

Integrated security systems.

Integrated security systems.

Robert Verhulst

Robert Verhulst

ISBN: 9789402158441

No part of this work may be made public and / or multiplied by any means without prior permission from the publisher.

Thanks for the photo authorization to:
HTC parking & security bv the Netherlands

Do you have questions or suggestions about this book:
info@rcms.expert

Purpose of this work:

With this work, I want to give everyone involved in the design of an integrated security system with innovative technological security a guideline and to profile the choice of product and installation to the current state of the art technology.

This work consists of six chapters:

- I. General concepts.
- II. Integrated security.
- III. Access control.
- IV. Audio and video.
- V. Other tools.
- VI. General information and normalizations

Robert Verhulst

For RCMS BV

Revision 4.0

January 3th 2020

I. General concepts

Security or Safety ?

The two words very often tend to confusion. However, there is a very large distinction between the following sectors in security.

Sector of human protection or safety

- Fire security
- Disaster
- Emergency
- Riots

Sector to protect people and values or security

- Burglary security
- Access control
- Spying
- Sabotage
- Cybersecurity
- General monitoring and observation
- Fire detection

With the above sectors as an example, I will try to distinguish this further in this work, dealing with the use of "security" or "safety". From the factors cited, it is clear that unexpected or unpredictable danger plays an important role in the security sector.

Credentials?

In this work one usually speaks of credential when one means a means that is used to identify a person. Depending on the installation, this can be a badge, a tag, electronic key, a smartphone but also a form of a barcode.

Surveillance:

In this work, the word surveillance will frequently be used in the distinction of guarding. Surveillance in the sense of a form of complete observation and control. This is not only an alert and takes action, but also proactively follow an evolution, avoid an imminent danger, analyze behavior and take the necessary

action. Surveillance can only be executed by people with knowledge in this area and day by day activity on the domain to be monitored. Guarding is the following up of predetermined instructions and following up alarms after the facts usually executed by people with a little affinity with the dynamic event.

Onsite monitoring or remote monitoring!

In the case of onsite or local presence, the supervisor has knowledge of the activity and the environment, enabling him to evaluate detection much better and make proactive decisions.

Remote monitoring is always post event with little knowledge of what is happening on the site and will result in greater damage. Unfortunately, this choice is made from cost consideration.

Independence:

Should it be mentioned again that monitoring of a subject or a domain must be independent of the operation of this topic?

Examples from experience for clarification:

-A computer center is monitored with a number of cameras and sensors, a serious error consists in providing the uninterrupted power supply or the software of the surveillance in this space. A sabotage attack on the computer center will also disable the security system and leave the customer without evidence and further control on any action!

-A camera observes an emergency power generator but depends on the power unit for its power supply.

-A network must be independent and managed by the security services. Use of VLAN on an existing network is not permitted since the physical cable and equipment are always accessible by others and do not meet the same security regulations.

- An observation camera is powered by a local power outlet, other devices such as a refrigerator that shows an error or causes an earth leak will disable the camera.

Make a distinction between security and non-security, avoid complicated



structures such as PSIM (Physical security information management) which also includes technical monitoring and control. BCS (Building control systems) are a must for complex systems but demand other skills and can easily be remote controlled.

Bunker?

The place where real-time security decisions are made must be housed in a safe and well-protected place. An attack will usually be aimed directly at the target and in these circumstances security must remain in operation. If an attack is simultaneously or in advance aimed at the security station, it must be sufficiently reinforced to allow external intervention time.



In practical terms, the central system and control must be in a safe place, protected by physical means, access control and preferably invisible from the outside. Too often a security guard is seen as a night porter.

Within security limits:

An integrated system usually makes numerous connections with other techniques. However, the attention of an operator cannot be withdrawn by non-security-related notifications. Behind every non-security assignment can be a critical security situation. Critical technical conditions that are not directly related to security can possibly be reported and passed on to other authorized persons, this exception with short handling must, however, be limited. It is not the task of the security officer to adjust the temperature of a room, however a water leak can pose a security risk.

Keys:

Despite all the new technologies, physical keys have still not disappeared. Depending on the size of a site, you sometimes see thousands of unused physical keys, but they provide access despite electronic access control. Physical keys and pass-keys can be copied fairly easily and represent an additional threat. (it is not because the honest locksmith has a key made by the manufacturer that a burglar cannot make it)



There are even greater concerns for the keys of technical cabinets, which are usually universal! Bear in mind that the tamper contact of the cabinet will cause an alarm but cannot avoid sabotage.

Certain institutions have a key management software, system or an employee for this. A new approach with new technology can lead to an important ROI with higher security.

Aging:

If physical security equipment has a long service life, this is not the case for electronic products in the sector. Just like the evolution of keys over the last century, security technology has taken steps to protect against new challenges in line with the evolution of IT technology. One can generally say that installation of 20 years old no longer meets current expectations of security and efficiency.

Preparedness:

A state-of-the-art installation works in an invisible way to ensure the proper functioning of all parts in the installation. Previously, a good passive infrared detector was often regarded as a good sensor because it never caused an alarm !!! In current technology, each sensor or control must be connected to a network and provide sufficient information to ensure the original sensitivity.