SWISSPHONE

s.GUARD

Critical Incident Management for Professionals

Your solution to successfully manage critical incidents to protect people, buildings and systems.

Additional Modules:

s.GUARD COLLAB
s.GUARD IOT
s.GUARD SOS
s.GUARD MSG
s.GUARD FLOW

Coming Soon:

s.GUARD REPORT
s.GUARD TASK

www.swissphone.com

Possible Customer Needs

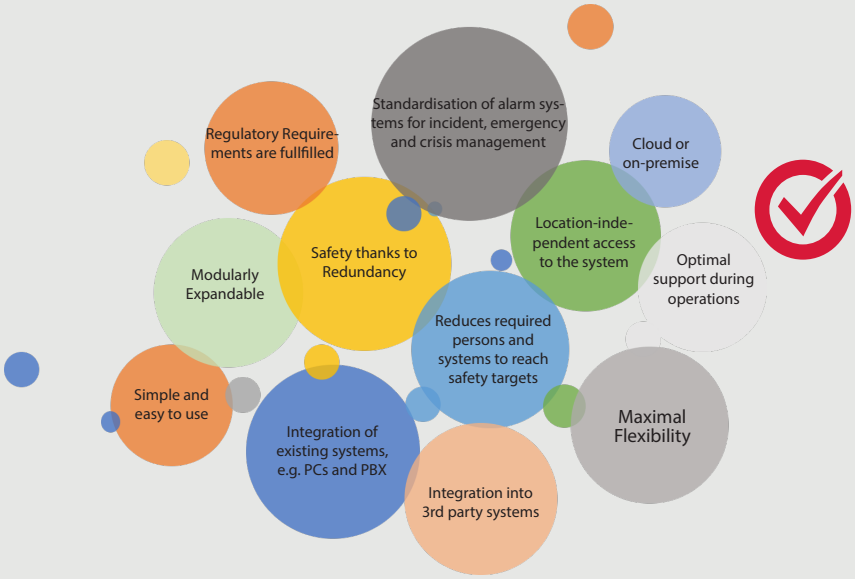
Or: What is a good Critical Incident Management System?

Unforeseen events can have serious consequences for companies. In order to guarantee the greatest possible safety and minimise damage, persons and groups must be able to be reached quickly. An effective alarm management solution reliably ensures that the right people can intervene on site at an early stage in an emergency. The basic need of customers for alarm management solutions is efficiency. The result can be diverse, such as efficiency in the sense of:

- Cost savings, e.g. because disruptions of production processes could be proactively prevented or very quickly eliminated thanks to secure alarms.
- Time savings, e.g. because alarms were sent quickly, reliably and with the right medium to the right person thanks to effective management.
- Reduced complexity, e.g. by reducing the number of systems and providers, outsourcing services and automatically integrating master data

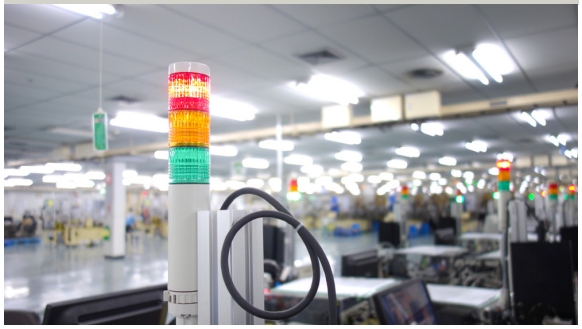
In order for an alarm management solution to be as effective as possible, it must be adaptable to specific customers and industries and be modularly expandable.

In summary, an alarm management solution is efficient and effective if the following points are given:



Critical Incident / Example

Malfunctions in Production, IT, Building Mgmt



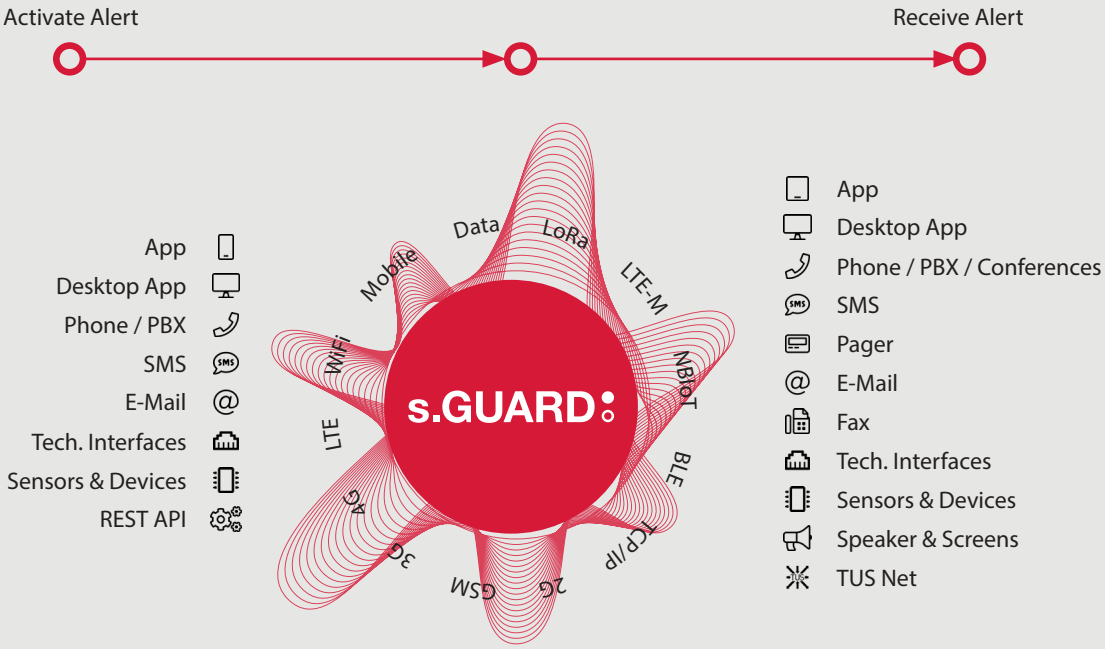
Critical Incident / Example

Fire

Zürich Main Station, 2018

s.GUARD: In the «Engine Room»

Based on the solid foundation of our instaCORE connectivity platform, we integrate a large number of proven components and tools into a complete solution tailored to your needs and wishes.



