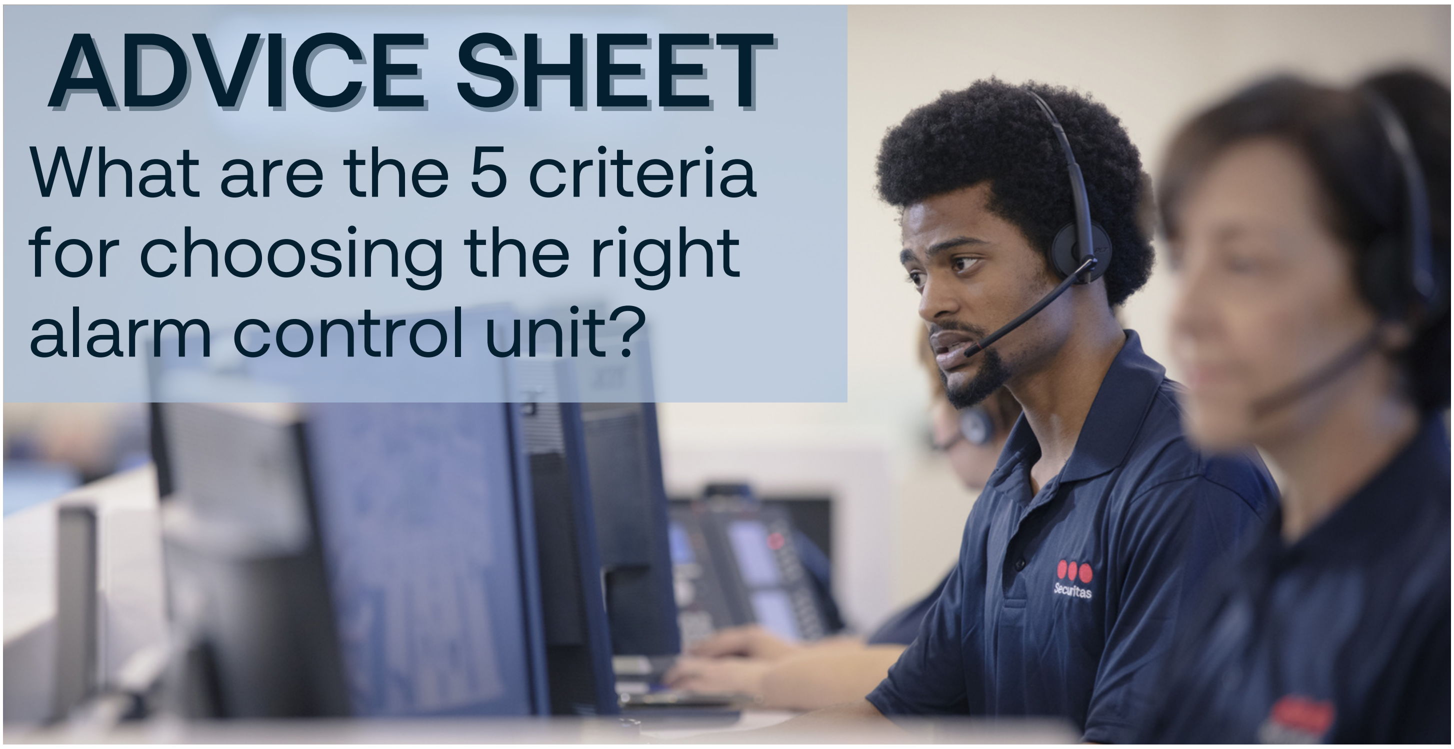
ADVICE SHEET

What are the 5 criteria for choosing the right alarm control unit?



Pascal Hulalka,
Solution Director

This decision is one of the many stages involved in setting up a security system, a sometimes complex operation that requires careful guidance.

To help you ask the right questions, our expert Pascal Hulalka, a member of Switzerland's alarm transmission standards committee, lists the 5 criteria to consider when choosing an alarm control unit.

1-PROTECT YOUR TRANSMISSION

Since the analogue network was discontinued in Switzerland, alarms have been transmitted over an IP (Internet Protocol) network.
Even when considered reliable, a network will rarely offer 100% availability. This means that while statistically reliable to 99.5%, your alarm could fail to communicate for 1.8 days a year and not warn you of an intruder or fire.
That's why, even for private users, I always recommend two-factor transmission, i.e. wired IP and a 3G or 4G modem, should the wired connection be interrupted.
Similarly, it's a good idea to choose a service provider with a redundant alarm centre which, as with the transmitter, will provide a back-up for the receiving and processing of alarms.

