Celab
COMMUNICATIONS

Guide to robust communication systems

How do you strengthen communication systems so they can withstand the challenges of incidents, crises and war?

Guide to robust communication systems

How do you strengthen communication systems so they can withstand the challenges of incidents, crises and war?

The answer is: it depends entirely on your organisation. Different preparations and measures are required depending on your operations, your current communications environment and your requirements.

By robust communication, we mean systems that can maintain sufficient or acceptable function even during disruptions, outages or increased load.

This article is intended to provide guidance on different ways of thinking that can help you develop and/or complement your communication systems in order to improve resilience against potential threats — and thereby meet both internal and external requirements and expectations.

This article is part of a series intended to help you "bulletproof" your mission- or business-critical communications environment. We recommend reading the articles in the following order:

- Introduction to Preparedness Communications — Why prepare?
- Guide to Risk Analysis for Communication Systems — What can go wrong?
- Guide to Robust Communication Systems — What can we do about it? (this article)
- Guide to Reliable Backup Communications — What do we do when that is still not enough?

The overall purpose of this article series is to give you a number of "lenses" through which you can examine your communications environment, making it easier to identify appropriate measures for your specific conditions.

Since this guide only addresses how existing systems can be strengthened, it assumes that you already understand the practical communication needs and functions, as well as how these are provided. The review may also benefit from involving a supplier, consultant or internal resource with in-depth knowledge of the technical possibilities and limitations.

Increase Resilience

To create resilient systems, the system or systems need to be examined from several different perspectives. This applies both at an overall level and in detail, and from both internal and external viewpoints.

The different perspectives should help you:

- **Identify different ways to manage and/or eliminate risks identified in risk and vulnerability assessments.**
- **Find methods to prevent unnecessary future risks.**

1. Reinforcement

The first activity is about identifying the system's more or less obvious Achilles' heels. Here, each individual component in the system needs to be inspected and potentially replaced in order to produce a truly stable system.

Examples of Control Points

Category	Component	Questions	Possible measures
Software	Firmware, antivirus, firewalls, etc.	Release, version, specification?	Update, replace, upgrade.
Active components	Base stations, repeaters, servers, routers, etc.	Age, specification, installation, condition?	Maintenance, repair, replacement, upgrade.
Passive components	Antennas, cables, connectors, etc.	Age, specification, installation, condition?	Repair, replace, upgrade.
Safety equipment	Surge protection, residual-current devices, lightning protection, etc.	Age, specification, installation, condition?	Repair, replace, upgrade.
Dependencies		Is the system, or any part of it, dependent on other systems, services or suppliers?	See the following sections.

- **By specification, we mean verifying that the stated performance, capacity and quality of the component are aligned with the requirements.**
- **By condition, we mean the general health of the component in terms of wear and similar factors.**
- **By installation, we mean checking that the installation is correct, well executed and protected.**

