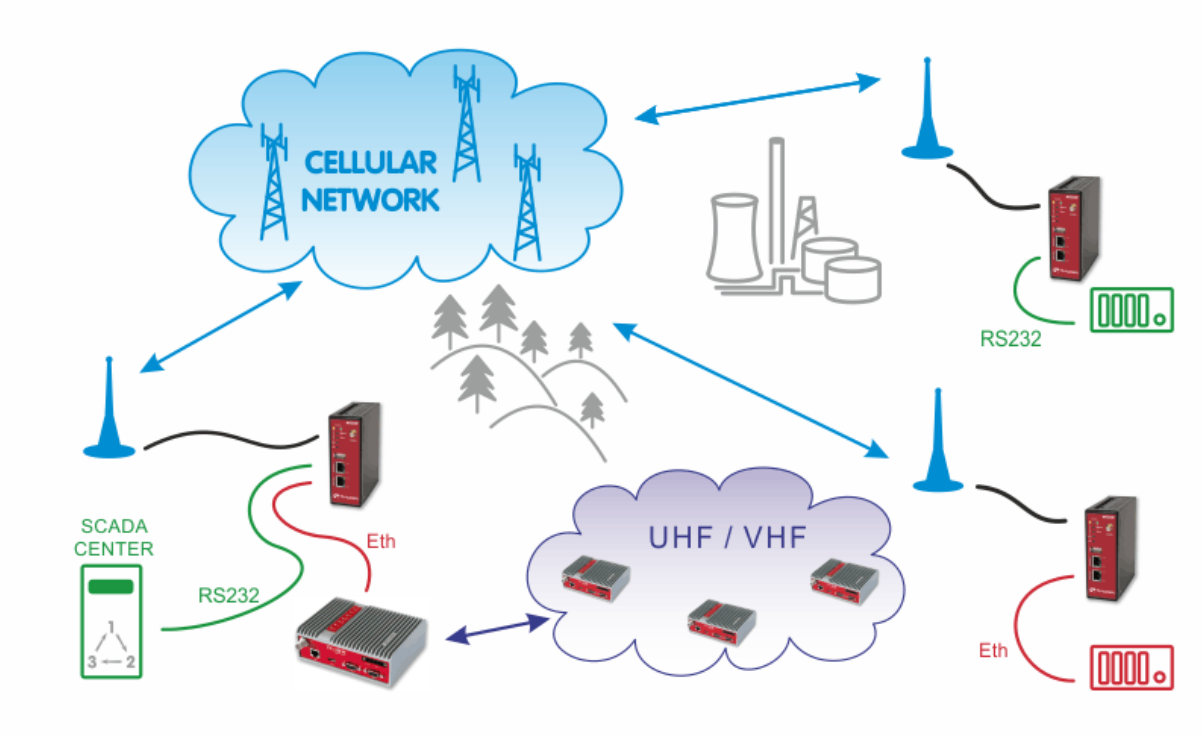
RACOM
RADIO DATA NETWORKS

Application notes



M!DGE/MG102i - Typical usage

version 1.1
3/2/2018

RACOM s.r.o. • Mirova 1283 • 592 31 Nove Mesto na Morave • Czech Republic
Tel.: +420 565 659 511 • Fax: +420 565 659 512 • E-mail: racom@racom.eu

www.racom.eu

Table of Contents

Introduction

This chapter is intended to be a brief overview of typical cellular network applications. If noted, a detailed example with all configuration steps is given. If there is anything missing or is unclear, do not hesitate to contact technical department for details via the <support@email.eu> e-mail address.

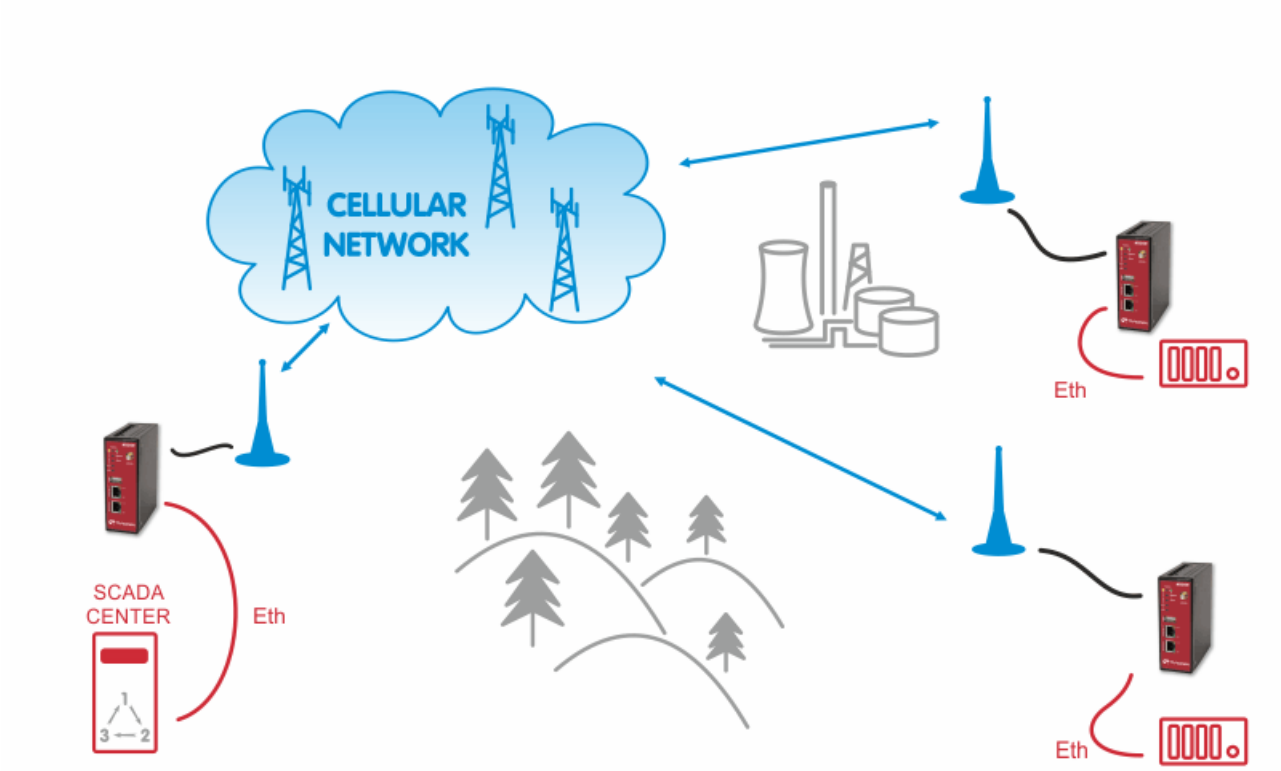
Note

While the terms “SCADA center” and “RTU” are used in the following pictures, any other device (ATMs, lottery terminals, surveillance cameras, etc.) with the same interface type (RS232, ETH) can be used.