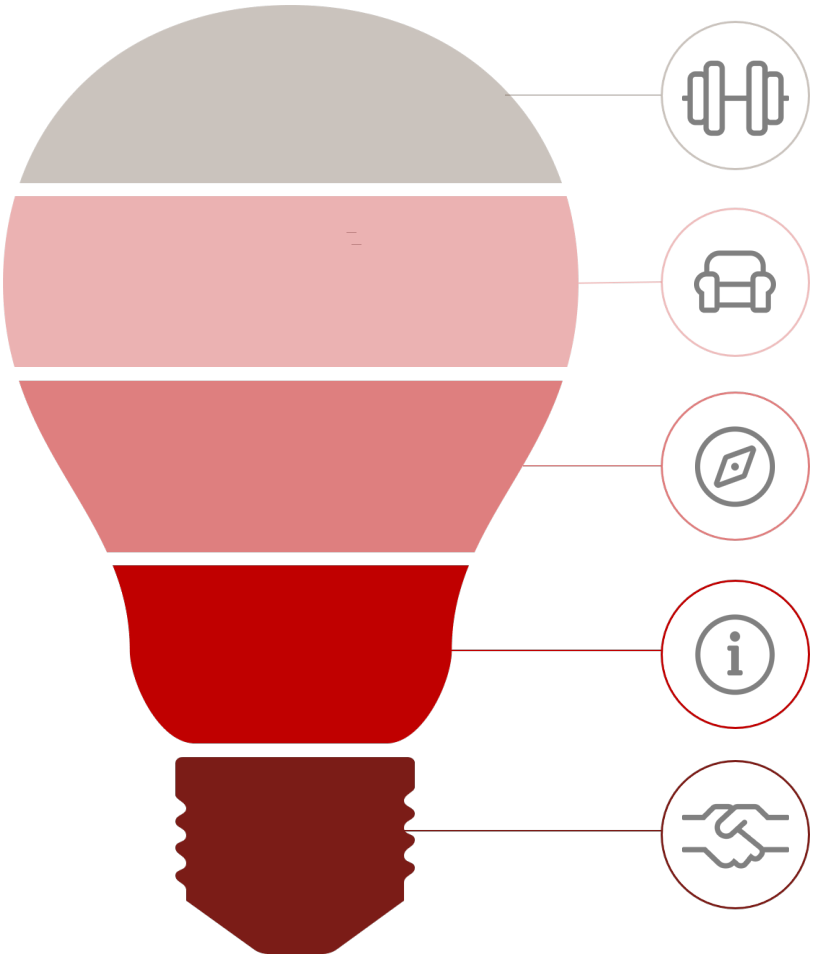
s.GUARD is available as an On-premise, Hybrid and Cloud solution:

Critical Incident / Example
Threat

Critical Incident / Example
Medical Problems

s.GUARD: The Basics

Of course, s.GUARD covers all requirements of an alarm management solution which should be taken for granted anyway:



1 Strong Alerting
- All channels
- Flexible escalation
- All your scenarios & groups
- With real-time control
- With maximum redundancy

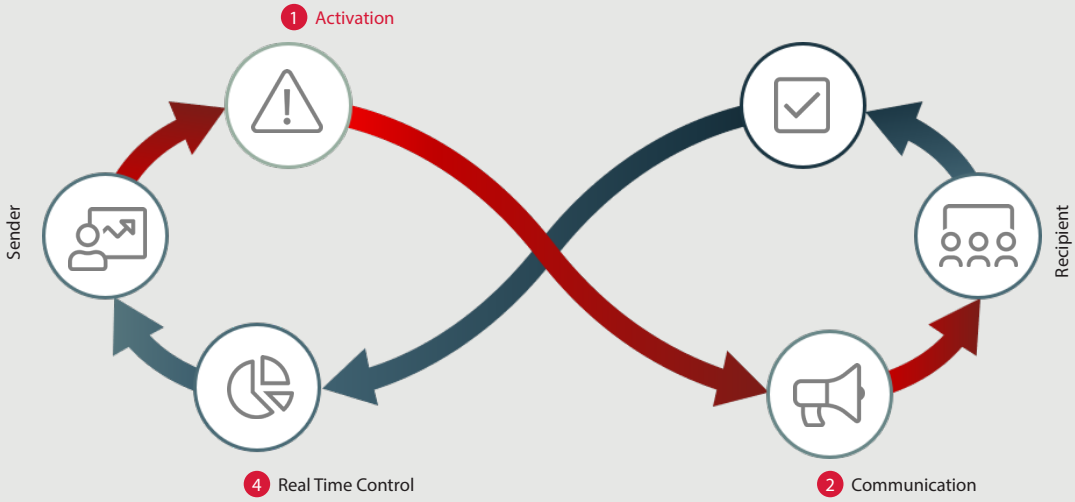
2 Easy to use
- Modern Apps
- Web-based administration
- With alarm simulator
- Focus on Cloud Solution
- With familiar devices

3 Flexible to use
- Modularly expandable
- For any number of users
- Any number of groups
- Hybrid and on-premise available
- Interfaces to technical systems

4 Informationen as needed
- Multiple images per alarm
- Freely definable texts & sounds
- Freely definable symbols & colours
- Freely definable language
- text-to-speech

