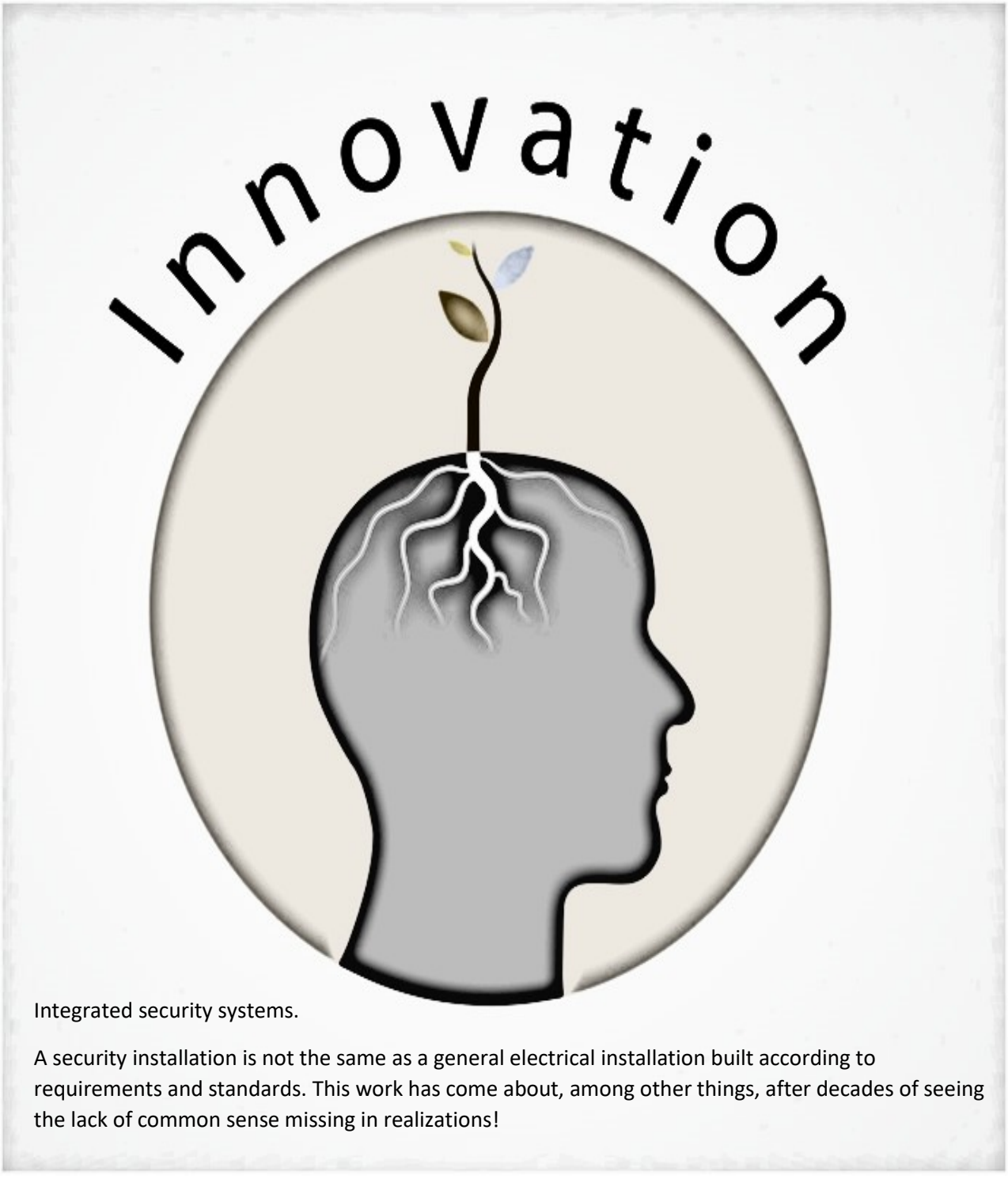
Integrated security systems.

Security systems cannot consist of one and the same standard solution!



Integrated security systems.

A security installation is not the same as a general electrical installation built according to requirements and standards. This work has come about, among other things, after decades of seeing the lack of common sense missing in realizations!

Robert Verhulst

Robert Verhulst

ISBN: 9789464480238

Thanks for the photo authorization to:
HTC parking & security bv the Netherlands
Dormakaba Belgium
Idemia France
Proton Data USA
Axis communication Sweden
Boon Edam bv the Netherlands

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

www.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. RFID
VI. Fence.
VII. Other tools.
VIII. Distance surveillance.
IX. Maintenance and adjustments
X. Cybersecurity
XI. General information materials
XII. Questionnaire
XIII. Conception
XIV Sustainability
XV. General information and normalizations

Robert Verhulst

For RCMS BV

Revision 30.0 March 2026

Security the beginning!

In reality, there is hardly ever a security study of the location, environment, structure, terrain, etc., of a new building or site to be built! Nevertheless, it is a security consideration before the moment that the architect puts a pencil on paper. Together with the first lines of a design, the important physical location must be followed with security advice. Solving risks afterward with electronic means is often difficult and an expensive procedure.

