New approach to industrial security offers also potential savings

Stein J[1], Weitz M[1], Schmid A[1]

1 Institute for Occupational Safety and Health of the
German Social Accident Insurance
Deutsche Gesetzliche Unfallversicherung e.V. (DGUV)

KEYWORDS: Industrial Security, Security, Safety, Industrial Control Systems, Controller Security Management, Remote Access, Network, Sustainability

ABSTRACT

In a survey conducted by the IFA, the extent to which the networking of control systems in companies has already progressed was investigated. The focus was on the networking of devices which, if compromised, could injure, or even kill people. A closer look revealed that a significant number of control systems are capable of injuring and killing employees if attackers manage to take over the respective control system via the Internet and control it maliciously.

The results of the study reflect the headlines in the news about current attacks on industrial control systems and show that networks in industrial environments urgently need to be designed more securely. This poses major challenges, especially for small and medium-sized companies, which often only have a very small IT team. The Industrial Security Laboratory at the Institute for Occupational Safety and Health has therefore developed a modular concept with which companies can make their production network significantly more secure with little effort.

An easy-to-implement concept shows how predictive maintenance can be safely implemented in an industrial environment. In addition, a model factory was set up to test a secure tunnel for industrial protocols. The tunnel can protect connections that have an extraordinarily high level of reliability thanks to the redundant use of WIFI and 5G. In future, it will be possible to remotely control construction machinery, for example, which is dependent on both a secure and reliable data connection.

The decisive factor for companies here is the practical feasibility and low resource consumption. Even embedded systems with low computing power can use the secure tunnel. In addition to the technical solutions, the concept is rounded off by organizational measures that guarantee rapid accessibility in the event of an IT security incident. A short film and an information platform were created for this purpose, with which all companies can create an emergency contact in just 5 minutes with which they can be reached immediately by authorities and security researchers worldwide.

1 INTRODUCTION

An increasing number of industrial control systems are being networked in industry. Security gaps in these complex systems can be attacked at any time [1].

While IT security gaps in companies have so far often enabled data theft and caused financial losses, compromised industrial control systems can also injure or kill people. An attack on a German steelwork, for example, meant that a blast furnace could no longer be controlled [2]. What in this case led to significant damage to the blast furnace also poses a considerable risk to a plant's employees. This and other recent examples illustrate how important security is for networked control systems.

The continuous improvement of databases on vulnerabilities has documented that critical vulnerabilities can very often be found not only in classic desktop applications, but also in industrial control systems [3]. In contrast, little data exists on current networking in industry. However, this information is crucial for an up-to-date picture of the situation, because a vulnerability can only be exploited if it is also accessible via an interface [4]. It seems plausible that the large number of vulnerabilities in control systems have hardly been exploited in the past because they were not accessible due to a lack of networking. Data on this is to be collected via a survey.

There is also a lack of reliable data on the frequency of successful attacks on industrial control systems. This is due to the fact that there are no data records of many attacks. Without IT forensic analysis, the attack on a vulnerability often cannot be detected and can be prematurely assessed as a component failure. If companies recognize an attack on a vulnerability, this event is often kept secret. As a result, very few attacks become public. Stuxnet, Trisis and a successful attack on the control system in a German steelworks in 2014 gained particular notoriety [1].

An analysis of industrial cranes showed that many radio remote controls send their control commands unprotected and an attack from a distance is often trivial [5].
The survey revealed that SMEs currently do not have sufficient resources for security measures in their operations. It is often even unclear who in the company deals with security issues. On the other hand, resources are often available for projects to improve sustainability. This project therefore looked for a solution that could not only improve security in the company, but was also sustainable.

From a manufacturer's perspective, the challenge is that industrial controllers often have little memory and processors with very low computing power.
In summary, it is crucial to protect the communication between the interfaces. The solution must be suitable for low-performance embedded systems and resources must be saved.

2 Data collection and setup of a prototype

The first step was to determine the current degree of networking and the potential risks within the companies. To this end, the IFA conducted a survey of 98 occupational safety specialists from various German companies.
The aim of the survey was to determine whether people could be harmed if all functions of the networked devices were maliciously remote-controlled by an IT attack. The protective measures already in place were not to be considered.