2. Redundancy

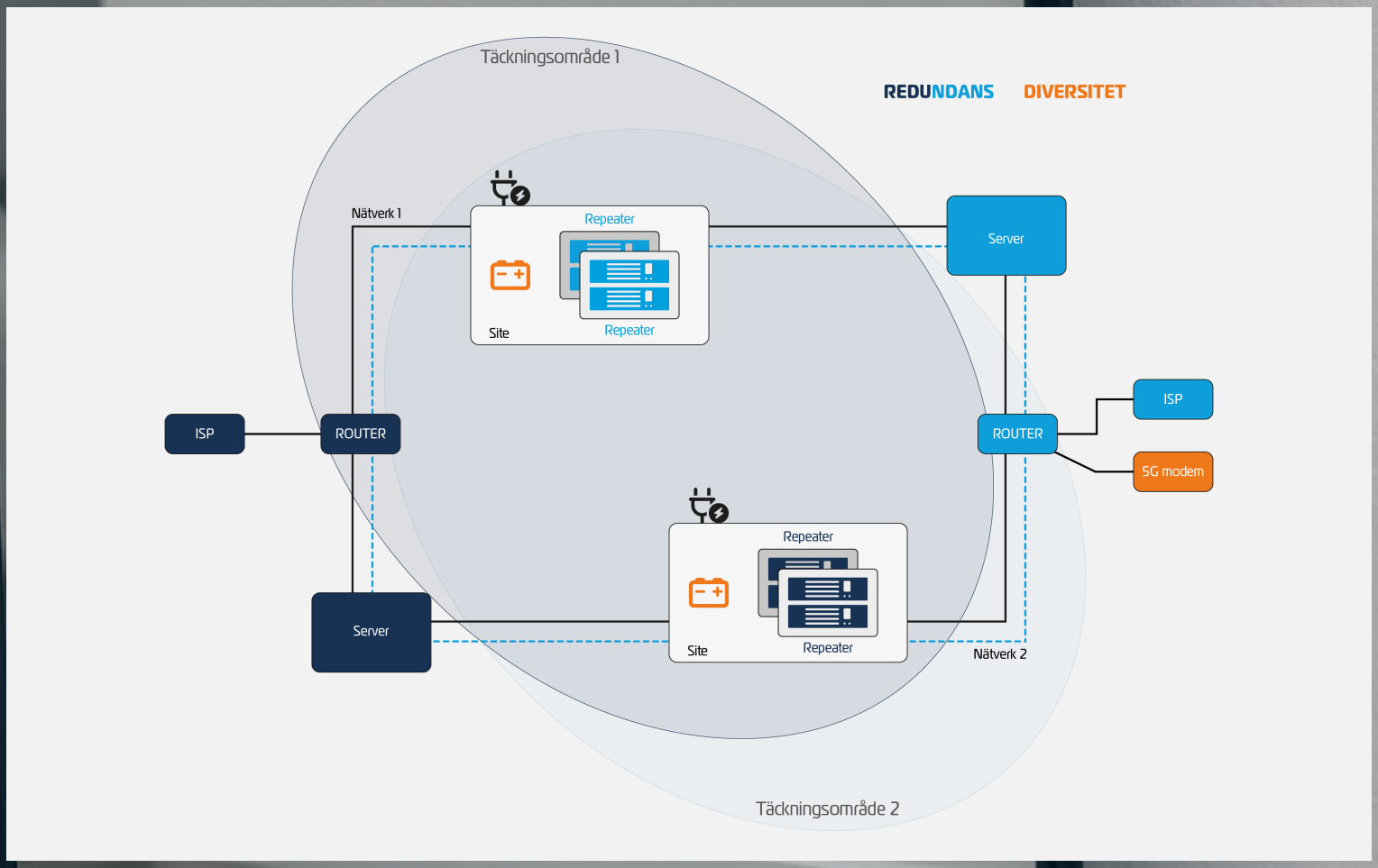
Redundancy means that there are extra resources, backup routes or alternative solutions that can take over if something stops working.

In a communication system, redundancy can consist of dual network connections, backup power, multiple servers, alternative base station sites, additional terminals or a separate backup communication system.

The goal is not always for the function to remain completely unchanged from the user's perspective. In some cases, it is enough that sufficient function is maintained until the fault can be remedied. The important point is that a single fault should not immediately cause the organisation to lose its ability to communicate.

Examples of Control Points

Category	Bottlenecks	Possible duplication
Dependencies	Internet connection	Parallel fibre connection from another ISP.
Active components	Base station sites	Dual sites with overlapping coverage areas.
	Modem, server, router, etc.	Speglad server-arkitektur. Virtuella miljöer.
Passive components	Networks, cables, connectors, etc.	Parallel installations. Overlapping coverage areas.


Täckningsområde 1
REDUNDANS
DIVERSITET
Nätverk 1
Repeater
Server
Site
Repeater
ISP
ROUTER
ROUTER
ISP
5G modem
Repeater
Server
Site
Repeater
Nätverk 2
Täckningsområde 2

3. Diversity

Diversity means that redundant solutions differ in technology, route, supplier, location or dependencies.