2-CHECK YOUR POLLING TIME

Polling is a technique for continuously and sequentially polling peripheral devices to check whether they have data to transfer.

To check that the connectivity between your installation and the professional alarm reception centre (or a manufacturer's cloud) is operational, small packets of data ("telegrams") are sent at regular intervals between the 2 systems.
24-hour polling for the wired IP section is enough to maintain a redundant system for private customers and SMEs. For larger structures, it is best to opt for a polling time of 30 minutes, or even 3 minutes for banks and jewellers.
In addition, once a week, it is customary to carry out a routine test to check that the alarm control unit is working properly from end to end on the site that needs protection, right down to the operator of the professional alarm control unit.

3-OPT FOR AN OPEN PROTOCOL

This issue is often the subject of debate, much as it was back in the day with the defenders and detractors of the Windows and Linux operating systems. Each system has its advantages and disadvantages.
- An open system means greater flexibility when it comes to interfacing with the existing infrastructure. Also, more people can test and make recommendations for improvements and changes.

Protectas
Rue de Genève 70
1004 Lausanne

+41 21 623 26 00
swiss@protectas.com

www.protectas.com

- An open system means greater flexibility when it comes to interfacing with the existing infrastructure. Also, more people can test and make recommendations for improvements and changes.
- A proprietary system or one developed by an integrator can be tricky to install (replace), and therefore more expensive to set up.

Today, the open protocols SIA DC09 and VdS2465 are full-featured open protocols (type of events, zones, etc.) and they are what we at Protectas have chosen to use. This allows us to move away from proprietary systems and provide a service regardless of the alarm system installed. In this case, simply adding an (alarm) transmitter that natively uses these open protocols means the manufacturer's system can be interfaced at a reasonable cost.

In all cases, whatever the protocol, encrypted communication is essential to minimise the risk of hacking!

4-INTEGRATE FULL VERIFICATION

Having a blind system has become archaic.
If you're wondering exactly what this means, then read on. Full verification means using every possible means to check that a break-in is actually taking place.
In remote surveillance, this is an essential prerequisite for requesting police intervention.
A call to the authorities that is not justified by a formal check could result in financial sanctions. It is possible to fully verify the situation on-site or remotely.
Physical verification consists of a visit to the site following the triggering of an alarm. The remote surveillance operator who manages and receives the alarm signals immediately dispatches a security guard to the customer's site to establish the origin of the alarm and why exactly it was set off. This is a verification operation that complements a remote surveillance service.

Once the incident that caused the alarm has been established and verified – a burglary, for example – the security guard will take the appropriate precautionary measures. In most cases, the police will be called in. They can also carry out emergency access repairs.

Video or audio alarm verification involves logging into the customer's alarm control centre to check video/audio recordings or the live stream from the cameras/microphones monitoring the detectors that have been set off.
So this is done electronically and remotely, saving an enormous amount of time. Today's technology is really helpful here because it can take time for a security operative to physically get to the site.

GOOD TO KNOW. The live stream is only activated when an alarm is triggered. A remote surveillance device cannot spy on you when you are at home.

As you can see, it is essential for private customers or businesses with a remote surveillance alarm system to supplement their security system with a physical, video or audio alarm detection service.

5-MAKE SURE THAT THE SYSTEM IS RELIABLE

Alarm systems are assessed based on various criteria so that they can be certified to something known as the "alarm standard".
For Europe, there are 2 alarm standards (these new standards will eventually replace the various alarm standards across different countries):
- the EN 50131 series for "intruder and hold-up alarm systems". This standard guarantees high-performance levels for both for the consumer and the retailer, who can use the certification to promote their product.

For private customers, a grade 1 or 2 is generally sufficient.

For shops and businesses, grades 2 and 3 are more suitable (risk to investment ratio)
- the EN 50136 series for "alarm transmission systems and equipment".

This standard covers single and two-factor channel transmission and determines how often polling is needed according to the maximum acceptable transmission time.

Here I would recommend SP2/DP1 for private customers and DP2/DP3 for business customers.

If you have any questions or comments, please contact me by email; I'd be delighted to hear from you:

pascal.hulalka@protectas.com