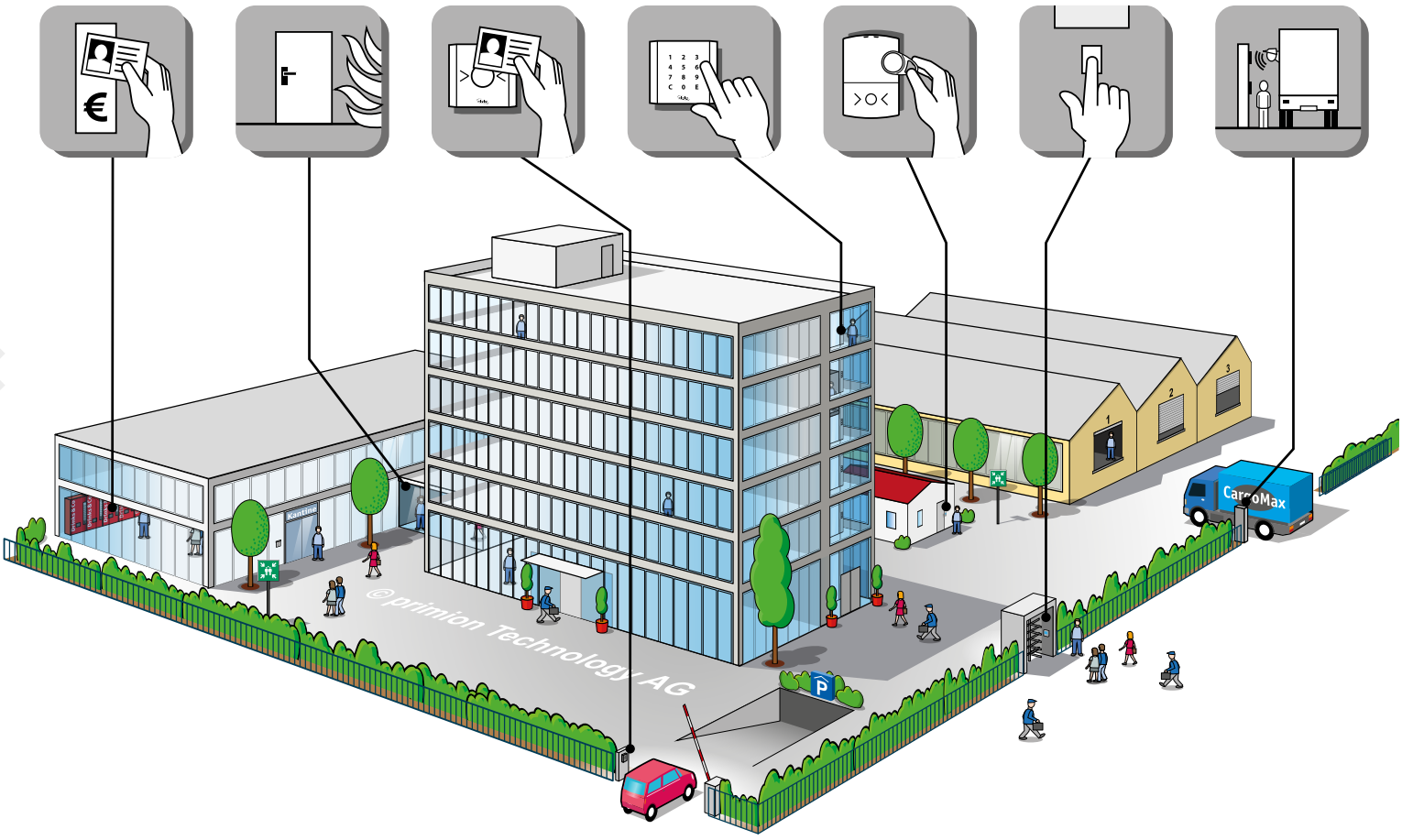
VdS approval for the Hazard Management System psm2200

