AMPEG

# AMPEG
## Security Level Management

Keep the attack surface small

## ZF Friedrichshafen AG

A new hub for the corporate security level management

*A Security Lighthouse Case Study*

## A new hub for the corporate security level management

**At ZF, AMPEG Security Lighthouse is a reliable instrument to test the security level of the entire company. At the same time, the system has proven to be an interactive platform for transmitting the respectively-applicable requirements of IT security. In addition, the individual security teams use this tool as a basis for planning their work and measuring their success.**

ZF is a global leader in driveline and chassis technology as well as active and passive safety technology. In 2015, ZF acquired the US-American company TRW Automotive and integrated it into the group as the "Active & Passive Safety Technology Division". With its headquarters in Friedrichshafen at Lake Constance, ZF is one of the biggest automotive suppliers worldwide. With its approx. 135,000 employees at around 230 sites, it is represented in approx. 40 countries.

Together with the newly integrated devices of TRW, ZF's worldwide IT infrastructure has approx. 80,000 terminals and 10,000 servers. About 90% of the server landscape is virtualised, but the clients are conventional hardware. Like many other companies with industrial manufacturing, ZF has many production lines with IT components, which have been used for many years. They too have to be maintained and looked after by IT Security because the systems as a whole are far from reaching their planned life expectancy.


*The ZF Innovation Truck – a truck prototype with a length of over 25 meters – can be conveniently maneuvered via tablet remote control with zero local emissions.*
*Source: ZF FRIEDRICHSHAFEN AG*

### Efficient check of central standards

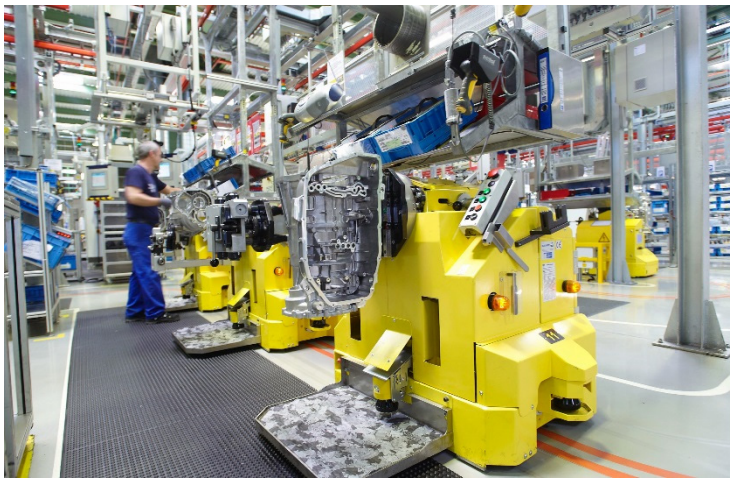
The company's entire IT is centrally controlled from Germany. The requirements developed at the headquarters are applicable on a global level and are communicated to the employees in a fair and co-operative manner.

The employees should understand and accept the guidelines and standards and act as partners of the IT management when it comes to implementation. Information security is also centrally organised and operated from Friedrichshafen. The group coordinator for IT security exercises superordinate control. On an organisational level, ZF has incorporated the Security Division into the productive IT. "The advantage of this model is that IT Security is directly involved in the IT project planning," Michael Schrank, Head of IT Security at ZF, explains.

## A new hub for the corporate security level management

"For this reason, IT and IT Security act in concert. Their decisions are received with the necessary attention, and they are truly implemented on a global level." For Schrank, the clear, simply structured organisation offers a true increase in security. "If we have to take measures at short notice because of imminent danger, we can do this quickly and without much delay. Companies with e.g. several CISOs for various units in the organisation need much longer for these processes."

In 2014, ZF started to search for a tool, which offers a reliable overview of the current IT, security status of all IT components in the global network. The group experts saw considerable need for improvements in this area: "We tried to determine the overall status manually using the various consoles of the system and security management tools," Schrank explains, "but this proved to be too complex and time-consuming. And we were unhappy with the quality of the results."



*8-speed automatic transmissions for passenger cars are produced at ZF's location in Saarbrücken. Source: ZF FRIEDRICHSHAFEN AG*

Searching for a remedy, the team assessed the "Security Lighthouse" solution offered by AMPEG. The monitoring system is coupled by 'collectors' to the system and security management tools in the network. There, it collects and correlates the collected status information nearly in real-time and compares them to the company's internal security requirements. The system processes the results in such a way that, among other things, they are visualized on a world map, representing the security level of the individual locations by traffic-light colours. In the event that there are some discrepancies or errors at one location - such as virus patches which are not applied, missing software updates, omitted patches or delayed system feedback - the operator can investigate the problems in more detail by just one mouse click, retrieving increasingly detailed information about network segments until getting to the individual systems.