Integrated security ?

Definition:

All the elements, software, hardware, and organization—that form a whole for a safety system where all these things form the necessary connection to one total safety solution.

What it is not:

Achieving this goal doesn't necessarily mean a single, centralized system with central oversight.

Create a dependency matrix to determine the most suitable solution.

I. General concepts

Security or Safety ?

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

Sector of human protection or safety
- Fire security
- Disaster
- Emergency
- Working conditions
- 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.

Three essential points for a security system:

Sensors, cameras, substations... all elements that are part of a security system must be protected against sabotage, destruction, false effects, defects, and interference of any kind... This cannot be avoided often, but it is critical that an alarm is raised. Signaling is the result. (e.g., a shooter or laser shoots at a security camera from outside a fence)

> *A detection device that cannot do this is not suitable for security!*

A security installation may not contain a “single point of failure”!

> *Make a matrix of all used elements including power supply and have your installer show the resulting damage on each part.*

Any security system is only operational if it can also control its proper functioning state at all times. To this end, anomalies of all kinds must be translated as alarms.

.

It is not unusual that due to renovation, advertising campaigns, events, etc., a detection device is unintentionally or deliberately no longer able to carry out the desired detection.

Proactive or reactive?

Traditional and legacy security systems are reactive systems where damage is usually detected after the alarm, or rather, the system reports that damage has been detected. Fortunately, thanks to AI and advanced technology, we are now entering a world with proactive systems.

Fundamental flaws despite inspection certificates for legacy systems :
- No remote interaction - No reliable identity of authorized persons
- No information about the functioning status of detectors
- No proof of confirmed detection
- Increased risk of persons present
- Maintenance to verify operation

Advantages of a technologically sound system:
- Identification of the cause of the alarm with evidence
- Interactive from anywhere with video and audio
- Each device reports optimal operation
- Minimal maintenance

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 or QR-code.

Surveillance:

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 follows an evolution, avoids an imminent danger, analyzes behavior, and takes the necessary action. Surveillance can only be executed by people with knowledge in this area and day-by-day activity in the domain to be monitored. Guarding is the following up of predetermined instructions and following up on alarms after the fact, 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 considerations.

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 been 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 of access control and preferably invisible from the outside. Too often a security guard is seen as a night porter.

Internet !

Internet communication is now indispensable, in most places one can obtain a very high reliability. However, in danger such as war and terrorism, it is the most sought after means of sabotage!

WiFi:

Wi-Fi is a widely used modern wireless communication method. Usually connected to the internet, audio and video communication can be conducted almost anywhere in the world. Communication takes place in the 2.4 GHz or 5 GHz band. When an internet connection is present, all the cybersecurity risks are present. On the other hand, communication can be easily disrupted by using a jammer. However, Wi-Fi can also be used completely privately as part of an OT network. A jammer is a high-power electronic transmitter that disrupts communication within a frequency band.

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.
Distinguish between security and non-security, and avoid complex structures like PSIM (Physical Security Information Management), which also incorporate technical monitoring and control. Building Control Systems (BCS) are essential for complex systems but require different skills and can easily be operated remotely.

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 passkeys 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.)

Please note: often a key with lower access can be adjusted by drilling and/or filing to obtain higher access!

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 key management software, a system, or an employee for this. Often the key is linked to an electronic fob with key detection in a cupboard. A new approach with new technology can lead to an important ROI with higher security.

Or do you use a traditional key… or do you use an electronic key?

The user will be granted unconditional access without identifying the correct person!

Advantage with electronic keys, the access can be switched off and changed remotely.

Key cabinets:

Many institutions, after daily searching for the appropriate key in whose possession, decide to purchase a key cabinet.
This step has one great use, with good management you can find the key, but security and the cost of management are an important negative factor that should not be underestimated.

Two common forms:

- Regular cupboard with key where the location of the key can be found with labels, the absence of the key indicates that someone has taken it. Such a cupboard requires minimal management by a person in charge who owns the door of the cupboard and who keeps a diary of who takes what and when the key will be returned. Efficiency savings can be considered between ease of finding the correct key and limited security. Usually this is a form that can be used well for a smaller number of keys. However, there are situations where hundreds of keys are kept and seven administrators are employed to manage the key room with a minimum of two people 24 hours a day!

-Almost similar cabinet with electronic control. This cabinet is opened using an identification tool such as a badge, tag or smartphone. This identification provides access to the cabinet and a number of keys that can be removed from the lock system. When the key(s) is removed, chronological information is stored of the person who gained access and the keys they took with them. Undoubtedly higher security, but an expensive investment that does not solve the problem of copying and stealing keys, management cost and identification cost still not solved.

Conclusion: mechanical keys are never safe and limit efficiency in the workplace.

Cabling in general:

Factor 1 is the violability, a damaged or cut cable will undoubtedly have the consequence of disabling part of the security. An installation carried out according to good workmanship will signal the error, but part of the installation is and remains out of control!

Edge cabling or cabling between sensor and local control unit takes many forms and without exception requires an alarm message when a malfunction or interruption occurs!