5 Taylored Collaboration
- Checklists
- Chat
- Multiple choice answers
- Conference calls
- Documents (also offline)

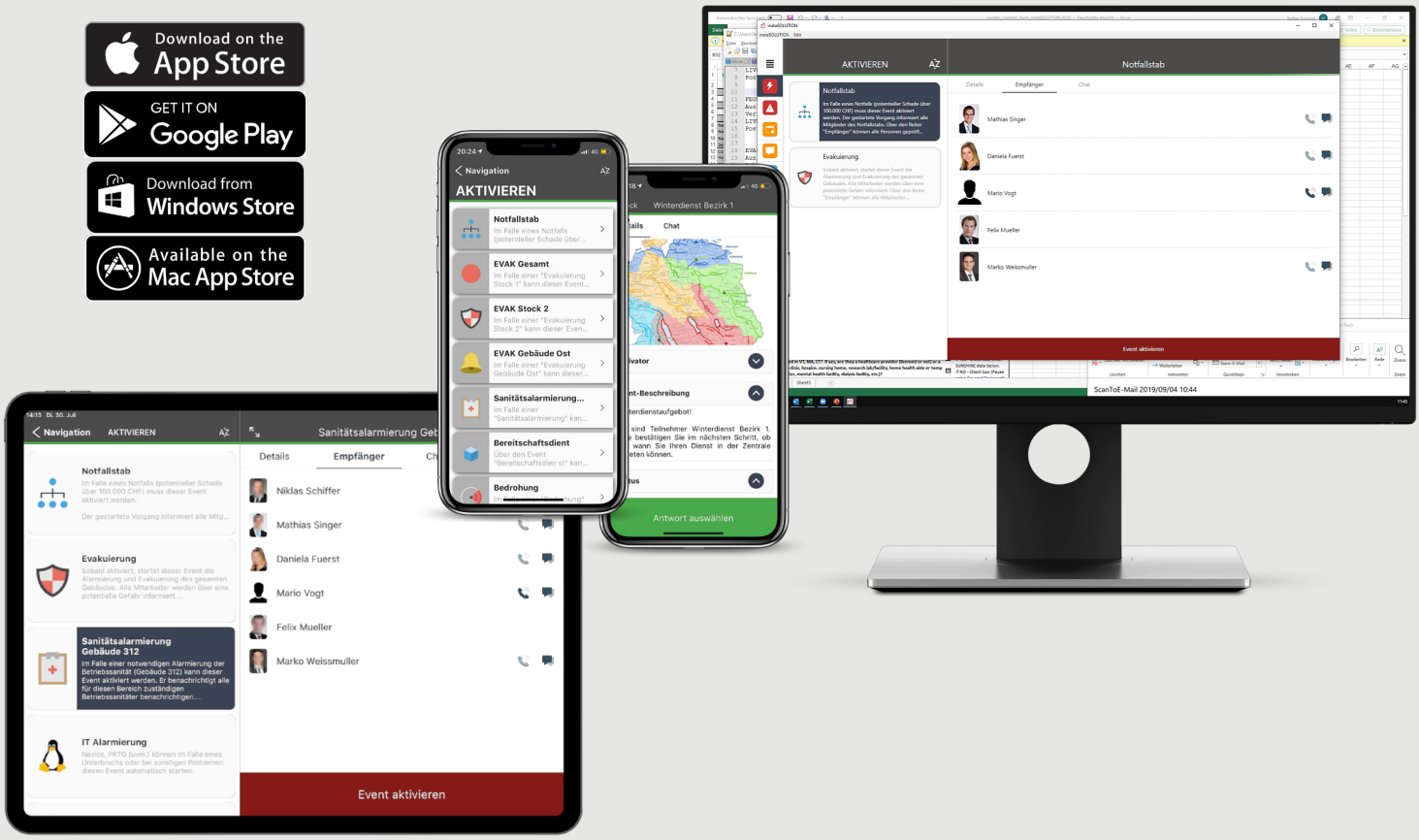
The Standard Cycle:



s.GUARD: The Apps

With our apps you not only have more information at your disposal, you also have all possible usages of our solutions at hand.

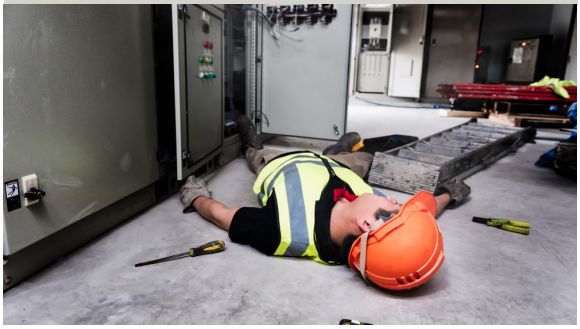
And of course the apps are available on iOS, Android, Windows, MacOS and as web-app (so you don't need to install a client, if you don't want to).



Critical Incident / Example
Amok

e.g. Menznau 2013

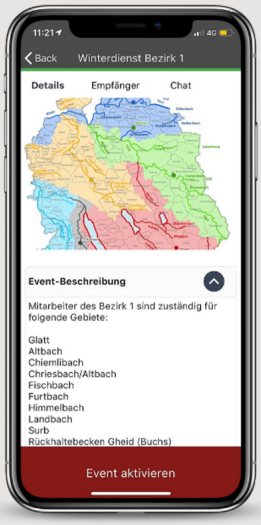
Critical Incident / Example
Accidents & Lone Worker



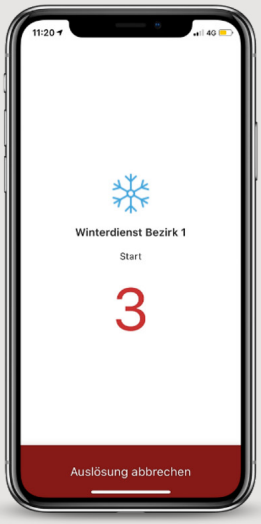
The Apps, and more

Symbols:
Shortened Reaction times
Errort reduction

Detailled Descriptions:
e.g. Pictures, Maps, Recipients
Text adjustable on the fly



Countdown:
Reduces false alarms
Duration adjustable

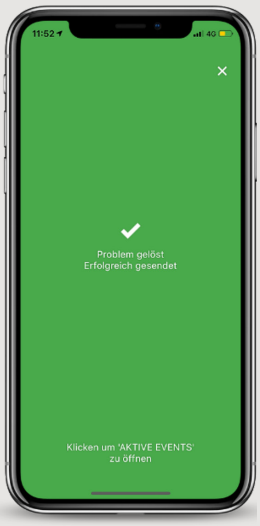


«always loud»:
App overrides volume settings
Unless you do not want that

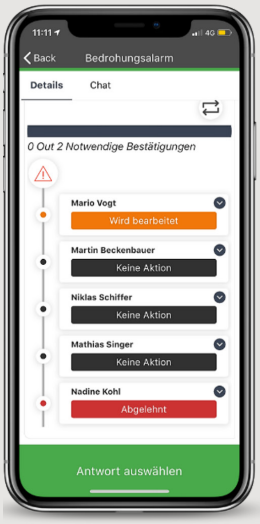
Fast reaction
All information at a glance
One-click Reply

Multiple Choice Answers
Freely definable content with clear colour language
Response status (e.g.„confirmed“ depending on response)

Intuitive user guidance
Feedback on interaction
Clarity



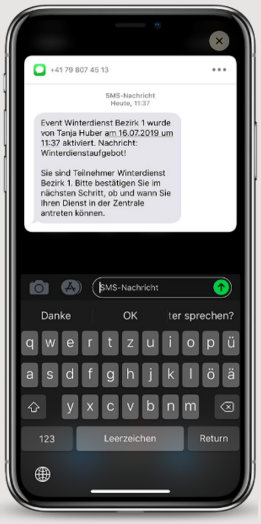
Live Protocoll
real-time control
Statistics (also graphical)



Chat, Documents, Checklists
Optimized communication
Information & Support

Telefon & Conference
Smart Conference Call
Fast: 1 call / s and morer

SMS, E-Mail etc.
SMS, E-Mail, Pager, Fax
Speakers, Screens



s.GUARD: Advanced Alarm-Management

In case you need more than just the essentials...