1. A Standalone M!DGE/MG102i in the Center

This simple and easy solution is feasible for small networks with up to about 20 M!DGE/MG102i units. Note that the center reliability in this arrangement is limited by the reliability of the Cellular service in the central location.

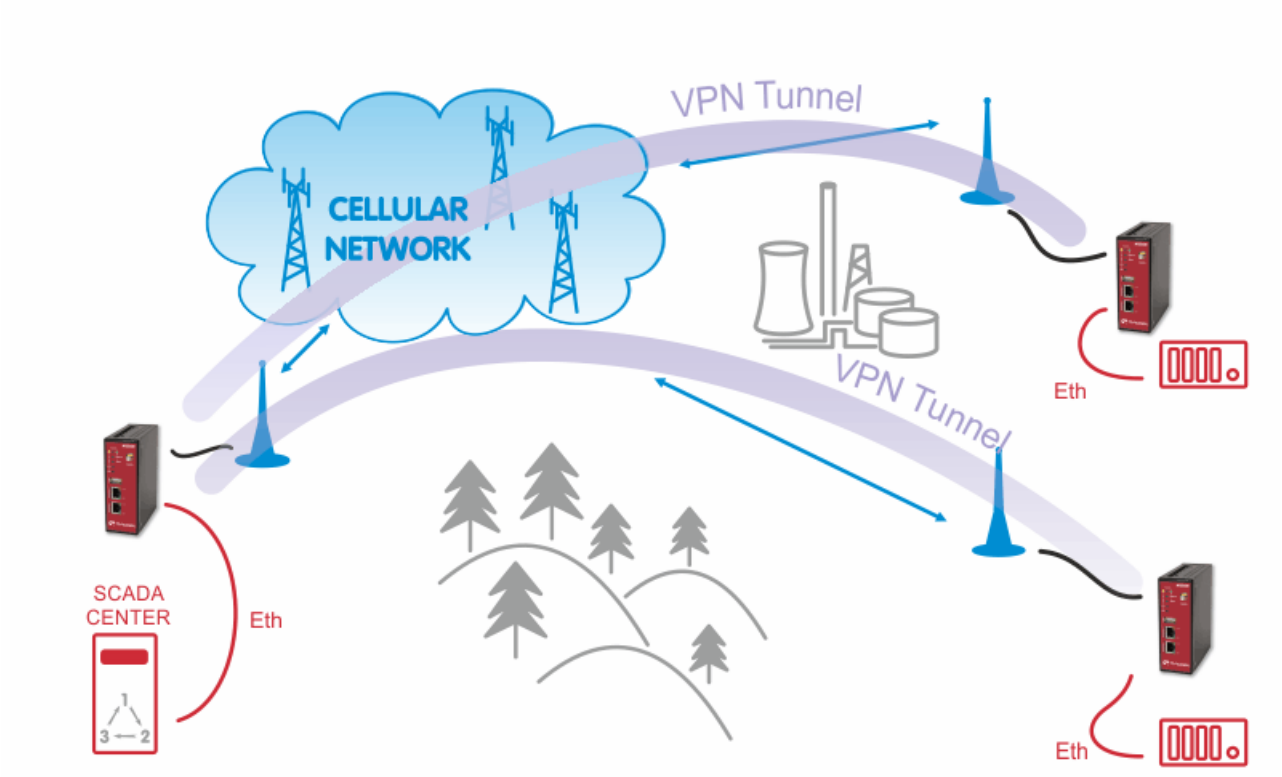
1.1. Central M!DGE/MG102i – without VPN tunnels



This solution is possible if

1. you have your own APN within the defined private IP subnet.
2. all the units within the general “internet” APN have public IP addresses which are given statically or dynamically (usage of Dynamic DNS is a must in this case).

1.2. Central M!DGE/MG102i – with VPN tunnels



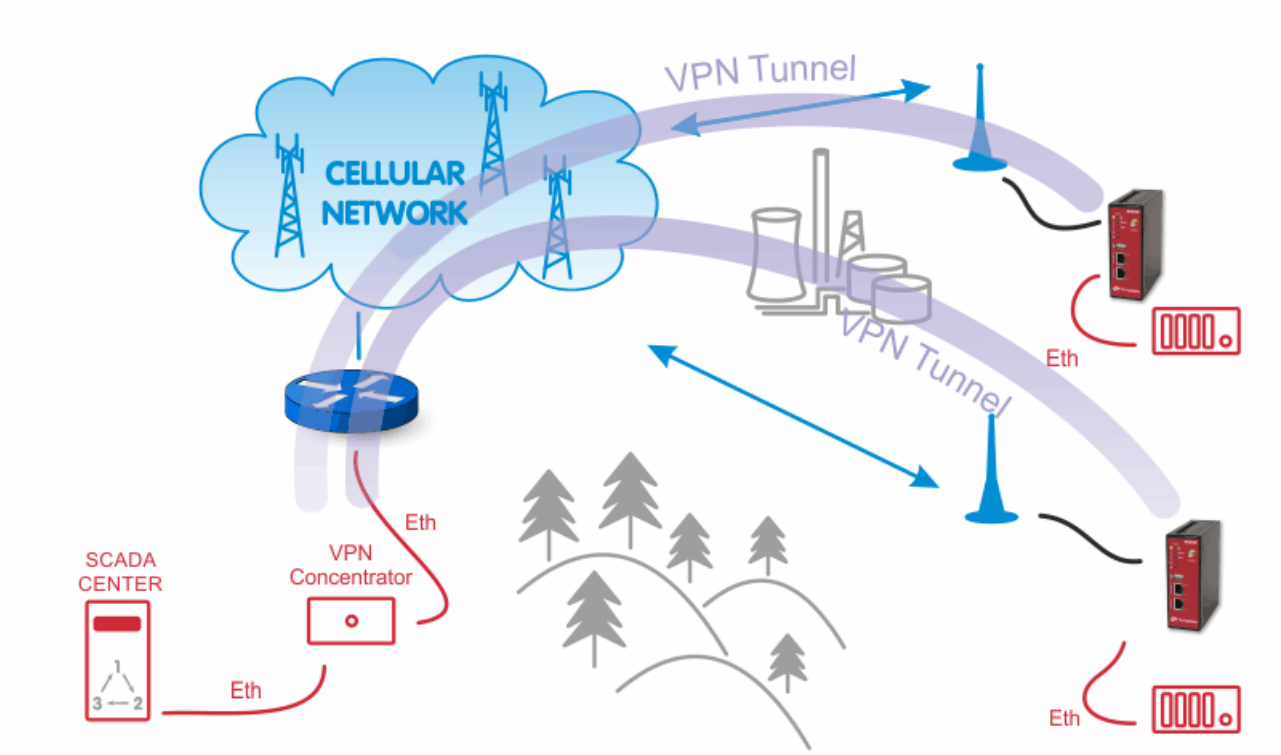
The central unit must be reachable from all clients. The central unit must have the public IP address which can either be static or dynamic. In case of dynamic IP address, the dynamic DNS functionality has to be configured and enabled.