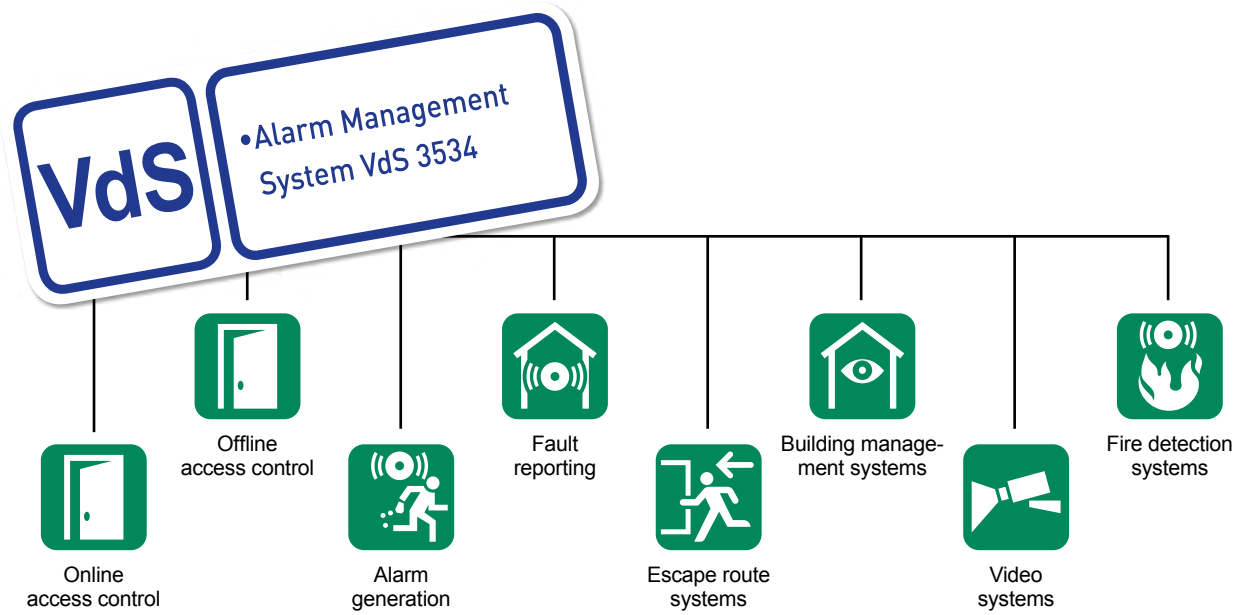
Compliance with the DIN EN 50518-2 testing specifications confirmed



Until now, the focus has been on the integration of classical security technologies into a Hazard management mystem (HMS). Today, the drive is towards achieving the "intelligent building", that integrates the complete building management technology, including security, into one user interface. The efficiency of such a solution is very dependent on the communication between the different disciplines that come under building management technology. The more information there is, the more clearly this can be made available to the user and the more it can be used to trigger interactions between the individual disciplines.

In the ideal world, the HMS should have VdS approval in accordance with VdS 3534, in order to confirm compliance with the current testing guidelines laid down by DIN EN 50518-2 (Alarm receiving centres ARC). At the same time, this gives the operating company certification from an independent institution in respect of the quality, reliability and security of the software. This increases the security of investment and makes the HMS available for certified deployment in Security Command and Control Centres (SCC) across Europe. Interfaces create the bridges. They safeguard the integration of all the building's technologies into

“Investment and planning security are a central issue.”



one management system. A primary HMS understands, converts and delivers the information from all connected technologies. It brings together the data points and notifications from the sub-systems, such as Access control, Intrusion and Fire detection systems and BMS, at a central point, and offers the option of visualising them through a single user interface. In this way, individual disciplines and their technologies are united into a single, overall and networked system. The user can control the whole technology network through one application. The multiple deployment of individual components brings cost reductions, e.g. through the multi-functional usage of an opening contact for the Access control system, the Intrusion detection system and the Heating, ventilation and air conditioning (HVAC) system. The result is effective risk prevention.

Many systems “speak their own language”. Interfaces bridge these language barriers. Information from the connected disciplines, e.g. VMS, is made available as data point models in the central database. In this way, reactive control commands can either be automated through the management system or created manually by the operator. Information and control buttons are visualised through the application interface or shown as Workflows.

Planning and investment security

Investment and planning security are a central issue, as given for example, by the range of interfaces offered by the management system, the functional scope, and the future expansions guaranteed by the manufacturer. There have been great advances in the standardisation of interfaces in recent years. Today, you can differentiate between proprietary and generic or standardised interfaces that can be designed to operate unidirectionally or bidirectionally. Efficiency and system-openness play an important role.

