



Security of TSAT2100/50 Satellite System

Data security issues when using TSAT 2100/50 as a communication medium can be discussed on two different levels:

1. Risk of intruders connecting to the network and reads the contents of the data or transmitting falsified data.
2. Risk of intruders jamming the link

1. Risk of intruders connecting to the TSAT 2100/50 network

To be able to connect to a TSAT 2100/50 network and read the contents of the communication link, it is necessary to pass several levels of obstacles:

1. The correct satellite position, and the utilised frequencies and polarisation need to be known: This is information that can, depending on security policy of the network operator, be classified as confidential. However, to obtain full control of the flow of information, the satellite operator's information routines must also be assessed.
2. In addition, the Ku-band to baseband signal processing hardware, the modulation method, forward-error-correction scheme, the access methods and internal proprietary data processing schemes and interpretation methods would have to be known and copied. In reality, this means that a TSAT 2100/50 terminal would have to be used.
3. Having acquired the information on satellite frequencies and polarisation, and having access to a TSAT 2100/50 terminal, the terminal still would have to be configured with the correct set of parameters to be able to connect to the network and decode the information contents. Again, this is information that the network operator may choose to define as restricted.
4. On top of this, TSAT 2100/50 comes with a configurable network parameter that is explicitly defined in order to inhibit access from other TSAT terminals not belonging to the network. Every terminal in a network must be configured with a 3-digit carrier identity code, unique for the network, in order to be able to connect to the network. Again, this is information that the network operator naturally would choose to define as confidential.



It should also be noted that, as far as falsifying data is concerned, TSAT 2100/50 security is virtually total, as there is no way of intercepting data from a terminal, reading it, and replacing it with false data, as would be possible when using terrestrial lines as transmission medium.

The conclusion is that by applying reasonable security measures concerning restricted access to network parameters, access to network data is easily controlled. If security levels beyond what is provided by TSAT 2100/50 as described above is required, application data encryption schemes should be applied.

2. Risk of satellite signal jamming

If the purpose of the intruder is not to acquire or falsify data, but to destroy the information in order to obstruct the operation of the network, the matter is different. In principle, it is enough with the information under par. 1. above in addition to satellite transmission equipment in order to jam the network, if one should wish to do so. To meet this threat, the network operator should take required measures to restrict access to information concerning satellite position, frequencies and polarisation. As an additional measure, a low-cost, automatic dial-up backup facility utilising terrestrial telephone lines can be implemented, in order to remain network operability in case of satellite link breakdown.