# Surveillance distribution networks

## Enhance air defence with a sensor data network and Tactical Data Links (TDLs) capable of fusing and securely sharing data between national centres and across borders

To defend against increasingly sophisticated airborne threats—from drones to hypersonic ballistic missiles—many countries have deployed advanced national sensor networks. These networks gather data from numerous in-country sources to enable its analysis and distribution at high speed. However, existing approaches typically do not allow the managed and secure sharing of selected intelligence with national centres as well as defence partners.

This white paper proposes an approach for a surveillance data network enabling selected information to be exchanged across security domains. Properly implemented, this would provide C2 systems, airports, command posts, TOCs and partners with different responsibilities and even in different countries with a shared early-warning capability and enhanced situational awareness beyond their own surveillance capabilities.

FREQUENTIS

## Opportunities and threats

Events in Ukraine have acted as a wake-up call for NATO and other mutual defence groupings within Europe. Equally, many other countries worldwide require military cooperation in border protection or missions across borders. Facing increased threats, countries are seeking to improve their defence capabilities by enhancing their ability to share surveillance data with allies.

Countries are procuring a variety of defensive missile systems to protect themselves against multiple threats. Synergies achieved by networking the deployed systems across national borders can enable the cross-border exchange of sensor data across security levels via a secured network. By creating interfaces between multiple national sensor networks, countries can magnify the impact of their investment and gain a mutual early-warning capability.

Figure 1 shows a typical scenario: countries B and C are friendly and exchanging sensitive sensor data. Their radar coverage is shown by the grey and blue circles. A potentially hostile drone is approaching from the direction of country A. The drone has been detected by radar 2 in country B, but is not yet visible to radar 3 in country C. In this scenario, country B could send geographically filtered data about this specific section of radar to controllers in country C. So that country C can receive and process the radar data, the sensor data stream would need to be converted, taking into account the heterogenous sensor infrastructure in both countries, varying standards and structures in sensor data, and different ASTERIX versions or proprietary formats. As required, the data could also be sanitised or encrypted.

To create the proposed transnational sensor network outlined in figure 1, the countries must overcome a number of challenges. These include:

- harmonising the interfacing of legacy systems and new technologies
- fusing data from multiple types of sensor
- handling cyber security in a complex sensor data environment
- managing security levels between domains
- ensuring delivery of the relevant information only
- overcoming bandwidth limitations through controlled degradation of service
- handling classified data appropriately
- providing user-specific data services
- offering user control of sensors
- providing central management, monitoring and analysis.