The purpose is to reduce the risk of common-cause failures. For example, two connections may be redundant, but if they run through the same ducting, both can be knocked out by the same excavation work. Two subscriptions may provide some redundancy, but if they use the same underlying mobile network, diversity is limited.

Diversity is therefore not only about duplication, but about ensuring that the backup solution is sufficiently independent from the primary solution.

Examples of Control Points

Category	Bottlenecks	Potential redundancy
Dependencies	Power supply	UPS, battery backup, backup generator.
	Internet connections	Mobile and/or satellite connection.
Active components	Base stations	System-specific functions.
	User devices	Direct mode, such as two-way radio.

4. Monitoring

No matter how robustly a system is built, there is always a risk that individual components will fail or malfunction. For this reason, some form of monitoring and alerting is essential in order to avoid, limit the extent of or shorten the duration of potential problems.

Automatic monitoring may be built into the system or may need to be implemented using additional hardware and/or software. In simplified terms, these solutions work in two main ways:

- **Continuous monitoring: The system is actively monitored and automatically issues alerts when faults occur.**
- **Health check: The system is queried at regular intervals and responds with either OK or fault.**

Where automatic monitoring is not possible or not sufficient, regular manual function checks based on a defined checklist may be required.

In combination with the measures mentioned earlier, monitoring makes it possible to carry out repairs, replacements and other corrective actions before the function of the system is affected.

5. Separation

Geographical Separation

This is an extension of both diversity and redundancy, where mirrored and/or failover solutions also need to be physically separated.

This may involve server rooms in different buildings, separate cable routes or a mix of wired and wireless connections — all in order to spread vulnerabilities and thereby reduce risk.

Dependencies

If one or more dependencies have been identified that cannot be managed through diversity or redundancy measures, these may require further investigation.

The purpose is to determine whether the dependencies should and can be avoided entirely, or whether satisfactory robustness can be achieved despite the dependency in question.

6. Access

Under this heading, access to the system — both physical and virtual — should be assessed and limited to what is absolutely necessary. The purpose is to prevent problems caused by human factors, whether unintentional or intentional.

Entry point / Opening	Possible measure
Virtual ports	Close or hide.
Physical areas	Lock and restrict access.
Virtual permissions	Limit permissions.

7. Service Level

The final point is to review or establish a service level agreement that ensures that maintenance, repairs and other corrective actions can be carried out to a sufficient extent and with sufficient urgency.

Regardless of whether the agreement is standardised or customised, the service levels should reflect the organisation's tolerance for outages and disruptions.

Replacement Equipment

The analysis may show that individual components need to be readily available for replacement when required. Such replacement equipment may be included in an SLA, but it may also be worth investigating whether it is more practical to purchase and store these items locally.

Conclusion

Technology Choice

Can your current system be improved in all necessary areas in order to achieve the desired or acceptable level of resilience?

If the answer is no, it may be worth investigating whether other technologies or systems would allow you to achieve acceptable resilience.

Backup Communications

If you have carried out a complete review of your communications environment and implemented all possible measures according to this article, but still cannot eliminate all relevant risks, a backup communication system may be necessary.

More on that in the next article in the series: Guide to Reliable Backup Communications.

About Celab

+46 (0)303 24 60 00
info@celab.se
https://celab.se

Celab Communications AB is a Swedish company within the Tången Group that, since its founding in 1978, has achieved significant success in mission- and business critical communications.

By this, we mean solutions for organizations where reliable communication is essential to operational success and/or employee safety.

The company's foundational concept is to provide communication systems based on world-leading equipment, which, through our unique expertise, are developed, refined, and optimized specifically for our customers and their unique operations.

Celab COMMUNICATIONS

HQ Rollsbovägen 20, 442 40 Kungälv
Stockholm Elsa Brändströms gata 56, 129 52 Hägersten
Karlstad Lagergrens gata 2, 652 26 Karlstad