# SESSION BORDER CONTROLLERS (SBC)

## Shall ANSP SBCs be ED137-specific?


### Abstract

Security is the main concern tackled by organisations when they have to connect to networks they do not have direct control on and have therefore considered as untrusted zones compared to the internal network. The SBC function is important to ANSPs to separate internal and external communications in order to prevent attacks to their internal network devices. SBCs can be standard devices, not specifically designed for ED137 purposes, protecting the general ANSP LAN rather than a VCS.

The MULTIFONO® M800IP® solution from SITTI includes radio and telephone gateways, allowing a better management of the voice and data streams with physical independence between external and internal LANs. This feature can be provided by dedicated blades acting as gateways as independent parts of the VCS, which represent a better solution as compared to a server-based architecture.



Roberto Weger

roberto.weger@sitti.it


15 May 2020


**SITTI S.p.A.**

Via Cadorna 73 - 20055 Vimodrone (MI) - Italy

www.sitti.it - sales@sitti.it - +39 02 2507121

# 1. SECURITY IN IP NETWORKS

As a matter of fact, the IP technology is increasingly influencing our life in daily activities, thanks to the capability of conveying many different types of information streams on a common infrastructure. The convergence of voice and data onto one multimedia network pushed ANSPs to consider the adoption of new technological solutions to gradually move away from old-fashioned analogue links and circuits towards a common, widespread, cheaper approach to communications, in order to better cope with their tasks.

Numerous converging aspects concurred in paving the way to the transition to IP, among which more powerful processing machines, faster networks, decrease of IP elements maintenance costs, development of new standards and protocols, easy products availability on the market, obsolescence of legacy connections, etc.

As a consequence of the convergence of multimedia (data, voice, video streams) onto one single common infrastructure, there's virtually no distinction in the type of messages flowing through a node in the network. The same routers in the network may in fact at the same time be dispatching data for flight planning, voice from a controller and a video stream from a virtual tower, all encoded as IP messages.

The advantage of such an approach is clear: reduced costs, easy maintenance, fast fault repair, automatic rerouting in case of unavailability, unprecedented configuration features, rapidity in the deployment, lower staff training needs, etc. All this can be summed up into one word that is the leading driver for most decisions: cost effectiveness.

On the other side, the drawback of this approach is the potential of reduced security. Standard communication protocols and a common network infrastructure help implementing the new technology, but open up the possibility of misuse of the technology itself.

When using legacy connections (especially in one-to-one links), the interception of a communication mostly required to be physically connected on the line along its path and was generally limited to one single connection at a time. This is no longer the case with IP, because if an ill-intentioned hacker gets full access to a network router, even from a distance, he can potentially intercept, disrupt, manipulate many different connections at the same time.

Security is therefore paid a constantly increasing attention by ANSPs who want to preserve the content of their messages from any possible attack, eavesdropping, listening, modification, cancellation, not forgetting other specific IP attacks such as denial of service.

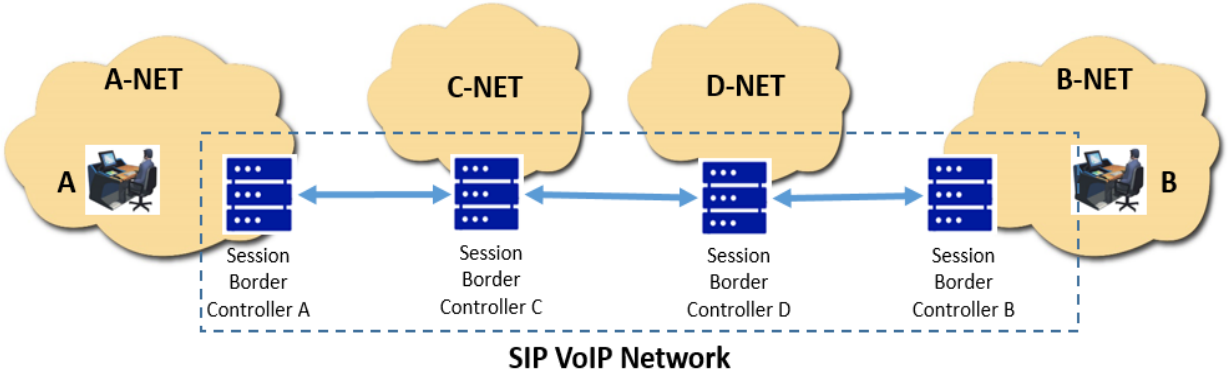
## 2. SESSION BORDER CONTROLLERS

Security is of fundamental importance in all data exchanges, but particularly in the field of Air Traffic Control and Management (ATC/ATM), because the consequences of attacks could be here devastating.

A plurality of means can be adopted to secure that the messages flowing to and from the network are well-formed, come from a trusted sender, are directed to a valid addressee, contain valid information, are authorized, and so on. Network firewalls can provide some sort of protection, but they do not go down deep enough into the technology to provide full protection.