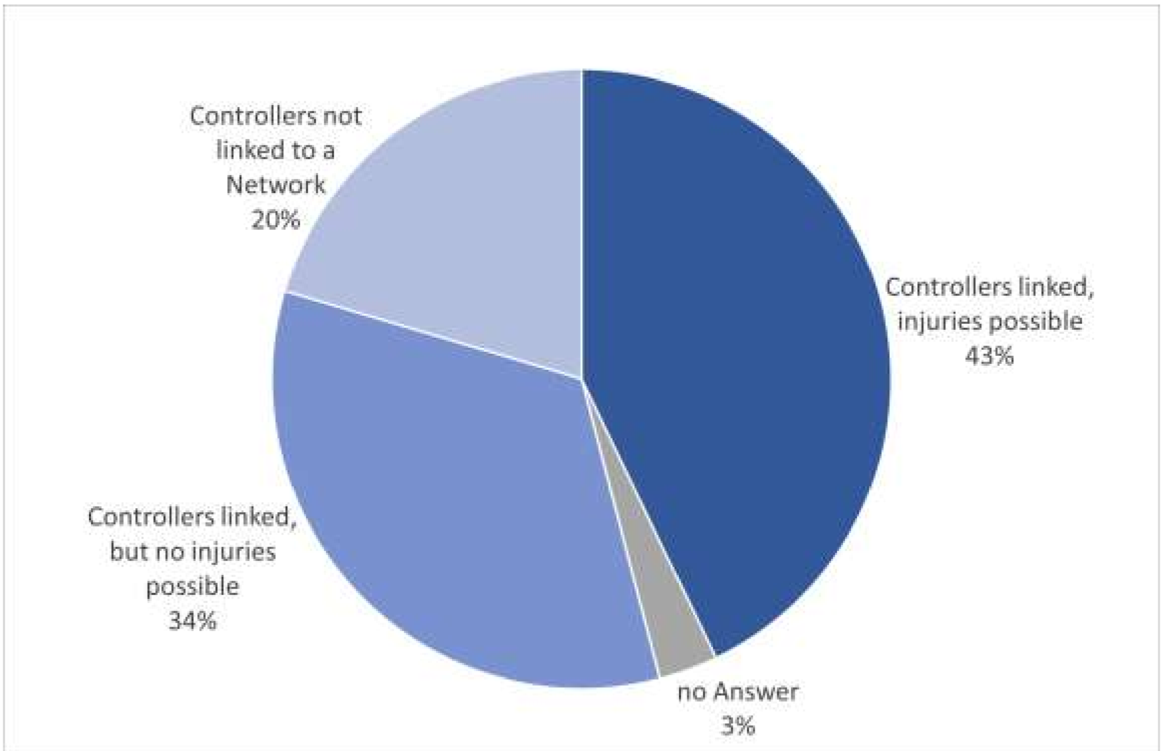

Figure 1: Survey on the current degree of networking and potential hazards in industry. Of 98 occupational safety specialists from various companies surveyed, 20% stated that there are currently no networked control systems in their own company. 34% of those surveyed stated that there is networking, but that the machines and systems are inherently safe and that employees cannot be injured even if the control system is corrupted. 43% of respondents have networked control systems in operation that can injure people if security gaps are exploited.

A typical protection of network connections is the use of a VPN tunnel. However, many VPN solutions cannot be used in industrial networks due to their high resource consumption and high latency. The very new VPN called Wireguard advertises itself as having fewer functions with only around 4,000 lines of code, but with significantly lower resource consumption, lower latencies and higher data throughput [6].

Industrial protocols are very sensitive to lost or delayed network packets. Even a delay of a few milliseconds or the loss of 3 packets can cause a control system to stop operating and be set to a safe state.
The IFA's Industrial Security Laboratory therefore investigated whether Wireguard is capable of providing a stable VPN tunnel for ProfiSAFE on an embedded system.

To this end, two gateway systems were set up to transmit the data packets from two industrial controllers with security functions via a Wireguard tunnel.

Tests were carried out both via a wired network and via wireless networks. Because the Wireguard Tunnel transmits its encrypted data via UDP, multiple connections could also be used redundantly.
One possible application would be to establish a connection via both WIFI and 5G for the remote control of construction vehicles. As long as one of the two radio connections is available in sufficient quality, the connection remains stable. The secure state is only initiated when both radio connections are lost.