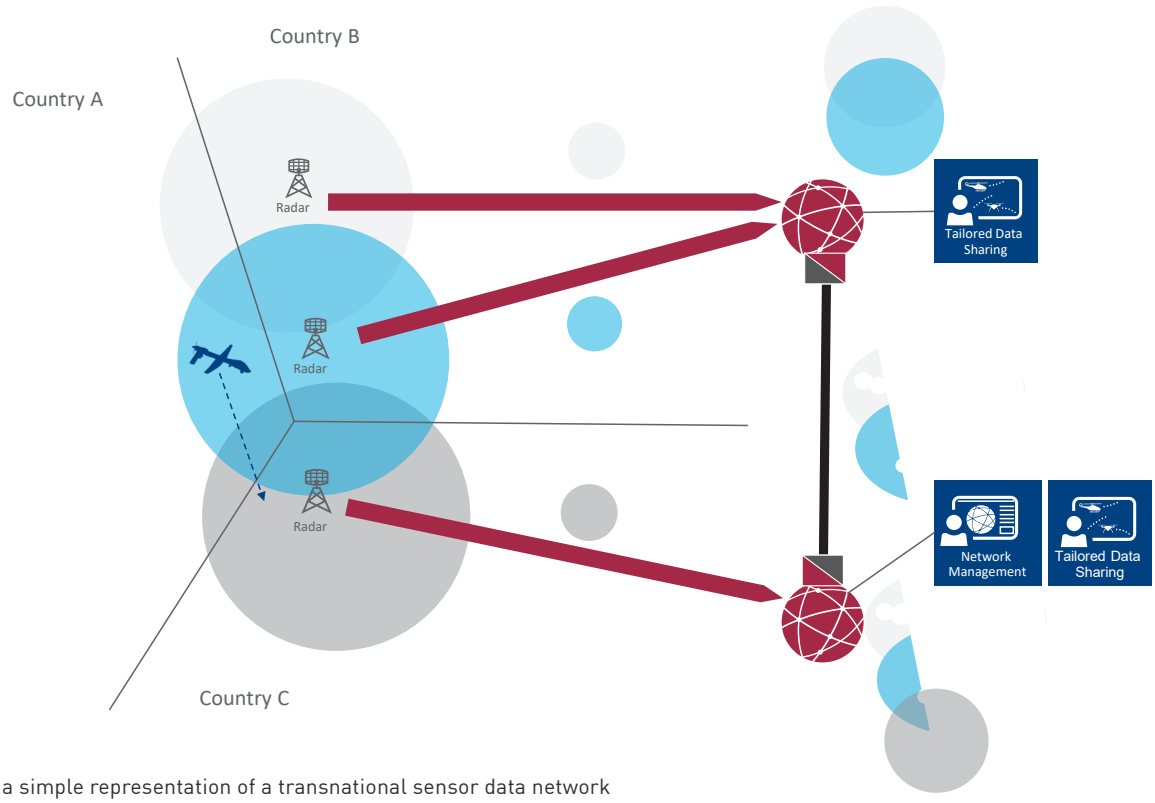


Figure 1: a simple representation of a transnational sensor data network

This paper will now consider each of these challenges in turn, explaining what they imply for countries seeking to create a transnational distribution network.

## Interfacing

Improving Air Defence capability to meet current and future threats by combining information from legacy and new surveillance sensor technologies. The key to achieving flexibility and rapid interoperability in complex network scenarios is decoupling surveillance sensors from proprietary technologies of original manufacturers. Standardised protocols like Asterix, CD-2, TDL as well as proprietary formats are supported.

## Multi-sensor data fusion

The heart of intelligent networks is the fusion of sensor information from various systems and domains. This process involves extracting information from available sources such as:

- Both classic stationary and mobile radar technologies as well as primary, secondary, 3D
- New and future technologies (e.g. passive radars, phased array, missile sensor technology, quantum)
- Air situation calculations
- Tactical Data Links (TDL)

This fusion provides a basis for higher processing levels such as:

- User-specific analysis, classification and fusion
- Intelligent algorithms such as AI-supported analyses and decisions
- Determination for further mission-specific information distribution.

## Security gradient

The exchange of data between network gateways with security gradients must be defined and controlled. Individual users should receive only the information appropriate for them given the group to which they belong.

In addition, communication channels must meet the applicable information security requirements and, where necessary, be supplemented by additional cryptographic components and firewalls.

## Provision of information

Countries will have different sensor landscapes (different manufacturers, types and generations of sensors) and will use a variety of data formats. When it comes to cross-border data exchange, the ability to control changes to the entire infrastructure will therefore be limited. The formats and properties of data entering the network will be subject to constant change; for example, new sensor software releases, sensor updates, additional data sources, or simply different sensor operating states.

In order to be able to process this heterogeneous sensor data consistently in a target system, the information must be reliably made available with as many of the original properties as possible, regardless of any changes in the input formats.

In particular, this means that the format of the data passing into and out of the network must be defined, verified and quality-proofed. This will require content analysis, filtering and conversion, as well as tuning and specific adaptation of the data streams to the requirements of individual users—for example, those with limited network bandwidth.