1 **Your all-in-one solution**
With s.GUARD you cover everything from a status change to a malfunction, an emergency and a full-blown crisis from a single source

2 **Flexible Logic**
Make your processes safer and better with more logic, be it with an alarm status «in process», by means of position data or flexible acknowledgement of an alarm.

3 **Lone Worker Module SOS**
With freely configurable, will-independent detection, a multitude of comfort and safety functions, a flexible cockpit and the (optional) alarm reception centre by our partners.

4 **Interfaces à la carte / AP**
s.GUARD provides a very large number of interfaces for third-party systems, be it for security or building technology, for production or the healthcare sector. Our open API gives you maximum flexibility.

5 **Security thanks to IoT**
Thanks to the Internet of Things (IoT), many things in the security sector are becoming simpler and cheaper, which means that you can get the most out of your organisation even with limited resources.

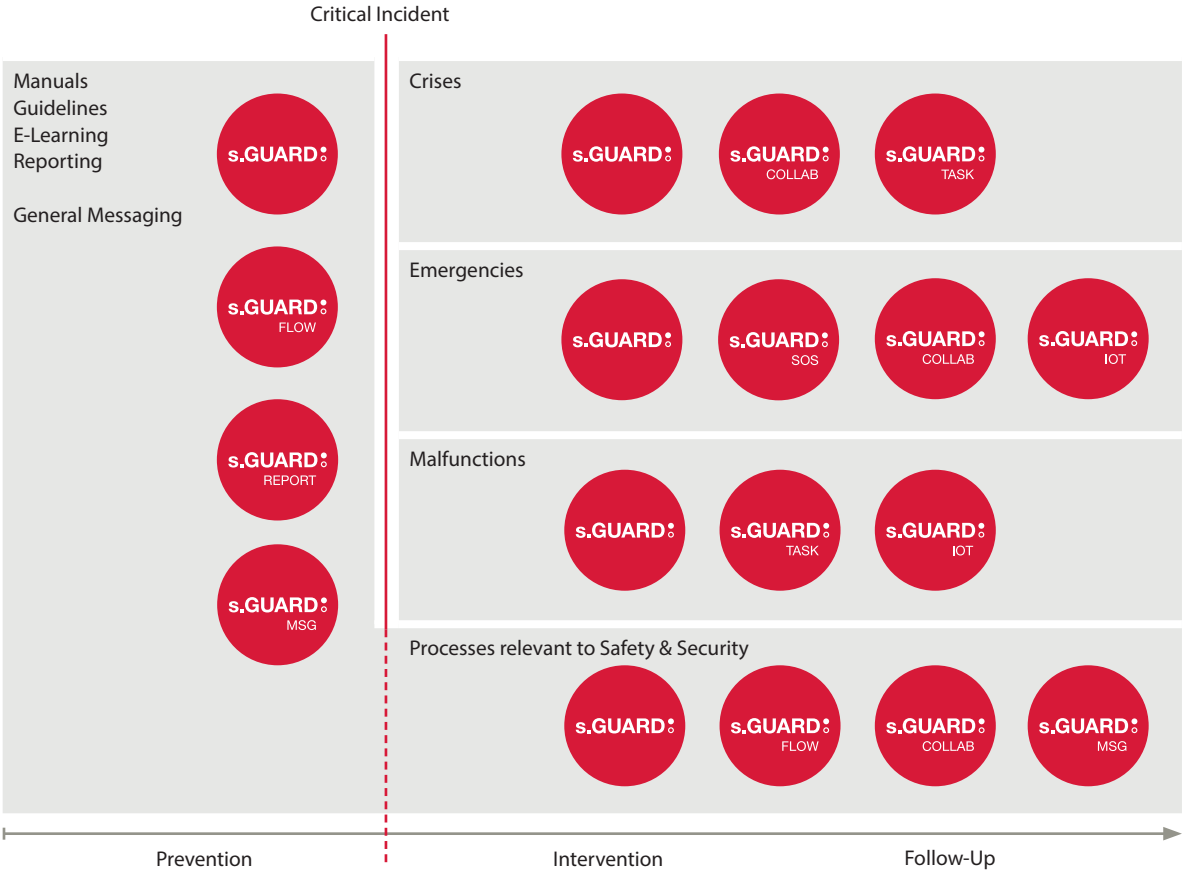
Critical Incident / Example
Social Media «Shitstorm»

Critical Incident / Example
Sabotage & Ransom

s.GUARD with Modules: Your all-in-one solution

With s.GUARD, you cover everything from a status change to an indicent or a malfunction, an emergency and a full-blown crisis from a single source. This unification has several advantages:

- Reduced complexity, e.g. by reducing the number of systems or system providers, outsourcing services and automatically integrating master data.
- Reduced costs due to economies of scale
- Increased acceptance of the solution by employees, given they only have to familiarize themselves with the system once