Network cabling between central units and local controllers is never carried out other than with a well-designed network with PoE. This network consists of a TCP/IP ethernet communication with encrypted communication and control of the trunk between ethernet switch and edge device. Ideally, sufficient bandwidth should be provided to enable audio. It is preferable to provide a redundant network such as loop cabling between switches and the central units.

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.

Drop the PIR detector:

PIR detectors used for movement detection are at the end of life since cameras can make far better detection and give prove of detection. A PIR can be placed out of direction or sabotaged with a spray. A camera is tamper-free due to internal image analysis and constant communication. In addition, a PIR requires a power supply while the camera is powered by PoE.

In general no detection should any longer give an alarm without having the ability of having a prove of the origin of the alarm.

Law and regulations:

In the last decade, regulations, standards, laws, and ordinances have been created that do not always simplify a security concept. Moreover, people think they are secure complying with them! These rulings are to be considered as a first step or a basement to create a security system and clearly not the end objective of the concept. French, German, and English national security institutes speak in a modern way of "*guides*", "*guidelines*", "*richtlinien*" in published documents. Laws and standards are drawn up under the influence of manufacturers and lobbies and often have the result that they are no longer thought about but implemented. Even worse is a current trend of inspections according to standard rather than by operation!

In my personal consultancy studies, not a month goes by without a confrontation with nonsensical situations where security is limited by legal regulations.

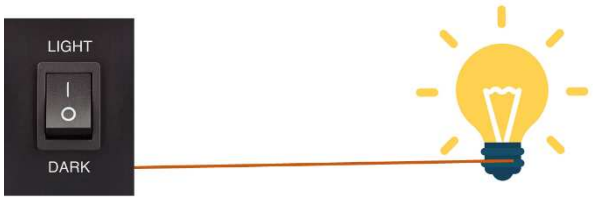
Power supply:

Each device requires a power supply; a table must be compiled, and the required autonomy determined. Determine which factors affect the overall mains power supply and which earth faults could cause an interruption. As-built documents should include a single-line diagram of mains power connections for all connections in the system, from the electrical input to each device. Also, consider the capacity of splitters in network switches for PoE power supplies. Low-voltage power supplies for devices must have a balanced autonomy.

Function retention and function control :

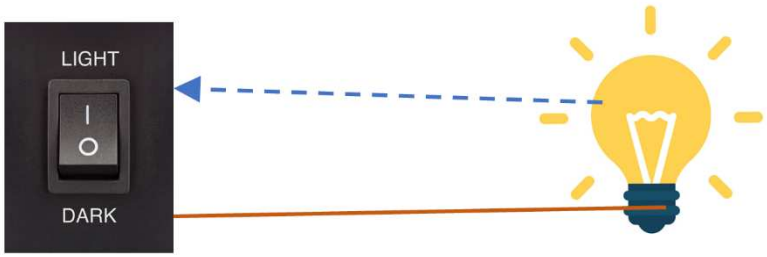
In contrast to electrical installations, a security installation must be built with functional integrity. Simple errors must not interfere with the continued operation of a security system.

Lighting installation switch controls lamp without controlling the lightchange:



Security technology:

Function check switch controls the lamp and the resulting light is checked as confirmation:



Function retention is guaranteed by loop cabling or redundant cabling:

The above principles are a first step, but for many applications and certainly for fire, it is also necessary to determine what can be lost in functionality with a single error.

Intervention, evacuation, invacuation:

These three concepts are related to each other and all have a model of implementation and each has a mutual relationship. A predetermined program of implementation and connection must be drawn up for this. This requires clear observation and controllability from an operating center.

Intervention generalities:

In this article I make the safety expert think about the safety and the safety aspect of blind intervention. For many years now it has been possible for an alarm system to initiate an intervention directly or indirectly without there being even a single indication of the danger that arises for the intervention team and for the people involved! This unimaginable situation can only be understood in the case of safety, with fire as an example.

Conclusion: an intervention should not take place without having been able to identify the emergency with images, sounds or other detailed information that reflect the nature of the emergency.

Intervention:

-Must always be done according to plan according to the knowhow concerning the facts.
-The operating center of security, which is inaccessible, may never be left, except when it is compromised (eg fire)
-The very first intervention is to use all possible remotely controllable means to remedy the situation from the operational center, to protect people and means.

-The second degree of intervention is to instruct people present to perform actions for protection. (staff with knowledge of risks and site knowledge)
-The third degree is to call for external professional reinforcement with limited knowledge about local

risks and infrastructure. It is important to make an immediate assessment of the necessary strength and time.

Some factors that should be taken into account:
1. The delay made by the intervener to the place of intervention, taking into account the time of occurrence and obstacles on the way. Please note that in the event of an attack, the intruder may not leave the road clear and may be more difficult!
2. Is access to the site possible at the time of intervention, who has the means to achieve the targeted goal.
3. Is guidance from a knowledge center informed about the site possible activity during the intervention?
4. The attack may have happened through an inaccessible route for the intervention team. (eg roof)
5. The attacker with knowledge of the site can plan the way back from the site differently than the way there.
6. The security center crew can never physically participate in the intervention and must provide guided communication.