ARP GUARD by ISL

SUCCESS STORY

Unauthorized Hardware Detection at Mercedes-AMG GmbH

Mercedes-Benz

As part of the continuous expansion of the IT security infrastructure of Mercedes-AMG GmbH and its growing number of external partners and service providers who use their own IT equipment, the objective of Mercedes-AMG GmbH was to be able to detect and localise this external equipment in the network and avert any risks.

This detection was to be guaranteed independent of the network device connected and of the operating system, throughout the campus and without renewing the already existing LAN infrastructure (Local Area Network).

The appliance **ARP-GUARD** from ISL was used as a basis in a redundant set-up employed for load distribution. Other desirable functions could be easily implemented with the appliance which is based on a Linux architecture.
The mode of operation can be explained in brief as follows: As soon as hardware is connected to the network, the system checks in its database to determine whether the device is recognised as being a trustworthy network component. If the device is known and legitimate, access to the network is granted accordingly. If the device is unknown, has been taken out of service or classified as untrustworthy in any way, it is automatically transferred to a quarantine VLAN (Virtual Local Area Network) which is very restricted in its function thanks to a firewall. This isolation of the hardware from the rest of the network contributes to a great extent towards protecting the network infrastructure and the systems connected to it. Other security interests, such as the migration of know-how or protection against unknown computers which are possibly infected with viruses and malware, are served.

DaimlerChrysler <COMMUNICATIONS2>, Stuttgart

Press Release

Mercedes-Benz