Session Border Controllers (SBCs) are vice versa specifically designed to secure end systems when using SIP-based VOIP technology. This is the case of voice communications in the ATC field, based on the EUROCAE ED 137 world standard.

Generally speaking, Session Border Controllers (SBC) are network elements aimed at controlling, managing and protecting SIP based VOIP communications at the borders between two parties, or as a gateway point for the connection to a wider network. For many reasons they can be seen as a sort of sophisticated combination of firewall + gateway + proxy.



Session Border Controllers have the task of verifying that inbound and outbound messages are not malicious and carry consistent information. SBCs may also provide address translation features that transparently map an address onto another. Among many others, the main features provided by SBCs are

- **Security**
  Control over Denial Of Service (DoS) attacks of various kinds
  Check of malformed packets (protocol packet inspection)
  Data encryption
  SIP header analysis
  White- and blacklisting
  Registar service with authentication

- **Connectivity**
  Address adaptation
  Proxying
  IP protocol dual stack and conversion (IPv4 – IPv6)
  NAT traversal
  VPN termination

- **Quality of service**
  Rate adaptation and limiting
  Call admission control (e.g. maximum number of simultaneous calls)
  Traffic prioritization

It is not required that all these functions are active on a given SBC, but these are the main application areas, where the use of a Session Border Controller can be beneficial.

## 3. RECOMMENDATIONS ON SBCS

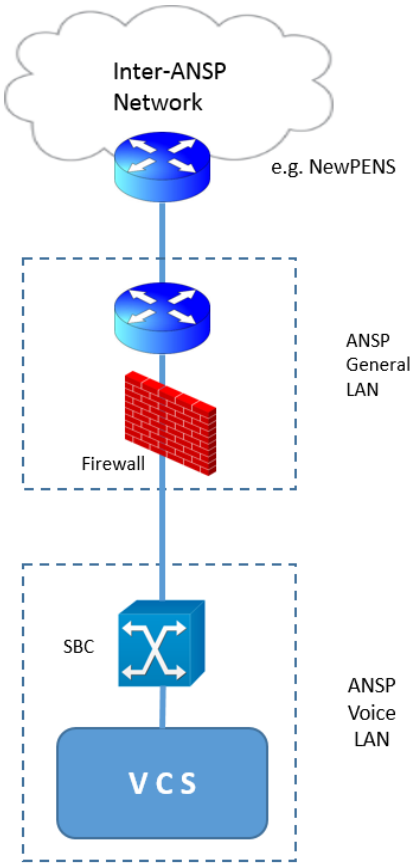
At the time the present white paper is written, EUROCONTROL (the pan-European, civil-military organisation dedicated to supporting European aviation) is finalizing specific documents aimed at the identification of requirements that apply to SBCs. Among them, three are noteworthy:

- ✓ [1] – Voice over IP security baseline, edition 1.0, April 2020
- ✓ [2] – SIP Addressing in ATM VOIP, edition 1.0, November 2019
- ✓ [3] – SBC Implementation Guidance, draft 0.4, March 2020

## 4. WHERE DOES SBC FIT INTO MY NETWORK?

Security is a constant concern for all ANSPs. Session Border Controllers are meant to be installed and configured at the “border” of their networks or subnetworks or pieces of networks in order to guarantee that inbound/outbound traffic is secure in terms of connection and content.

SBCs are physical or logical devices that are designed to handle the combination of private and public domains, allowing to effectively protecting and de-coupling the two sections of the network they are intended to connect. They may typically implement the so-called Back-to-Back User Agent functions that split SIP transactions in two pieces, on one side facing the ANSP internal VOIP network and on the other side managing the traffic from the outer world.