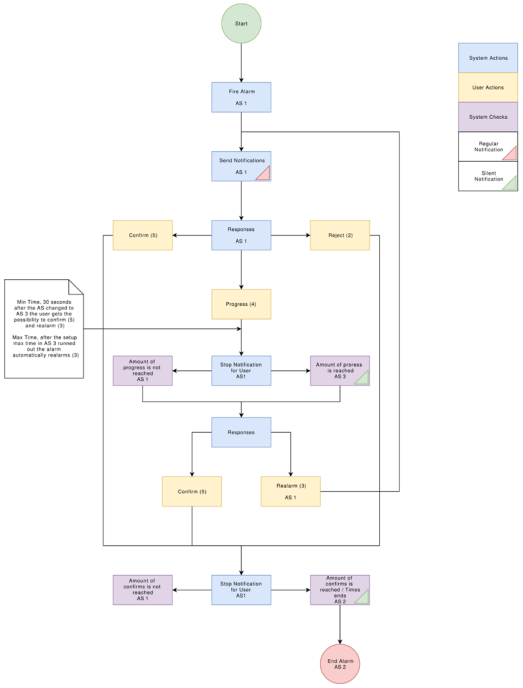


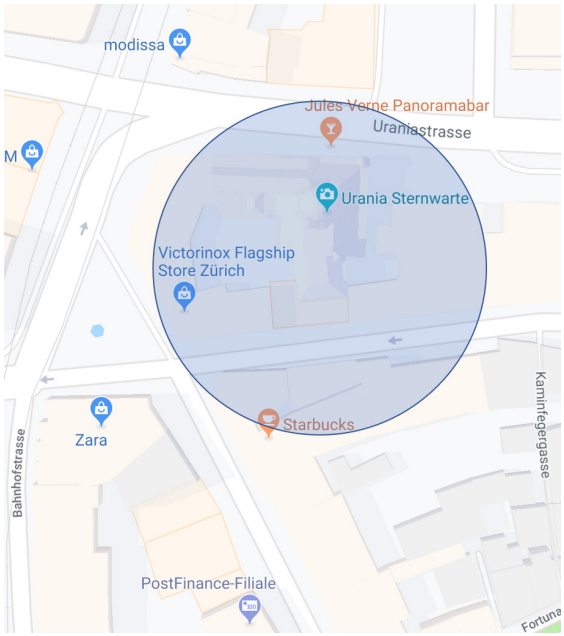
Critical Incident / Example
Evacuation (Fire, Gas etc)

Flexible Logic & Escalation

s.GUARD offers you a much more flexible logic than comparable products, not only in terms of (multi-stage) escalation and integrated verification steps, but also thanks to the possibility of setting an alarm to «in progress» and either completing it later or setting it to «re-alarm» (manual or automatic).

Furthermore, you can also trigger or receive alarms depending on the position (e.g. of a user), be it by means of «indoor positioning» or a «geo-fence».





- Flexible alert-stopping criteria (e.g. «4 of 10 persons have confirmed», «Only one person», «All persons») allow you to mobilize the right number of persons.
- Time-controlled and event-based alarm triggering and follow-up alarms allow you to trigger an alarm without having to manually execute the triggering.
- Schedules allow you to define exceptions for holidays, Sundays and more with just a few clicks. If desired, your users can (temporarily) unsubscribe from an alerting process flexibly and event-based.
- With ad-hoc user groups you can spontaneously and on demand inform only certain persons about an event via app.

«1001» ways to escalate an alarm...

From channel to channel: → → ...

From user to user: → → ...

From user to group: → → ...

From group to group: → → ...

From internal to external: → → ...

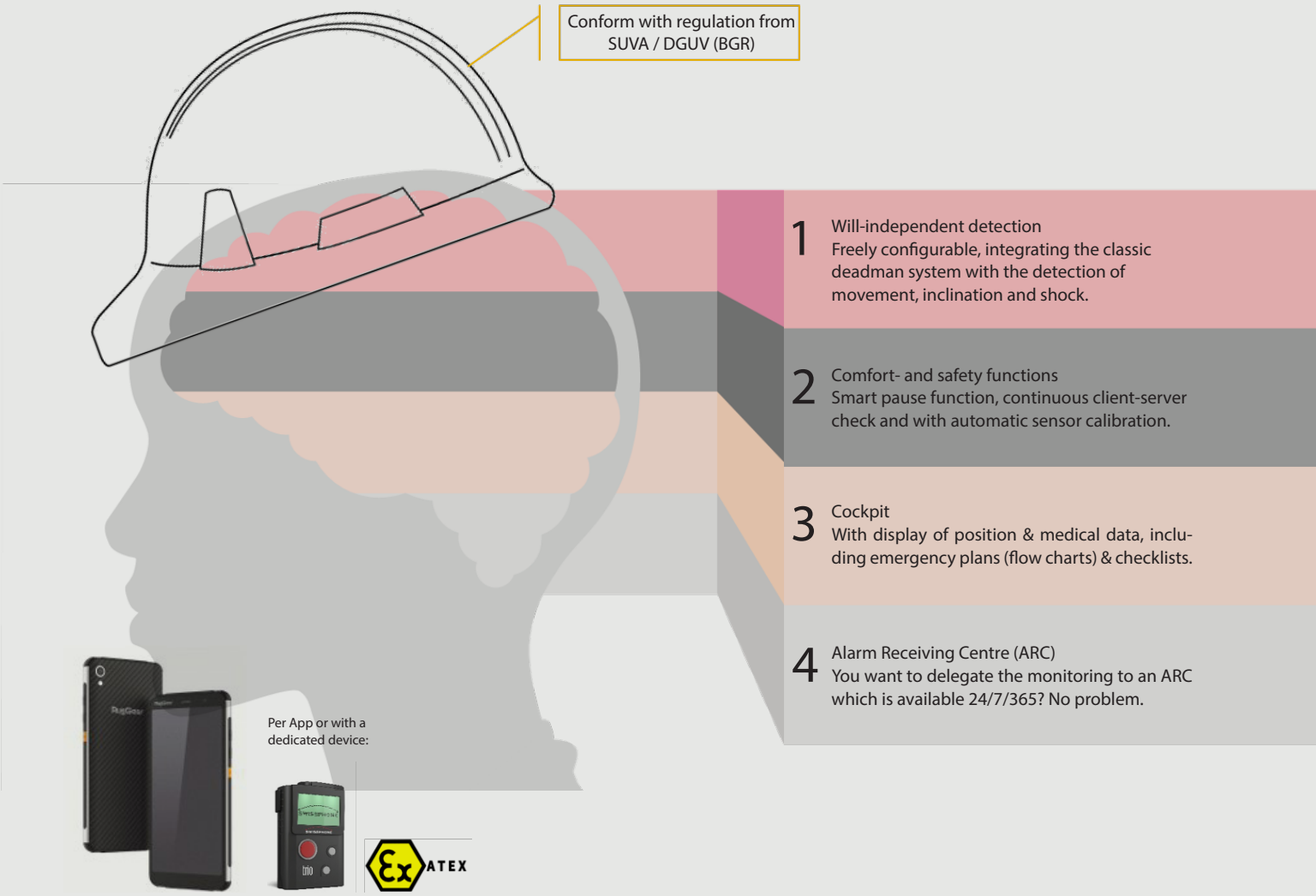
... and to combine escalations

→ → → ...