The clients can have static or dynamic IP address even within the private range, thus not reachable from “Internet”. After establishing the VPN tunnel with the server, the subnets between the server and clients are reachable as required.

VPN Tunnels have to be initialized from remotes to the center. The M!DGE/MG102i in the center is capable to simultaneously handle up to 10 OpenVPN tunnels (or up to 25 with Server feature key) and 4 IPsec tunnels. This means that up to 25 remote units are possible for the first application and other four units for the second application.

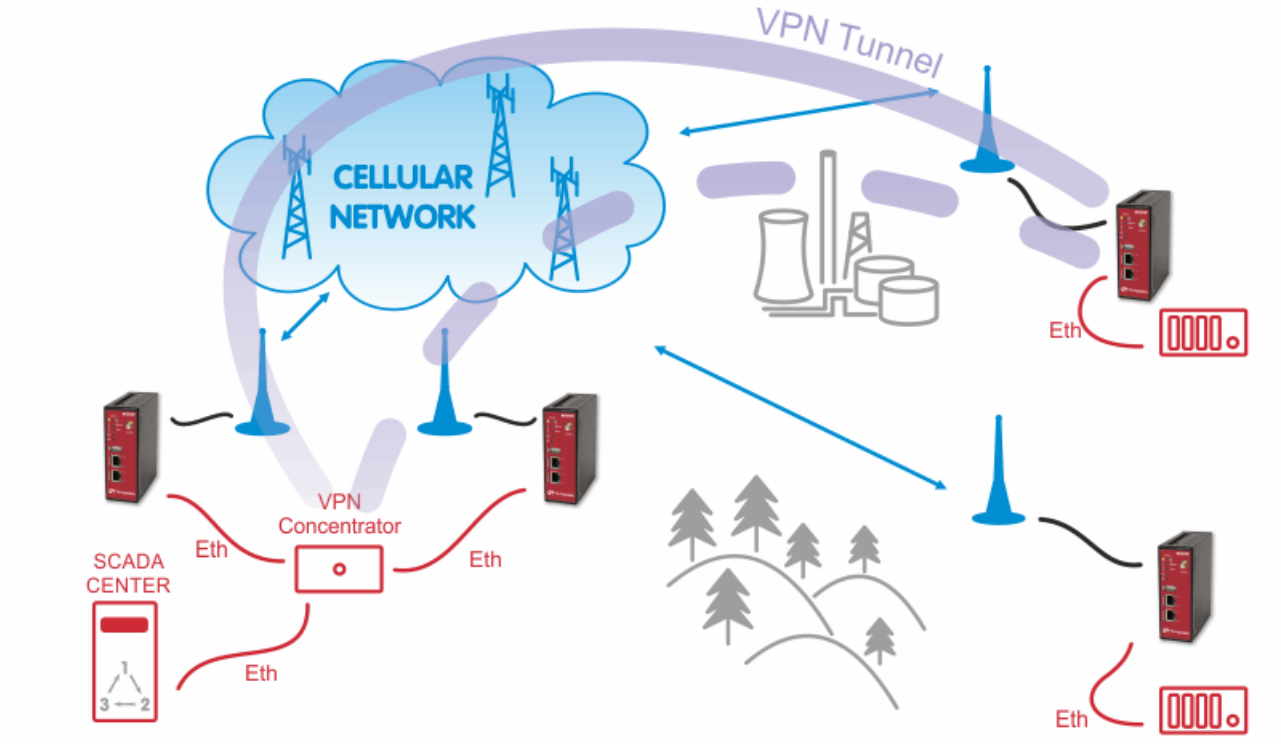
Note

VPN tunnels bring some additional overhead which causes higher data volume. Keep this in mind if paying to the service provider per data volume and not a fixed sum of money.



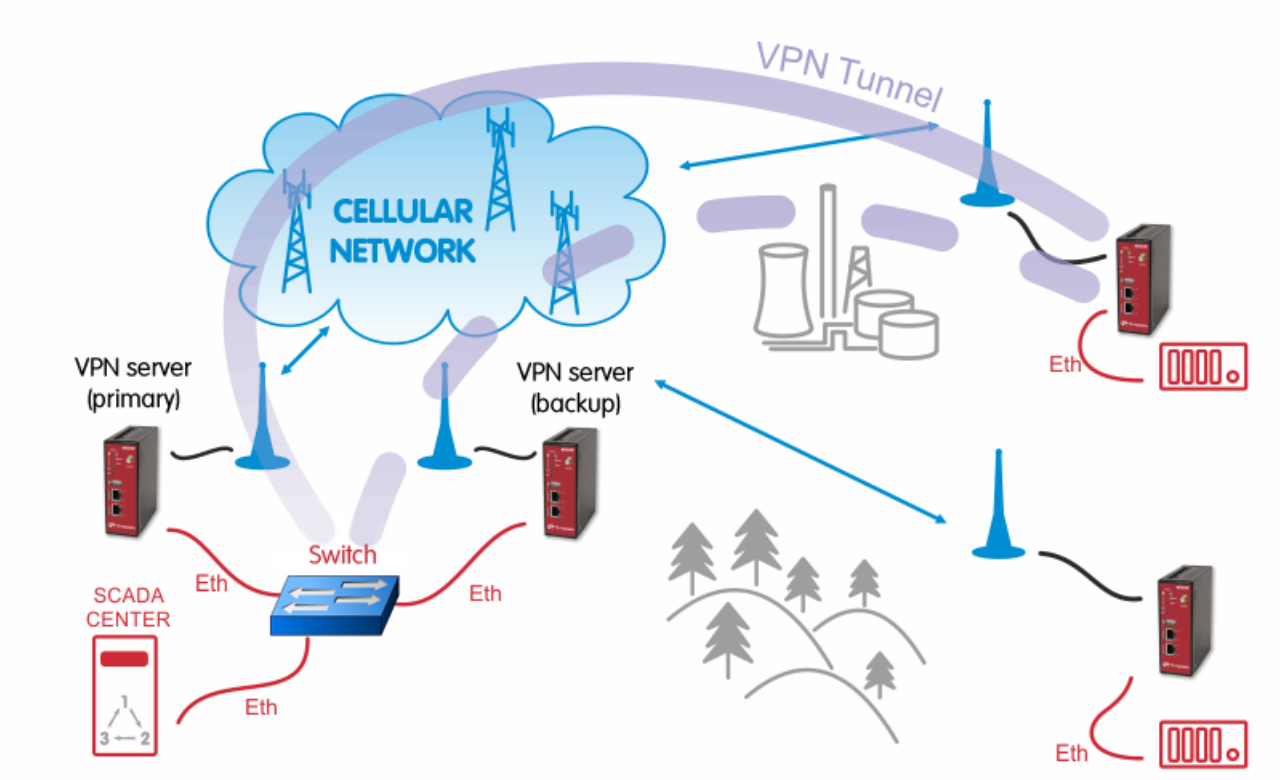
When a higher number of tunnels (i.e. a higher number of remote units) is required, VPN concentrator has to be used – a special router (e.g. CISCO) for IPsec tunnels or an ordinary PC (Linux/Windows) for OpenVPN tunnels.