If they are deployed consistently, standardised interfaces offer the benefit that the hardware can come from different manufacturers. The operating company can plan flexibly and price-sensitively. It is not →

→ dependent on a single manufacturer. Examples here are BACnet, OPC, Modbus, ONVIF, SNMP or also serial protocols. The interface protocol is a one-time development and it communicates with hardware where this communication protocol has been implemented. The prognosis about development trends is however a hot topic for discussion as in many cases, standardisation means a reduced performance and functional scope. And as before, there are products on the market where the standard has only partially been implemented.

Proprietary or "manufacturer-specific" solutions offer the possibility of deploying the maximum performance and functional scope of the connected discipline in the management system. But freedom of choice when it comes to the components is limited, however.
In all cases, it is advisable to define the functional scope with the supplier/manufacturer and to limit it to what is really needed. Often, the whole scope is not required. This reduces development time and costs. The customer receives exactly what is defined in the agreed specification document. Frequently, an SDK (Software Development Kit) is required. Some manufacturers demand that an NDA (Non–Disclosure Agreement) is signed before the SDK is used and/or that an SDK licence fee is paid.
This has to be considered when planning the project, both in terms of the time and costs involved.

Mobile Application

Android and iOS as "state of the art" operating systems in tablet PCs or cell phones keep the operating company and/or the security monitoring company up to date at all times through their mobile clients. With the "Mobile Client" WebApp in psm2200, functionality, GUI and menu guidance have all been modified to meet iOS and Android specifications so that they fit to the display. This opens up a whole world of new options in relation to the maintenance, operation and servicing of technical equipment and also for intervention and alarm verification through video surveillance, countermeasures and the automation of management tasks. A rapid overview of building status and site monitoring are guaranteed. Effectively, maintenance work can be done on a "one-man maintenance" basis, thanks to the Mobile Client.

In the case of intrusion, the situation can be verified and evaluated through the Mobile Client, using a live camera stream from the affected area. For example, the emergency services can be authorised to access the video stream locally, allowing them to pre-evaluate the risk situation and if necessary, to initiate appropriate actions.
Further application options include Facility Management across buildings that are geographically separated. Mobile information about faults is distributed "on the fly" to the facility team, allowing the resource-optimised deployment of available staff.

Legacy systems – Investment security

The reality in the market shows that HMS integration projects are not always limited to new systems. If existing systems are to be integrated with later, newer technologies, a check has to be made as to whether they are capable of being integrated. Many older sub-systems for example, do not have interfacing options. As an alternative, it is possible to achieve a "hard-wired integration" with a greatly reduced functional scope, using relays and hardware. Development resources and competence have to be available in-house at the supplier/manufacturer, to be able to achieve such a customised integration. The success of the project depends on this.

When integrating different technologies, interfaces form the link between the HMS and the sub-systems. In the ideal world, there will be a single-source to cover everything from project concept to project completion. psm2200, with its one-stop-shop philosophy for the VdS-certified HMS, fulfils the ideal pre-requirements in this respect.

Important functions and features of an interface

Automatic data point transfer
The function for the automatic reading in of data point information from the sub-system when the interface is activated in the HMS during commissioning or when additional peripheral devices are added, reduces the installation effort and therefore the costs.

Data consistency
The interface must map the data from the sub-system, together with its states and state changes, uniquely in the HMS.

Analysis tool
This is needed for monitoring the data traffic over the interface, with optional filtering and archiving functions. Following on from this, the control functions can be customised and for example, malfunctions can be analysed and resolved.

Monitoring function
It must be possible to carry out function and live checks on all the interfaces and their connected sub-systems, in order to be able to identify breaks in transmission from security-relevant applications for example, and potential data losses, immediately.

Redundancy
To increase drop-out security, particularly in the case of security-relevant sub-systems such as Fire detection or Access control, the HMS should have the option of driver redundancy. This makes it possible to connect a sub-system twice, using a second interface.

Prioritisation
It should be possible to define the prioritised processing of notifications from sub-systems. Only in this way can highly security-relevant notifications from sub-systems be processed by the operator according to their importance.

Encryption
In security-relevant applications, particularly where the communication is done outside the secured company network, it must be ensured that secure or encrypted transmission options are in place. Only in this way can steps be taken to avoid the external manipulation of data.

Performance
The interface must have high performance levels. Neither the programming of the interface nor the HMS itself should set any limits on the data quantities that can be made available through the sub-systems.

Freely definable icons
When sourcing an interface, it must be ensured that the scope of delivery of the interface includes an icon library for the driver's data points and that additionally, it is possible to modify the icons in line with the operating company's CI/CD guidelines.