... and to repeat them

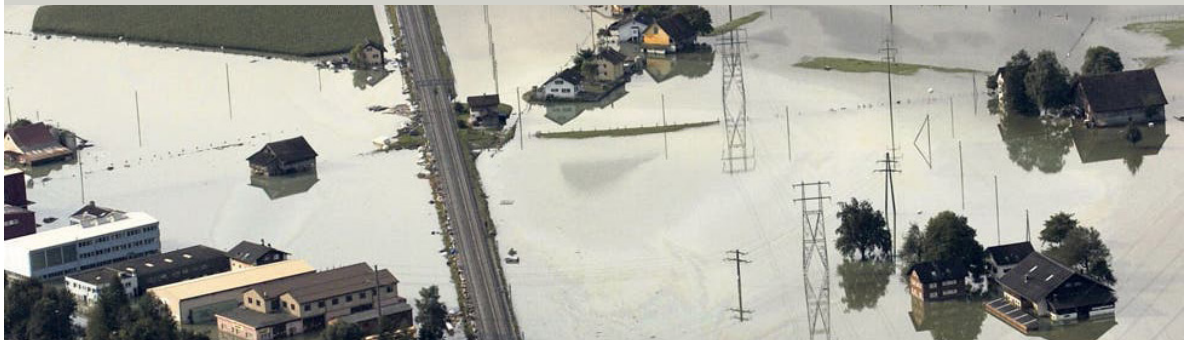
s.GUARD: Module SOS

The intelligent solution to protect your lone workers:



Critical Incident / Example

Natural Disasters



Interfaces à la carte / Open REST API

With s.GUARD you can combine a large number of technical interfaces into a uniform solution for a large number of areas (see below). However, our services go much further than just supporting the most common interfaces:

- Thanks to approx. 100 interfaces, you can integrate as many existing systems as you like.
- The integration of IT monitoring solutions simplifies the life of your IT organisation
- Thanks to the open REST API you can integrate virtually any third-party software

I/O

Open/close, buttons, switches, horns, relays, door opener, technical contacts etc.

Serial Interfaces

Fire alert systems, ESPA 4.4.4, ESPA OUT, ESPA PLUS, Desigo etc

Nurse Call

ESPA PLUS, ESPA-X, ESPA 4.4.4, Gets wireless, Johnson Controll, etc

TCP/IP

OPC UA/DA, Mod-Bus, BAC-Net, KNX, SNMP, SNMP Trap, Commend, XML, Wago, Elevators, Triple M etc.

PBX / TVA

PBX independent SIP, SIP-Q, S0, TO, S2, T2 (Alcatel, Avaya, Cisco, Microsoft, Mitel, Unify, 3CX, Panasonic etc.).

SMTP

Mail reader, Monitoring, Machines, Conversion zu push-, SMS-, Voice- or Paging- Messages.

Printer

Automatic protocols in various languages.

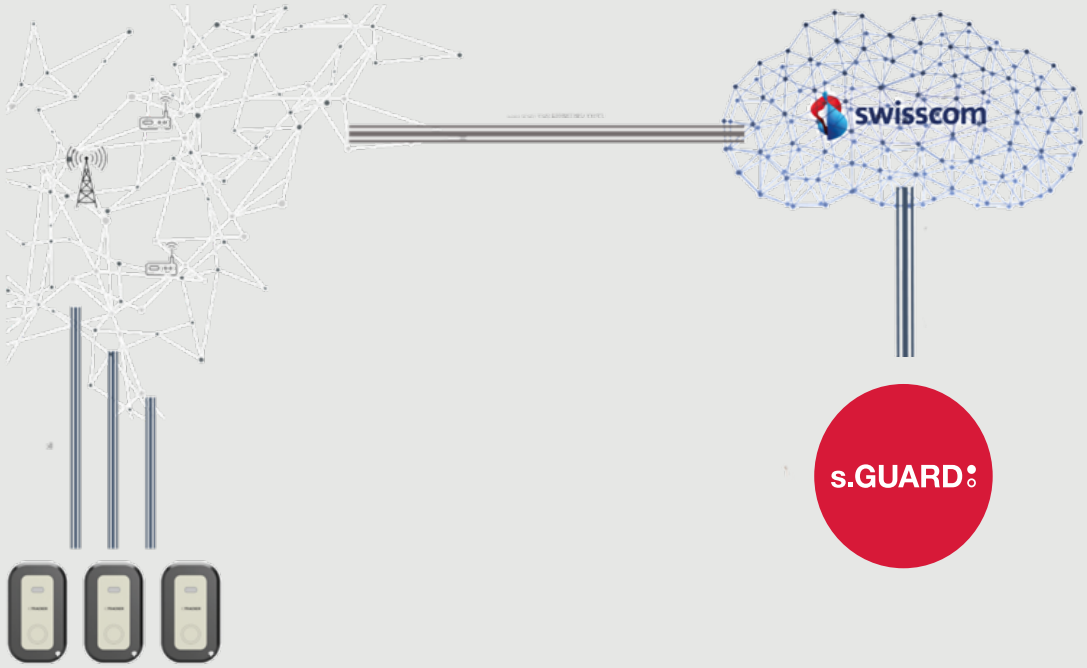
With s.GUARD, you can combine a large number of technical interfaces into a uniform solution: openers/closers, pushbuttons & switches, light call systems, access systems, building management systems, production systems and much more. instaSOLUTION is your partner for alarming and messaging in the fields of facility management, production and also for the special requirements of the health care industry.

- SMTP
- URL / http(s) POST
- REST API
- XML

PRTG NETWORK MONITOR · Nagios XI · ZABBIX · QNAP

IoT

Thanks to the Internet of Things (IoT), many things in the security sector are becoming simpler and more affordable, which means that you can get the most out of your organisation even with limited resources. A variety of sensors and actuators are available, from simple alarm buttons to multi-sensors that measure various environmental influences. Would you like to retrofit an existing system? Nothing easier than that, thanks to the combination of IoT with s.GUARD



Alarm triggering via IoT alarm button: one of many possibilities!