### Adaptability due to collector concept

"The concept of Security Lighthouse met our ideas on several levels," Michael Schrank remembers. "The first aspect was the collectors: From our point of view, this architectural feature promised to be a good starting point for possible extensions, individual adaptations and the implementation of our own ideas. The second feature we noted was the successful visualisation which helps the operators to quickly assess and localise possible problem areas." In addition, Schrank was interested in the role-based access model. It allows assignment of granular access rights for individual sectors and segments of the IT

infrastructure, offering the administrators insight only into the areas of the IT landscape which they are responsible for. ZF considered this to be the chance to use the tool flexibly at various sites.

For ZF, all three expectations were met. During the Proof of Concept (PoC), AMPEG was already able to show that for nearly all important ZF systems which were to be integrated, collectors could be made available as an "out of the box" interface solution. "The fact that the PoC went so smoothly against this background, and that we did not have to find individual solutions, made us expect a low-maintenance product," Schrank explains. From the very beginning, cooperation with the supplier proved to be smooth and easy: "When at the beginning a value of the status assessment did not fit, we just needed to call support – and in no time the problem was analysed and fixed, without any waiting times or long discussions."

### Fruitful cooperation between supplier and client

The final decision in favour of Security Lighthouse was then quickly taken. "Four weeks after its start we already had a functioning system which proved to be very useful," Schrank adds, "and after a year it was completely installed on a global level too – including the training of the employees." At ZF, AMPEG Security Lighthouse now collects and correlates data from sources like Active Directory, Update and Inventory Management, package management tools, the Configuration Management (CMDB, Security Instructions) as well as two anti-virus products.


*ZF monitors the current security status on the security information map of the security lighthouse in almost real time.*

Schrank reports: "Together with AMPEG, we have developed a new collector." It is an interface for configuration management. "From the idea to its implementation via its assessment, cooperation was effective and fair," the ZF expert continues. "AMPEG immediately accepted the idea, and after three months the new collector was already ready for use." Meanwhile, AMPEG has incorporated the interface into its range of pre-fabricated collectors. "In addition, ZF uses our latest CVE catalogue (Common Vulnerabilities and Exposures)," Michael Hänsel, project leader at AMPEG, remarks. "This resource helps when it comes to vulnerabilities, which are then correlated

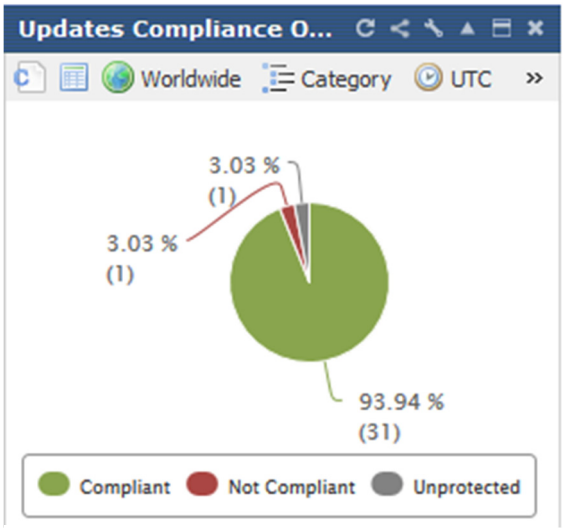
## A new hub for the corporate security level management

with the data from the update and inventory management already collected by Security Lighthouse."

Moreover, the visualisation of the security-relevant information by Security Lighthouse has proven to be as practical and flexible as ZF hoped. Among other areas, ZF uses the system at the Security Operations Centre (SOC) where analysts use it to better assess possible consequences of a known danger for the systems in the network and to be able to classify events and incidents more precisely. "For us, reporting is of the utmost importance," Schrank explains. "Today, we are able to show at any time without much effort whether and how we are meeting the agreed Key Performance Indicators (KPIs) of our security level. Measuring and comparison are executed automatically, and the results are processed in such a way that they fully meet management demands."

### Allotted use thanks to the role concept

On the basis of the role concept, it has also been possible to adapt Security Lighthouse to the work processes around the security level management, as requested by ZF. "There is not just one central control instance working with Security Lighthouse. Worldwide, more than 150 employees have permissions to access the system," as Schrank describes the use of the software. "We do not consider the monitoring tool to be a one-way system which simply passes top-down requirements by a superordinate instance. We use Security Lighthouse as a tool between the central division and the person responsible in the individual IT sectors for a fruitful cooperation to increase our security level." To achieve this, all target specifications and threshold values for the desired security level are entered into the system in Friedrichshafen. The teams worldwide use Security Lighthouse individually as an information platform, which shows minimum standards, and with the help of the monitoring tool they are also able to get information if their measures to meet the specifications and patch security gaps are successful.




*The global security level at a glance.*

For ZF, the next steps are the development of further specific collectors, and the integration of the IT landscape from the new "Active & Passive Safety Technology Division" into the status monitoring.

**This solution was implemented at:**

ZF FRIEDRICHSHAFEN AG
Graf-von-Soden-Platz 1
88046 Friedrichshafen, Deutschland
http://www.zf.com/

**With support from:**

AMPEG GmbH
Stavendamm 22
28195 Bremen, Deutschland
https://www.ampeg.de/