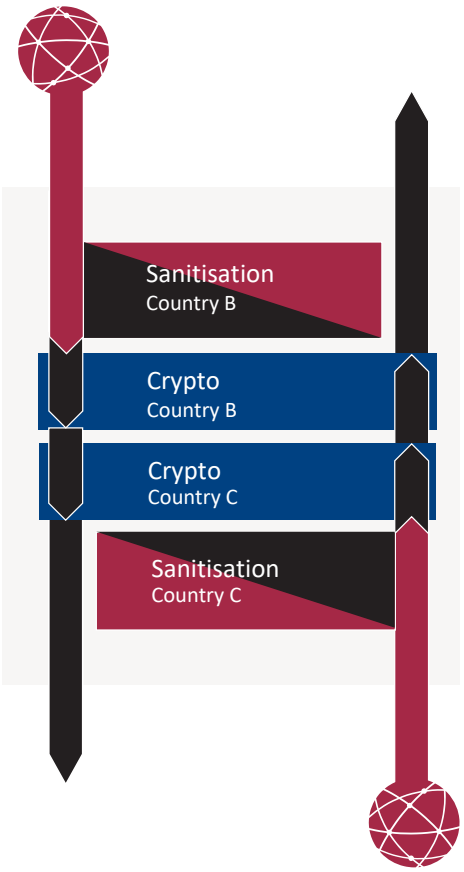


Figure 2: cross-domain security

## Bandwidth limitation and controlled degradation of service

For the users of the respective national target systems within a sensor network, not all data from a specific area will be relevant for daily operations. This opens the opportunity to selectively discard some information in the event of a bandwidth reduction.

A cognitive and information-based network can prioritise the data relevant to the user profile and discard any less relevant data in order to minimise latency and make optimal use of the available bandwidth. This prioritisation can be specific for each user profile, ensuring that all users have access to the most relevant data for their needs.

## Handling of classified information at network interfaces

Incoming and outgoing data should be analysed at network interface points. Information agreed bilaterally or multilaterally between national forces should be exchanged in the required format.

Classified data can be sanitised by geographic filtering, altitude filtering, content filtering, blacklisting and/or whitelisting. Sanitisation should be performed by the network. If additional country-specific (for example, National Security or NATO-certified) sanitisation systems are required, the additional sanitisation will be performed at the exit of the supplying network node.

## User-specific data services

The data made available to users and their target systems might be limited to the relevant use cases, based on the "need to know" principle. In other words, information should not be transferred directly from the sources, but should first be customised and delivered in accordance with the specific requirement profile.

The format of the information (for example, ASTERIX), the protocol (for example, TCP/IP) and the type of information should also be clearly defined.

In the event of data loss on preferred data channels, automated data path switching can automatically provide an alternative sensor dataset in order to transmit the required data stream to the target system without interruption.

## User control of the sensor

Some sensor types allow user control; for example, to control target tracking. To enable this control, the network should enable bi-directional data exchange with minimal latency.

## System-wide management

To ensure the efficient and accurate configuration, monitoring and maintenance of a sensor network, it is vital to provide management for different user groups, profiles and sites/locations. A decoupled solution harmonising the variety of sensor manufacturers and C2 in one management will allow for remote maintenance and the configuration of any number of distributed network node locations, thereby enabling the concentration of users with the highest skill profiles at the main centre locations.

Recording systems with radar analysis capabilities can complement centralised management, for example by detecting errors in incoming data or delays in the network, and automatically generate reports on network quality.

# Taking the next steps

By choosing an approach to heterogeneous and changing sensor networks that embodies the best practices described in this white paper, defence organisations can maximise the value of their air defence systems by creating a mutual early-warning capability. This can also increase situational awareness and combine the surveillance capabilities into a more accurate and comprehensive air situation picture.

# Frequentis capabilities

Frequentis is a global leader in communication and surveillance solutions for military ATC. Our deployments include MilRADNET, a nationwide sensor network for the Bundeswehr (German Armed Forces). MilRADNET supports the exchange and distribution of military flight surveillance and flight-plan data, making a significant contribution of the safety of German and pan-European airspace.

FREQUENTIS

FREQUENTIS AG
Innovationsstraße 1
1100 Vienna, Austria
www.frequentis.com