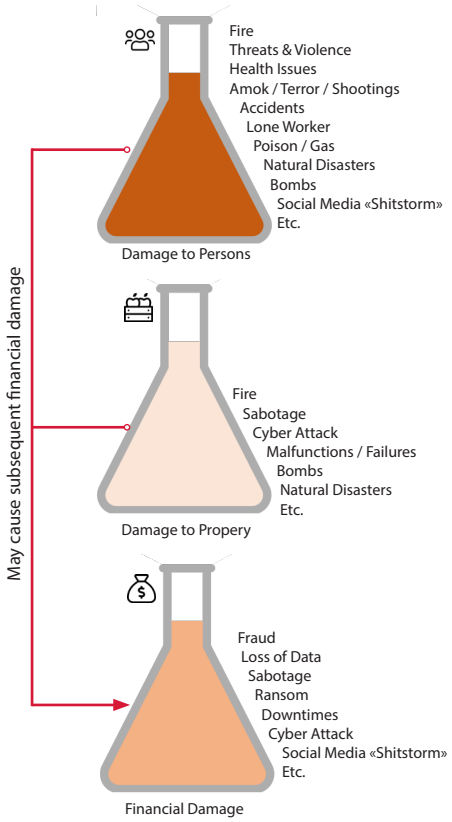
Advantages:

- No wiring
- Mobile & Flexible use
- Several years of battery life
- No interaction with your IT

- Battery warning integrated in s.GUARD
- Connection monitoring integrated in s.GUARD
- Acknowledge with feedback
- AES-128 Encryption

Why Critical Incident Management (at all)?

In a nutshell: Unforeseen critical events cause damage. In the simplest case, this means that e.g. property damage must be repaired, but the consequences can also be far more far-reaching. Even if, for example, personal injuries are immaterial (i.e. not directly of monetary value), it is still worth considering damages from a business and, above all, from an insurance and legal point of view:



Damage to Persons: Damage to persons is caused by injury to the body or health (also: mental health). The obligations of the employer in this respect are regulated, for example, in Article 6 of the Swiss Labour Code. By definition, personal injury is immaterial (i.e. not of monetary value), but can result in consequential financial losses, e.g. compensation for pain and suffering, fines, treatment and procedural costs and, of course, the loss of a valuable employee. Furthermore, personal injuries also lead to damage to the image of a company and to reduced motivation of employees, even if they are not directly affected. Both have a negative impact on your business and therefore represent a direct financial loss. In addition: Apart from all economic and legal considerations, the protection of employees also represents a moral value

Damage to Property: Damage to property is any degrading effect on the condition of an object which impairs its economic usability for the intended purpose. This can range from slight scratches (e.g. on car paint) to complete destruction (e.g. of a building). And, of course, property damage can also result in consequential financial losses. Water damage in a computing center destroys e.g. a hard disk (a property damage), the effort to be made to restore the data stored on it or the impairment of your employees (due to the failure) are however consequential financial losses.

Financial Loss: Financial loss is defined as damage to an asset with a legal owner, i.e. an incurred pecuniary disadvantage of a natural person or a legal entity. A distinction is made between real/pure and «unreal» financial losses. A real/pure financial loss is defined as a situation in which neither a person nor an object suffers direct damage, but nevertheless financial loss occurs, e.g. through fraud or theft, but also through a reduction in added value or profit, e.g. through operational disruptions and loss of production. «Unreal» financial loss, on the other hand, is the consequential loss resulting from personal injury or damage to property.

What the insurance pays (or NOT)

The case is relatively simple if your employees or your company cause personal injury or property damage to a third party. These - including consequential financial losses - are covered by your third party liability insurance. It already becomes more difficult with a pure (real) pecuniary loss to third parties, e.g. one of your employees defrauding a client: For this you already need a financial loss liability insurance. The situation becomes even more complicated with internal losses. Now, you may have property insurance (buildings or objects) as well as accident and per diem sickness insurance.

However, these insurances do not cover expensive consequential damage and damage to reputation. And the annoyance that arises for you will certainly not be covered.

«In simple terms, a critical incident management system is a very effective and inexpensive insurance against damage that you cannot otherwise cover or can only cover with extremely high premiums.»

Features & Advantages: s.GUARD

You connect what needs connecting. You can choose freely between a multitude of inputs and outputs (App, SMS, etc, see page 3) and of course you can define several inputs and outputs per event. Thanks to instaCORE, your information flows safely to the right place.

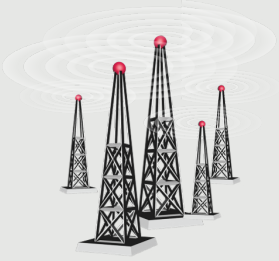
You can have any number of users per tenant. We are happy about 10 as well as about 10000 users.	Administration: You can securely access the web-based administration interface from anywhere.
You can freely attribute users into user groups; one user can be part of several groups.	User import: You can import new users manually, via csv import or via Active Directory integration.
You can easily define notification processes, i.e. determine who is informed when and how (e.g. via app).	You can choose between 4 authorization levels; depending on the level, more or less can be adjusted in the administration.
You can define any number of events (e.g. fire location A, survey employee B) and assign any users to them.	You can assign a language to each user individually. In the case of an event, the information flows in this language.
For each event you can determine which information should flow (e.g. text, images, sounds, position, documents).	Users can opt out of receiving messages, in their entirety or just for certain events.
You can escalate to other people, groups and events if there is not enough feedback.	As administrator, you can also deactivate entire events temporarily or time-controlled, e.g. for planned maintenance work.
Depending on the feedback, the event is set to the status open, confirmed or in progress.	With schedules you can define exceptions for holidays, weekends and more with just a few clicks.
At any time you have an overview/log of the feedback in the app, during the event or afterwards.	With ad-hoc user groups you can spontaneously inform only certain persons about an event via app.
Our 3-times clustered, georedundant server architecture guarantees maximum uptime and maintenance without interruption..	All changes to your settings are logged and all your data and settings are regularly backed up.
The sensitive data of your users are protected; we and our solution are GDPR-compatible.	A large number of inputs and outputs can be monitored at high frequency using a heartbeat.
Multifactor authentication prevents unauthorized persons from accessing the system (app & system administration).	Redundancy in communication channels and networks protects you against infrastructure failure.
All data is encrypted end-to-end, both in the dormant state and during transmission.	Our customer service is available 24/7/365 to ensure the optimal operation of your system.