1.3. Redundant M!DGE/MG102i – VPN tunnels only



Two M!DGE/MG102i units with Virtual Router Redundancy Protocol (VRRP) functionality can be used. The VRRP creates one virtual IP address for both units and this IP address is active for the local LAN. Two independent SIM cards (one in each unit) are used for obtaining public mobile IP addresses. The OpenVPN tunnel is the recommended tunnel type.

In the picture above, there is an additional VPN concentrator as a VPN server. We can also use M!DGE units to be the OpenVPN servers and configure clients to connect to one of them primarily and use the second one as a backup solution.

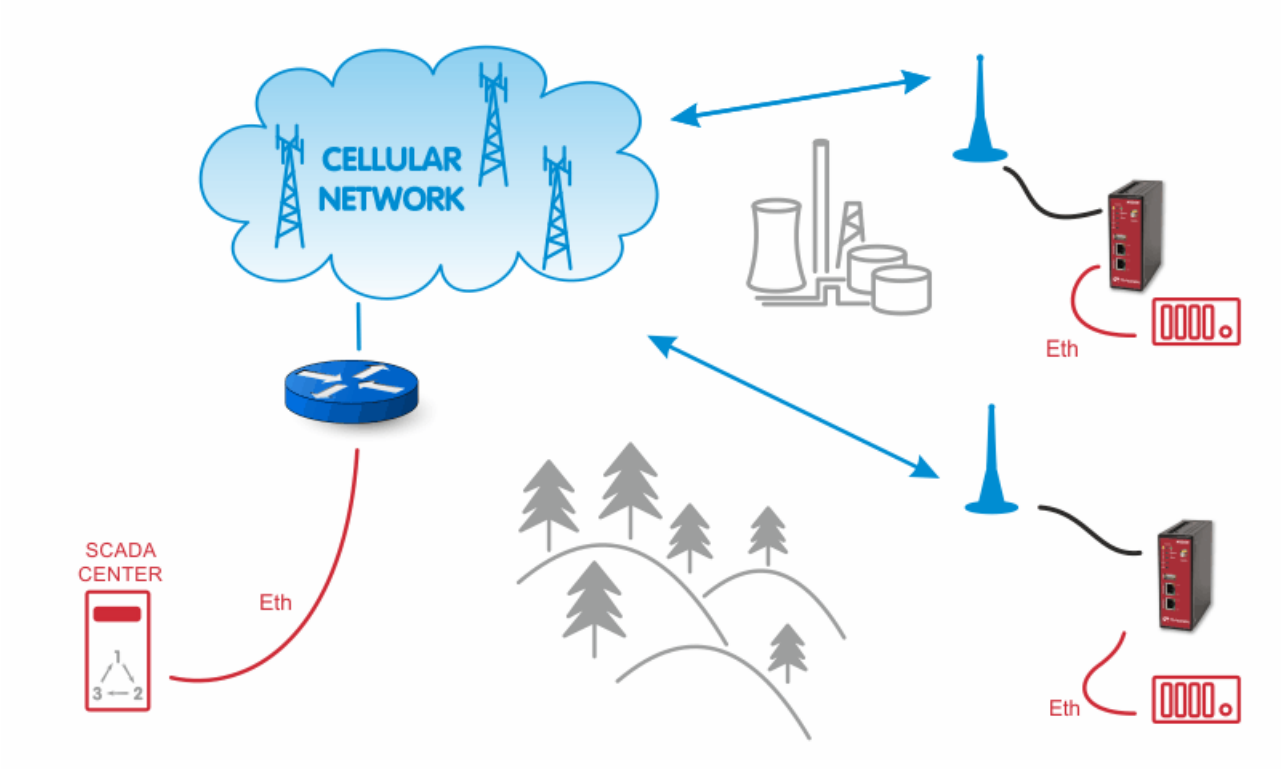


This solution increases the hardware reliability of the center. A redundant VPN concentrator (cluster) solution may be used to further improve the reliability. However a leased line to the Cellular network operator center is more reliable solution and it is recommended whenever the reliability of the network really matters.

