



# IT Security for Meteorological Measuring Networks



Dipl.-Ing. Gerhard Pevny

Logotronic GmbH Vienna, Austria

[gerhard.pevny@logotronic.co.at](mailto:gerhard.pevny@logotronic.co.at)

Mag. Roland Potzmann

ZAMG - Zentralanstalt für Meteorologie und Geodynamik

Vienna, Austria

[roland.potzmann@zamg.ac.at](mailto:roland.potzmann@zamg.ac.at)



# Overview



- Motivation for the project
- Basic technical requirements
- Basics of IT-Security
- TAWES technical solution
- Conclusion and actual state of the project

# Motivation for the Project

- TAWES - The Austrian public meteorological measuring network operated by ZAMG
- Since 2005 about 300 AWS
- In the beginning data transfer via modem over telephone lines (TUS), GSM
- In the last years change to Internet technologies on all levels (communication, datalogger, video cameras, ...)



Increasing risk of hacker attacks



# Motivation for the Project

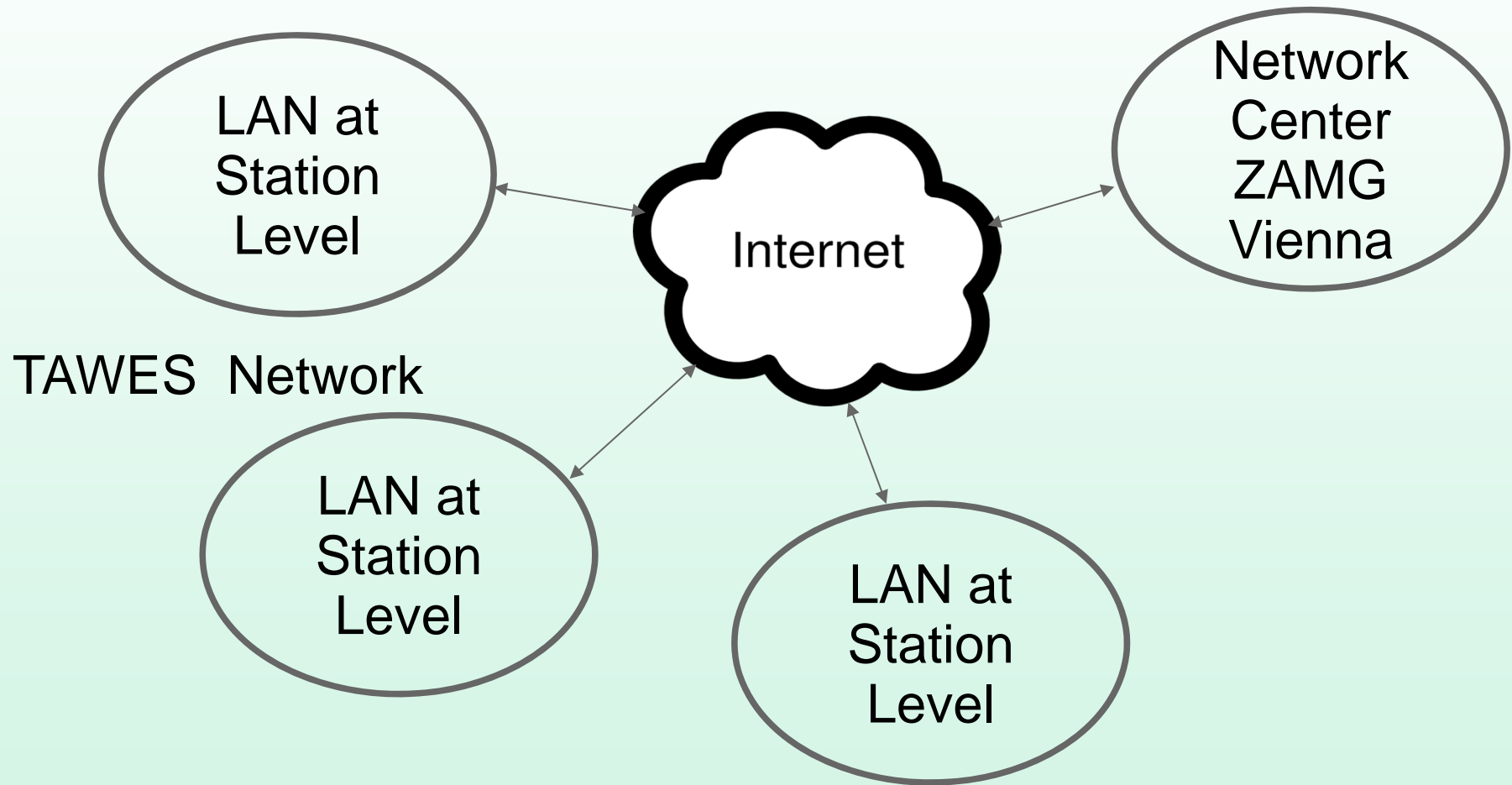


## Project targets

- Best possible IT security for AWS, central servers and maintenance workplaces
- Prepared for the Internet of Things - IoT
- Long system lifetime although using latest technological standards
- Independence of proprietary security solutions offered by service providers
- Update of the existing, well working measuring network, no complete replacement



