not define or require fixed propagation times, nor are any propagation delays caused by other effects clearly distinguishable from propagation delays caused by "proxies". Furthermore, a proxy in a transparent bridge configuration does not increase the so-called hop count of the IP packets, which would otherwise give a bridge

away.

Functionality

Of interest for the use of such a proxy are generally safety-critical systems, but especially military systems, which consist of at least two physically separate units that are connected to each other. These two units can be, for example, an active or reconnaissance system and a control or ground station, which are uni- or bidirectionally connected to each other. The preferred transmission paths are Ethernet or data links such as TCP/IP (Transmission Control Protocol/Internet Protocol) or UDP (User Datagram Protocol). The identification of the physically separated units or computers participating in the network is done via IP addresses. A computer or generally a device with an IP address is called a host in TCP/IP jargon. The mode of operation of the subject matter of the invention will be explained schematically in the following.

Legend

A	=	Active or reconnaissance system (e.g. launcher, drone)
B	=	Connection (Ethernet or data link, e.g. TCP/IP/UDP), uni- or bidirectional
C	=	Control or ground station
D	=	Proxy implemented in hardware and connected as a bridge
´	=	Change

State of the art

In the previously known prior art, A and C are connected to each other via B. Access to A or C is not restricted in this case.

If additional security mechanisms, such as encryption or authentication, are subsequently introduced to restrict or secure access from A, changes have been made to A up to now.

Case a) Use of a proxy

The proposal now is not to change A, but to proceed as follows:

Component A remains unchanged. The proxy D1 is inserted into the connection B and is located at A. The proxy D1 implements the new interface or the new security mechanism towards side C and implements this towards side A on the existing interface to the A side. In addition to proxy D1, the new interface is also integrated into C, which is therefore referred to as C'.bezeichnet wird.

Case b) Use of a second proxy

In this case, C also remains unchanged, because a second proxy D2 takes over the new interface. This case makes sense if only route B is distrusted.

In all cases, D is designed as a bridge, thus does not have its own IP address and cannot be attacked via B in principle. However, D can preferably have an additional interface that is not accessible via B. It makes sense, for example, to have an SD card or a USB stick via which it can be dynamically configured (software changes, key for authentication).

Application examples

Example 1

In the first example, an existing GBAD system (Ground Based Air Defence), consisting of a weapon system, such as a truck with launcher and weapon computer, is connected to the remote control station via Ethernet. The control station is a standard PC and can also be networked with other systems such as FüWES (command and weapon engagement system) or reconnaissance systems/radar. The software of the effect system with its defined command interface has already been introduced and approved. However, it cannot be ruled out that the command interface is also known in detail to third parties. Since the software of the existing control station, for example, has been identified as potentially insecure, the command interface to the control system is to be extended by additional authentication mechanisms (e.g. special launch code). For this purpose, it is no longer necessary to change the software and/or interface of the control system, because the change and implementation of the command interface can now take place via the hardware proxy. It is sufficient to exchange an SD card or a USB stick. These data carriers can also contain current security keys. The hardware proxy is physically located near the launcher or near the weapon computer and is simply interposed as a bridge in the existing Ethernet connection.

Example 2

In the second example, a drone is commanded via a data link from a remote ground station. This link is extended with additional or modified encryption or undergoes a format change. In this case, the drone is simply equipped with the proxy, which is not a major limitation due to its low power requirements and weight. The new encryption conversion is taken over by the proxy, which converts to the existing interface on the side of the drone.