2. A leased line to the Cellular Network Center

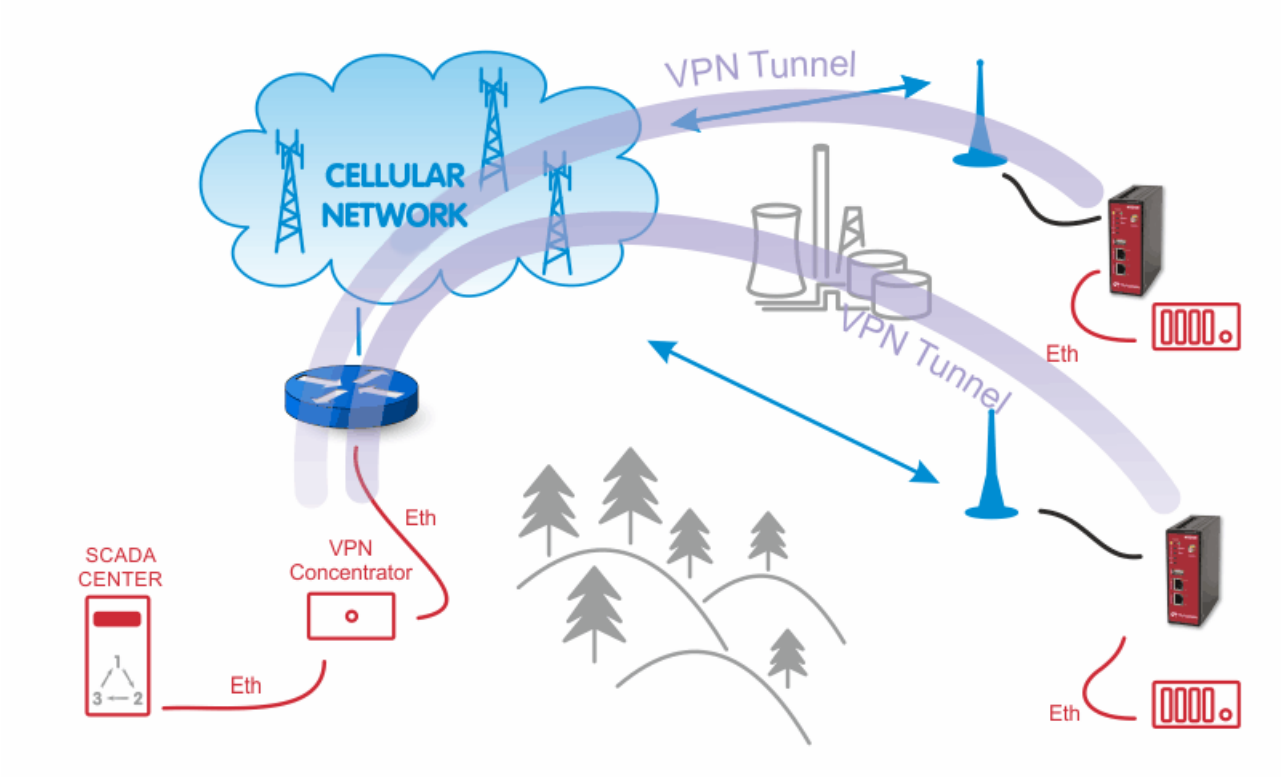
This scenario is feasible for networks with any number of remote sites. A leased line generally provides a better reliability than a wireless cellular connection and its capacity is not limited by the Cellular network technology available at the center location. The leased line connects the SCADA center directly to the operator's CORE WAN. Sometimes it can be substituted by an Internet connection between the SCADA center and the operator's center.

2.1. Leased Line Connection – without VPN tunnels



The solution is the same as in Section 1.1, “Central M!DGE/MG102i – without VPN tunnels”. The only difference is that we do not have M!DGE/MG102i in the center.

2.2. Leased Line Connection – with VPN tunnels

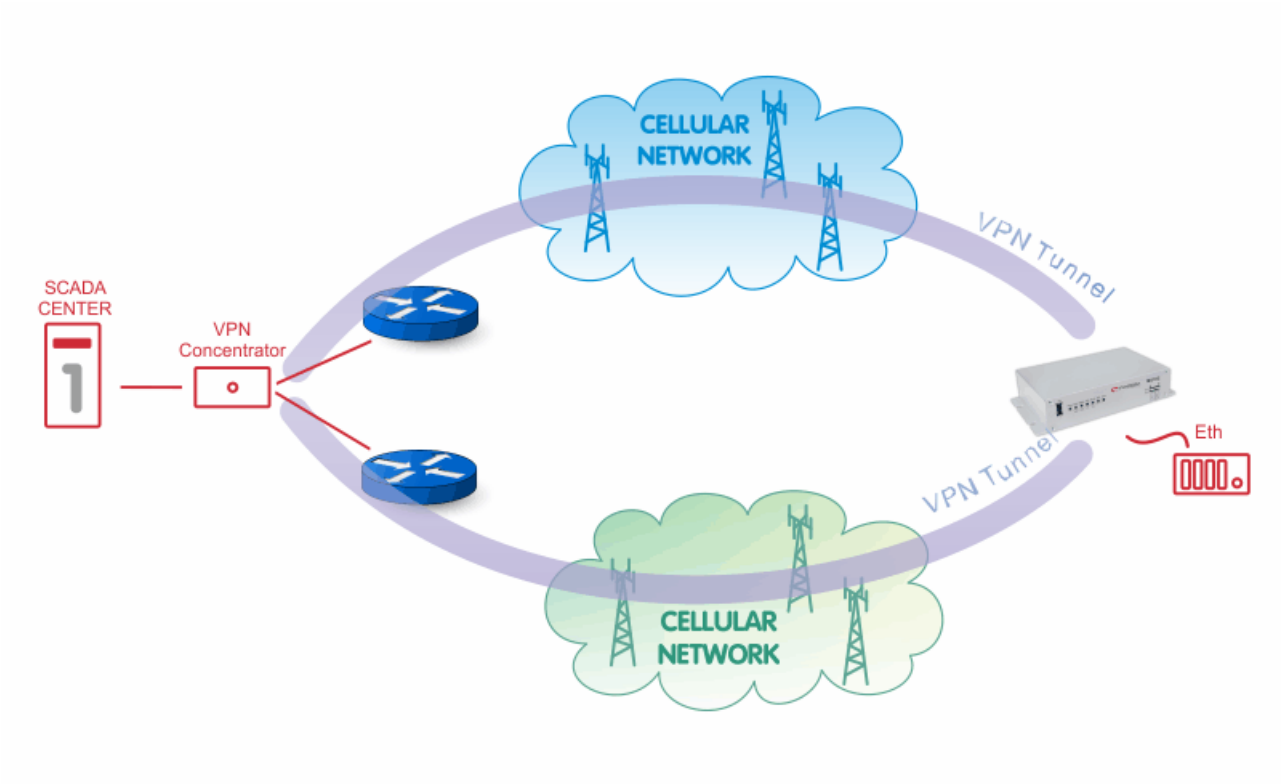


The solution is the same as in Section 1.2, “Central M!DGE/MG102i – with VPN tunnels”. The only difference is that we do not have M!DGE/MG102i in the center, but there is a dedicated VPN concentrator which can handle more than 25 clients simultaneously (e.g. CISCO). The redundant VPN concentrator (cluster) may be used for higher reliability.