# LAN at Measuring Station Level - TAWES V2.0





# Basic Technical Requirements



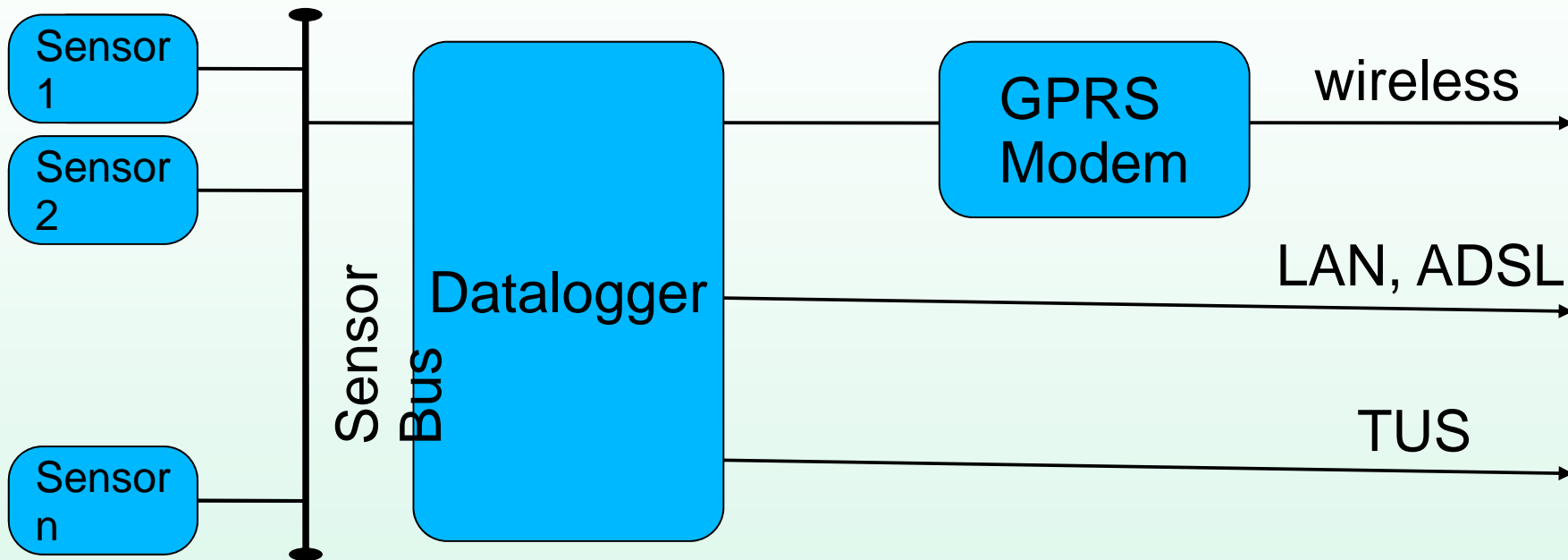
- Application of only well proven Internet standards
- No proprietary software nor proprietary protocols on network level
- Long system lifetime by using well established open source software and standard hardware from the shelf, for the network components, no „black boxes“ in the system
- Modular extension of the existing TAWES stations. Should be applicable also for other station-types.

The technical solution has to guarantee all of the following 4 IT-security requirements:

- **Authenticity** -> You can be shure, that you communicate with the right partner
- **Confidentiality** -> Only you can see yor data
- **Data integrity** -> What´ s sent is also received
- **Protection against malware**