We Connect People and Systems

With our modular, highly secure and flexible connectivity platform s.GUARD we connect what needs to be connected:

Our Focus s.GUARD	s.GUARD is your alerting and mobilization solution that allows you to communicate with a variety of channels. Thanks to intelligent feedback, you have a full overview at all times. Images, texts, sound and tags and much more create the information that is essential for targeted action.
Additional Modules s.GUARD COLLAB s.GUARD IOT s.GUARD MSG s.GUARD SOS	COLLAB Smart TelCos, Chat, Documents etc. IOT The Internet of Things MSG Messaging SOS Lone Worker Protection
Coming soon s.GUARD TASK s.GUARD FLOW s.GUARD REPORT	TASK Smart Task Management FLOW Processmanagement & Prevention REPORT Reporting of Potential Dangers

Platform / s.GUARD



Networks / Paging & MIOTY

Terminals / Pager

TELEPAGE® (Switzerland only)

All Use Cases, across the entire Alerting Chain

s.GUARD can be used for a virtually unlimited number of use cases - not least thanks to the add-on modules. The examples below are not exhaustive, and if you do not see your use case: Ask us, we will be happy to help you.

Prevention

- Training Sessions
- E-Learning
- Manuals
- Guidelines
- Near Miss Management
- Reporting
- Etc

Messaging

- 2FA
- Reminder
- Simple Info / Alert
- Etc

Fault Management

- Facility Management
- Productions Management
- Access Management
- IT-Alerts
- Etc

Mobilization

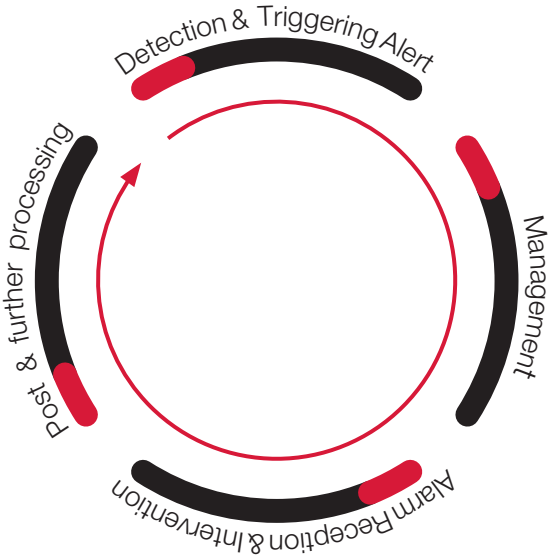
- Nurse Call
- Winter Road Maintenance
- General on-call service
- Etc

Emergency Management

- Threat
- Fire
- Evacuation
- Amok
- Lone Worker
- Medical Emergencies
- Cyber-Attacks
- Etc

Crises Management

- Crisis Management
  - Mobilzation
  - Digitaler Crisis Room
  - Collaboration & Communication
  - Etc



Cloud, On-Premise or Hybrid?

s.GUARD can be deployed exactly as you want it, as a public cloud, private cloud, on-premise or hybrid solution. Now what is what?

On-Premise	Private Cloud	Public Cloud	Hybrid Cloud
Your Servers	„Your“ Servers	Provider‘s server	„Your“ Server & Provider
In your Network	External Data Centre	External Data Centre	Int. & Ext. Data Centre
Operated by You	Operated by You/Provider	Operated by Provider	Operated by You/Provider
(Partially) requires Internet	Requires Internet	Requires Internet	(Partially) requires Internet
Single Tenant	Single Tenant	Multi Tenant	Single & Multi Tenant

Which is the optimal solution for you can only be answered by considering your individual circumstances. Relevant questions here can be:

- Are you forced for regulatory reasons to keep the data relevant for alerting in-house?
- Do you have an IT department that can operate the solution with greater than 99.99% availability?
- What are the costs and how transparent are they?
- Which variant can be implemented and how quickly?
- To what extent do you depend on the Internet?
- How well does each variant scale?
- With which variant do you get which support?
- Finally: What is important to you?

Qualitatively, the on-premise and public cloud variants can be compared as follows, with private cloud and hybrid cloud ultimately being mixed models that combine the advantages and disadvantages of the other two variants:

	On Premise	Public Cloud
Cost	Higher initial investment / Overall, e.g. over 10 years, higher costs.	Lower initial investment / overall, e.g. over 10 years, lower costs.
Transparency	The internal costs (maintenance, hardware, etc.) can often not be made transparent	Full cost transparency, as only annual license fees are charged, and nothing else.
Data Protection	Your data stays with you, and you are responsible for its protection.	Your data is with us, and we are responsible for its protection.
Availability	Your servers are your responsibility, and you determine the uptime.	The servers are our responsibility, and we therefore determine the uptime.
Skalability	Is ultimately limited by the hardware you use.	Quasi no limitation, the solution scales globally, flexibly and smoothly.
Time to Value	Since there is more work to be done initially, it usually takes some time before you can deploy the solution.	Depending on the complexity of the solution, you can work with it within days or weeks.
Support	Since responsibility is shared, support services will also need to be shared.	Virtually everything comes from a single source, and accordingly the responsibility for support is clear.

Swissphone

Critical Incident Management for Professionals

We are Swissphone

The Swissphone Group is your full-service provider for alerting solutions for emergency response organizations and comprehensive critical incident solutions for companies and the public sector. We serve you with all the technical tools you need to manage critical incidents across the entire alerting chain, whether in crisis, emergency, incident or prevention. Our solutions can be operated autonomously or fully networked, and are available to you in the cloud, on-premise or hybrid.

Our Strenghts:

check	**Our philosophy: Built for you!** Based on a solid foundation, we integrate a variety of proven components and tools into a coherent overall solution that is precisely tailored to your needs. And if you want a really special component or interface: Gladly!
check	**Technology of Today** The methods and technologies we use are state of the art today and will remain so tomorrow without exception, giving you the assurance that your solution will continue to meet your needs in the future
check	**Customer Support & Service** Your needs are our priority and we live service. Our employees are available to you at all times during the project and operation, and our flexible services aim to provide you with exactly what you need.
check	**IoT** With IoT, you can make processes in your organization more efficient, effective and transparent thanks to the link between the physical and digital worlds. We are your contact partner from idea and solution generation to implementation and operation.
+	**And of course: Swissness, Security & Data Protection** As Swiss companies, we are committed to the traditions of quality, security and data protection. We guarantee you reliability.

Cloud
Hybrid
On-Premise

Crises
Emergencies
Malfunctions
Prevention

Platform
Networks
Terminals

Autark
and/or
Fully networked

SWISSPHONE

Contact us: Long Range Systems UK Ltd,
Link House, 1880 Leek Road, Stoke on Trent, Staffordshire, ST27AH
Tel 0843 506 6000 Visit https://twowaypaging.com