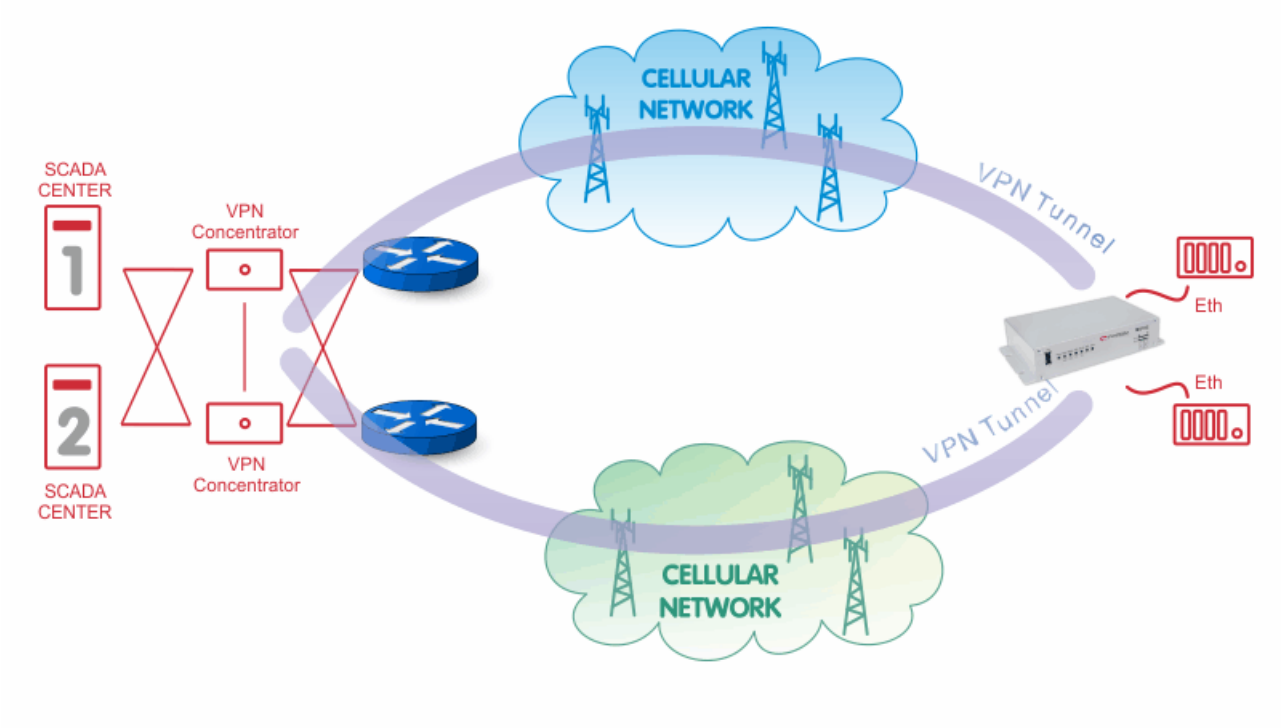
2.3. Redundant Connection of Remote Units using two different Cellular network providers

With a MG102i dual-SIM cellular router, we can use two SIM cards. If the primary provider network fails, the traffic is automatically switched to the second provider.

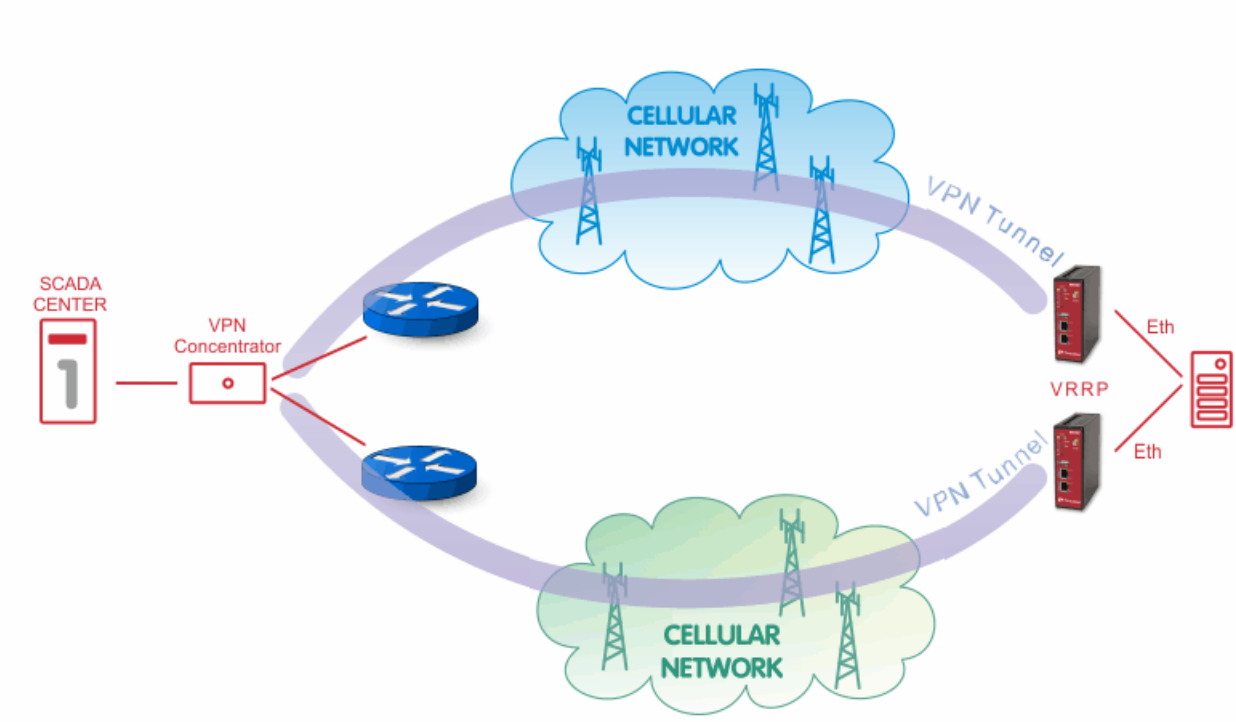
Even with a single provider, two independent Access Point Names (APN) can be used to improve overall reliability.