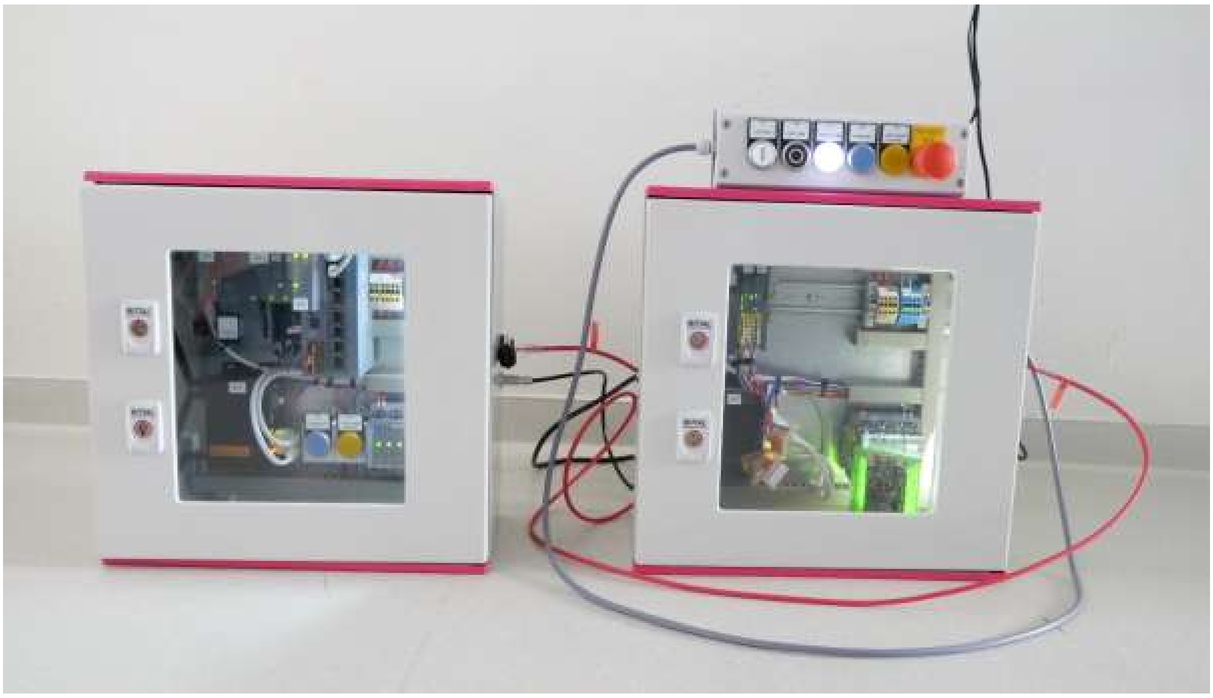

Figure 2: Evaluation of a Wireguard tunnel via two gateway systems for the transmission of safety-related data packets. A safety system controller in the left-hand control cabinet communicates with the components in the right-hand control cabinet via the wireguard tunnel [7].

Due to the comparatively short and free source code, Wireguard can be audited better than the very complex classic VPN solutions, which is particularly important in the industrial control environment.
By using free source code, improvements can be developed jointly and all users benefit from audits together. Because programmers correspond to around 10.5 tons of CO2 equivalent per year, this not only saves costs but also considerable amounts of CO2.

However, it is also crucial for the use of networked industrial components that manufacturers, operators, security researchers and authorities can communicate with each other quickly and effectively. To this end, both manufacturers and operators provide an emergency contact via which they can be reached for rapid communication on vulnerabilities. The study showed that the RFC 9116 specification is very promising. A short film was therefore produced for the companies' decision-makers. In addition, frequently asked questions from the companies were included in an FAQ [8].

6 REFERENCES

1. Stein J. *Angriffe auf vernetzte Industriesteuerungen*. DGUV Forum (2019) Nr. 12, S. 28-29
2. Federal Office for Information Security (BSI), The State of IT Security in Germany 2014
3. Catalog of publicly disclosed cybersecurity vulnerabilities https://www.cve.org/
4. Stein J. *Fernwartung von Industriesteuerungen* DGUV Forum (2021) Nr. 1, S. 24-27
5. Andersson J, et al *A Security Analysis of Radio Remote Controllers for Industrial Applications 2019*
6. *Donenfeld J. WireGuard: Next Generation Kernel Network Tunnel https://www.wireguard.com/papers/wireguard.pdf*
7. *Czimczik C, Weitz M. 2021: Sichere Industrienetzwerke mit Wireguard - final thesis for state-certified technicians, unpublished*
8. *Website about security.txt and RFC 9116 on https://cert.dguv.de/*