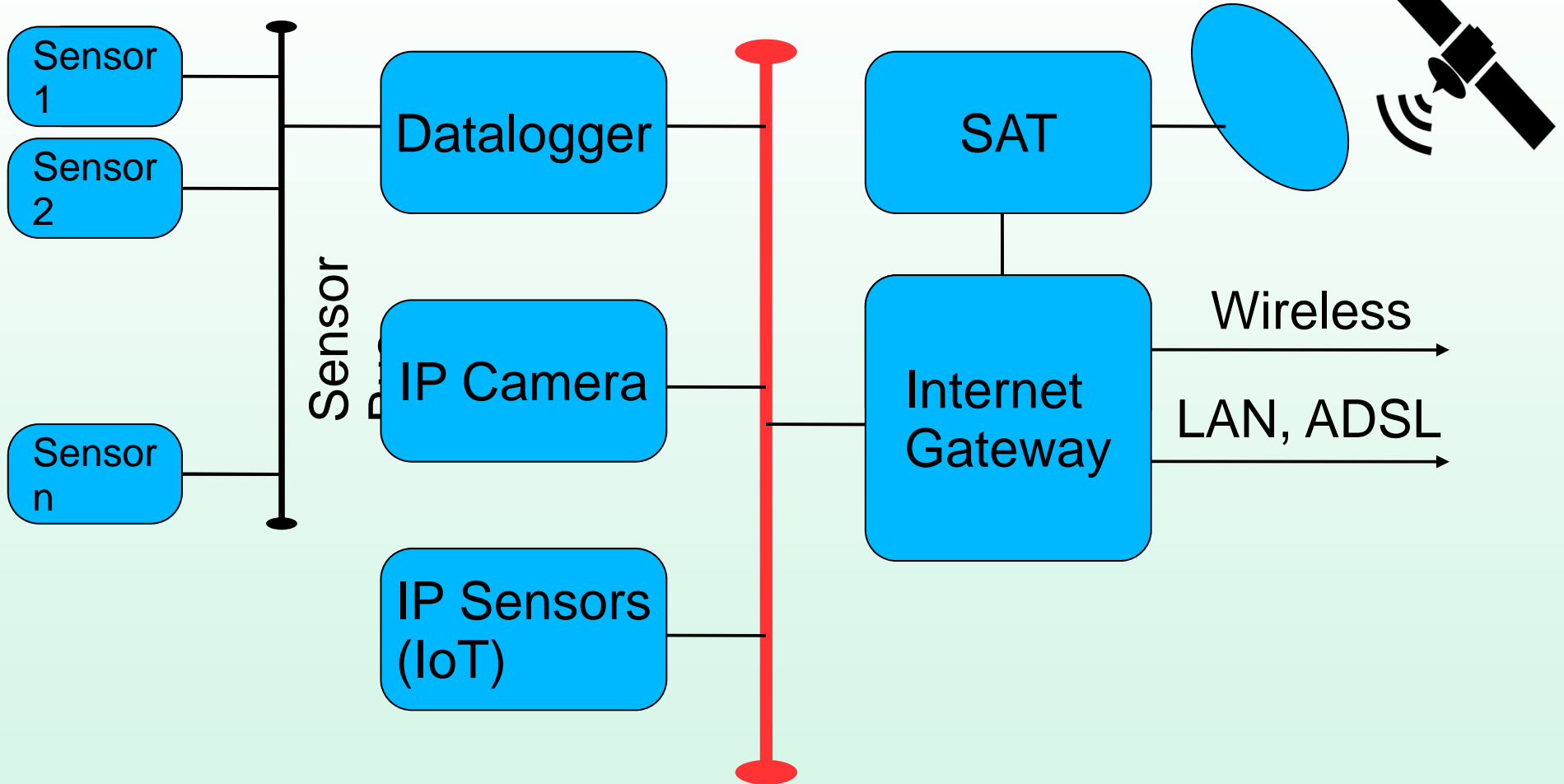
# TAWES V2.0 AWS Structure



Original TAWES Station Layout



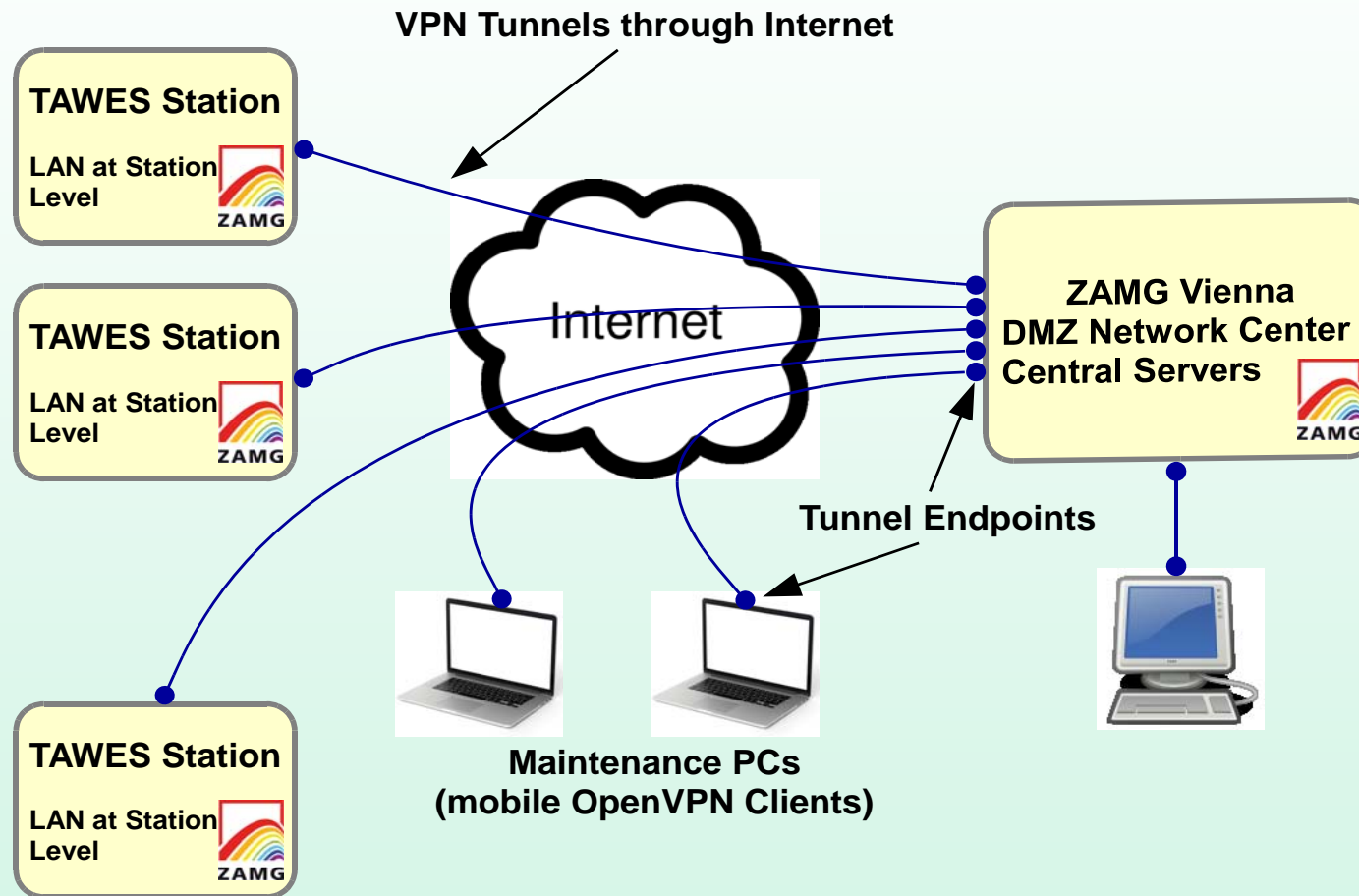
# TAWES V2.0 AWS Structure



TAWES V2.0 - Ethernet LAN at Station Level



# Technical Solution TAWES V2.0



# Tunnels through Internet



VPN Tools for creating tunnels:

- IPsec (Internet Protocol Security)
  - Old Internet standard, works on Internet Layer  
-> completely transparent for applications
  - perfect for point to point applications
- OpenVPN
  - Open-source application
  - perfect for remote-access applications



# IPsec - OpenVPN



Both systems are applied in TAWES V2.0

- IPsec  
Routine data transfer - point to point - AWS to server
- OpenVPN  
Maintenance network - remote access to all network modules
- Logically completely separated VPNs



# Authentication



Authentication by digital certificates (X.509 standard) = ID-cards for all network members

Advantages:

- One certificate per user
- Central administration of certificates by TAWES CA (Certification Authority)
- Easy installation of certificates at AWS and maintenance PCs
- Flexibility:  
Certificates with limited validity period, TAWES certificate revocation list



# Confidentiality, Data Integrity, Malware



- Both IPsec and OpenVPN offer highest security level by flexible and scalable encryption methodes
- Same security level as for i.e. money transfers
- Tunnelling offers the possibility to close stations and servers completely against all access from outside the TAWES network by simple firewall rules. Only data traffic inside tunnels is allowed.



# Additional Benefits



Additional benefits coming with nearly no additional effort by using this technology:

- AWS are establishing the VPN --> two-way communication without fixed station IP-addresses, the VPN, not the network provider is creating fixed addresses
- Hierarchical TAWES NTP-time synchronization
- TAWES DNS server, access to AWS by symbolic station name (url)
- Easy integration of satellite services (Internet via Sat)  
Actually in test operation: Inmarsat, Thuraya, Eutelsat TooWay
- Complete network communication monitoring by use of „Packet Capture“ functionality on all system levels.

# Conclusion, actual State of Project

- Laboratory tests ongoing since some months
- Field test operation just starting with a small number of AWS, but with complete network functionality including sat- and video-systems.
- Field test planned for about 6 months.



Field-Testbox