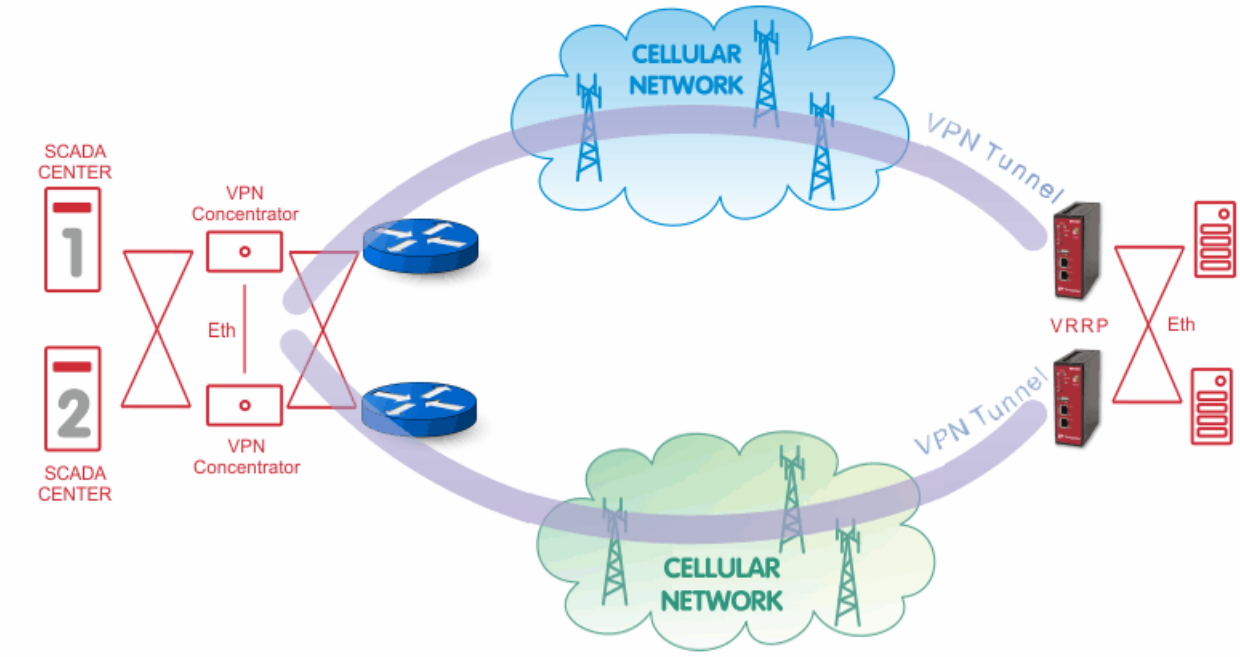
The fully redundant solution of the center is possible as follows:



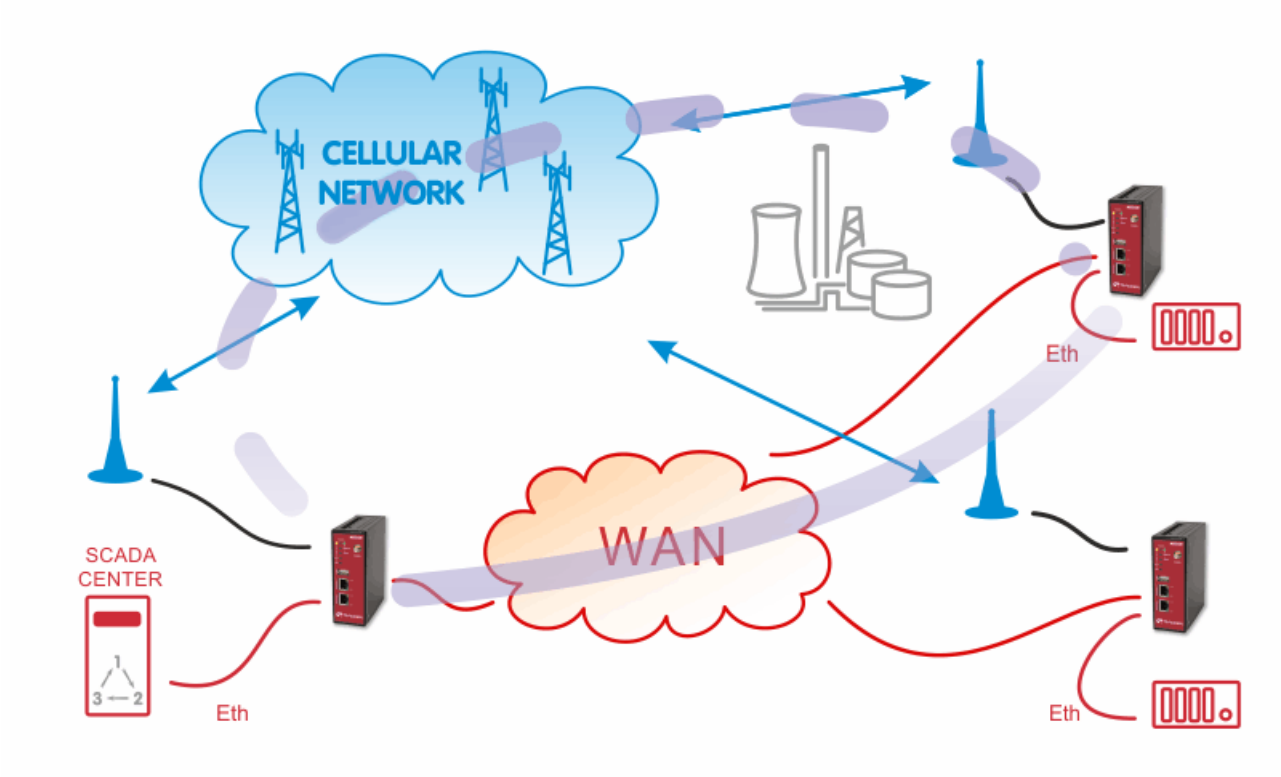
Remote redundancy with two M!DGE/MG102i units with VRRP activated – this solution can handle both the network service failure and the M!DGE/MG102i router (+ antenna installation) HW fault:



A fully redundant solution for both the center and remote locations is certainly possible:



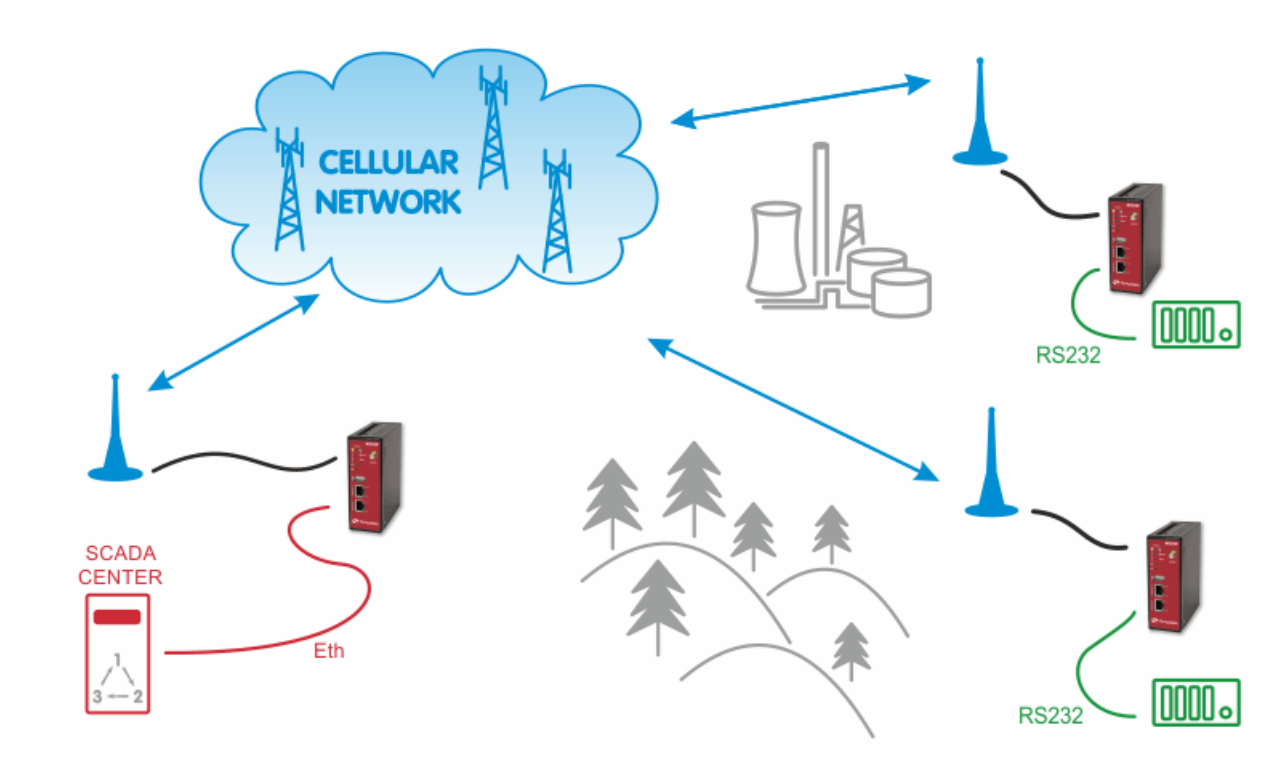
3. Backup of WAN by Cellular Network



Under usual circumstances, VPN tunnels between remote and central M!DGE/MG102i units are established over the WAN network. When the WAN fails, the traffic from/to the respective remote M!DGE/MG102i is automatically redirected to the cellular network.

4. Serial Port SCADA Protocols in Cellular Network

SCADA protocols (IEC101, Modbus, ...) on the serial interface (RS232) use proprietary addressing. Since IP addresses have to be used in the cellular network, a translation between the SCADA addresses and IP addresses is required.



M!DGE/MG102i has several ways how to handle the serial traffic. The preferred one is using the **Protocol Server** functionality. This feature is the same as in RipEX modems and it is a proprietary implementation of SCADA addresses to/from IP addresses translation. Thanks to this feature, point-to-multipoint, multi-master or basic point-to-point SCADA applications are possible to handle within Cellular network without the need of any additional device. Details in *Serial SCADA Protocols* [1] over Cellular Network aplication note.

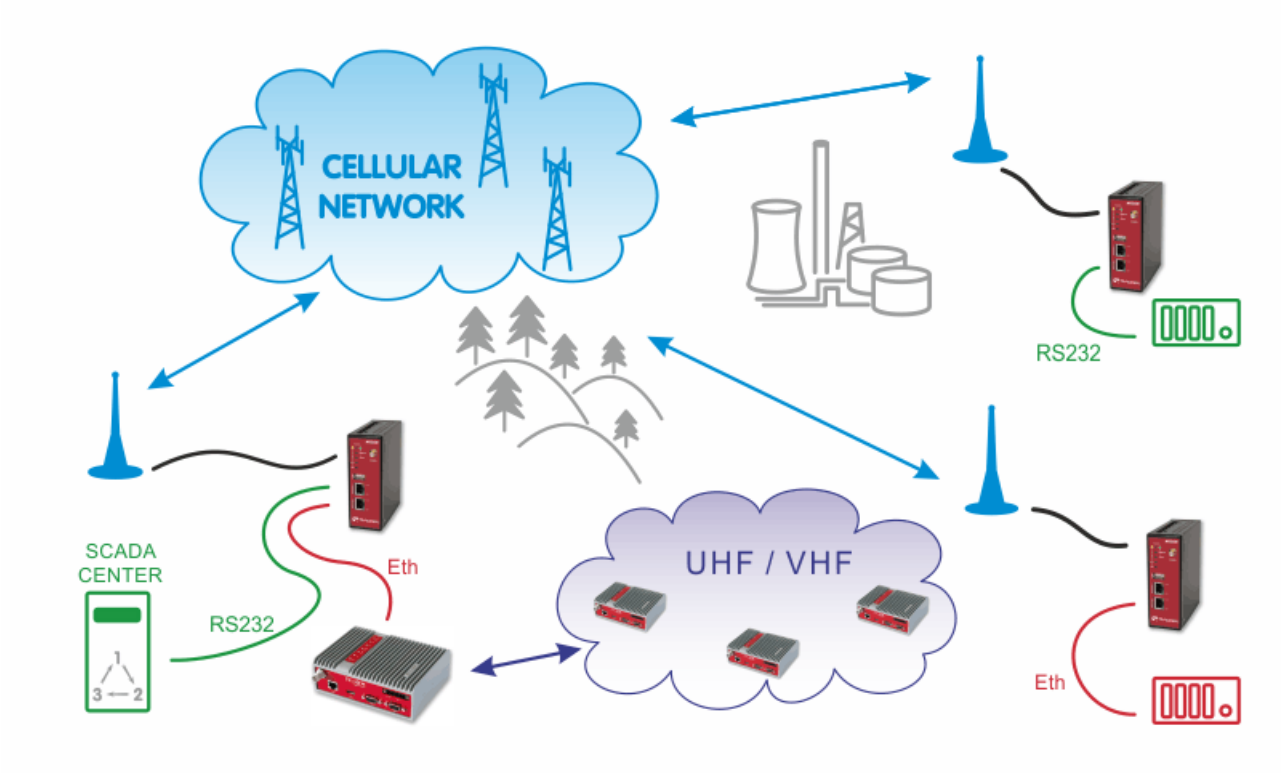
Another possible way is to configure **TCP or UDP server** which does not recognize individual serial protocols, but is capable to handle simple applications. Both implementations can be modified by the end-user to suit individual needs. This can be done via SDK programming which resembles very basic C programming. Using hostnames instead of IP addresses is possible in both options.

Note

The arrangements described in Chapter 1, *A Standalone M!DGE/MG102i in the Center* and Chapter 2, *A leased line to the Cellular Network Center* also apply to the serial SCADA protocols, but the DNS hostnames cannot be used with the Protocol Server feature, only with TCP/UDP Server.

[1] http://www.racom.eu/eng/products/m/midge/app/ser/index.html

5. Cellular Network and UHF/VHF Radio Data Network Combination



The picture above describes an arrangement, where part of the remote sites is connected over a private UHF/VHF radio network (e.g. sites requiring 99.9% availability) and the remaining sites are connected over the cellular public network (e.g. distant, isolated locations where it would be uneconomical to extend the radio coverage to).

Appendix A. Revision History

Revision 1.0 2017-12-06
First issue

Revision 1.1 2018-02-28
Termination of M!DGE UMTS routers manufacturing