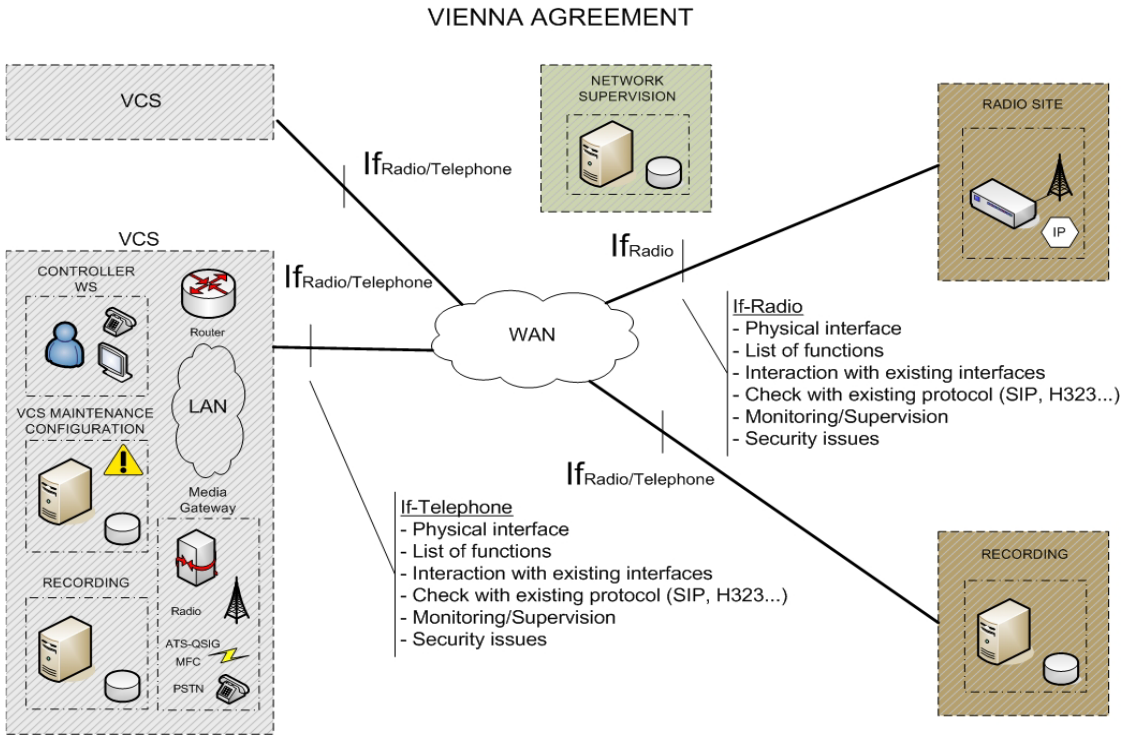

Europe is going to implement a common network infrastructure (called NewPENS) connecting all ANSPs to provide a common and controlled platform for data and voice exchange. Similar solutions are of interest in other Continents as well. The introduction of SBCs in such interconnecting networks allows hiding the internal network topology and addressing scheme, thus permitting more advanced security and processing.

When SBCs are configured (possibly in multi-redundant mode) at all edges of the ANSP network, the internal network is sheltered from malicious attacks and can be treated as a “Trusted Zone”.

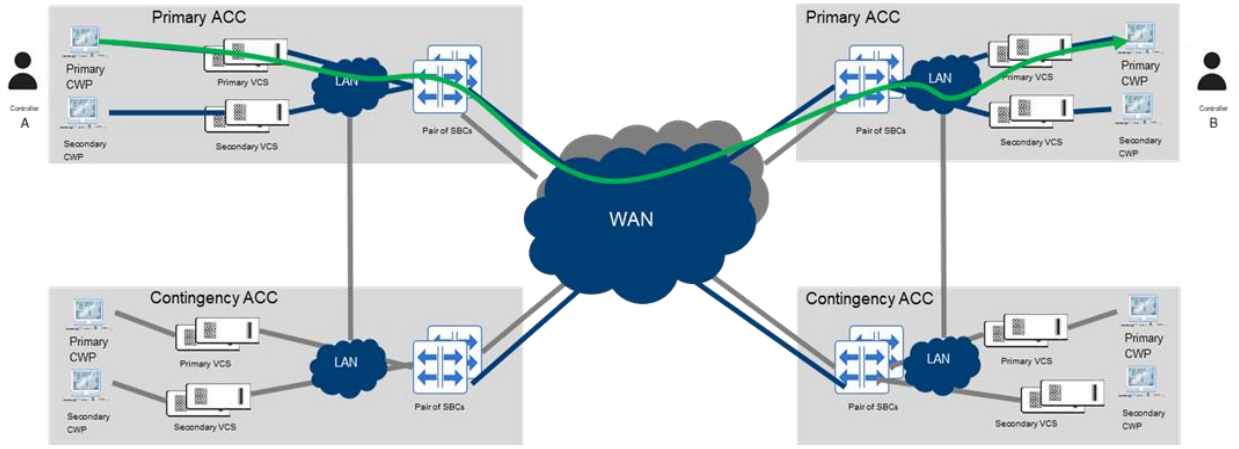
As shown in this picture (taken from document [3]), Session Border Controller features are required between the VCS and the ANSP General LAN that in turn provides access to a general WAN for IP communication to remote users. SBCs are used as the front end to the VCS in order to protect it from external intrusion and attacks, because in its absence the internal LAN of the VCS would be exposed and ED137 communications could reach the CWPs.

## 5. RELATIONSHIP WITH ED137

According to the so-called *Vienna Agreement* (explicitly referenced to by ED137), the voice management protocol defined by this standard is mandatory outside the VCS for all radio, telephone and recorder communications, which shall comply with ED137. Vice versa, inside the VCS (i.e. on its internal LAN) it is up to the manufacturer to implement the best solution to provide the final user with the required functionalities.




SBCs are therefore auxiliary devices that introduce a logical separation between the outer world and the ANSP LAN, as shown in the following picture depicting the route of a normal voice call between controllers A and B.



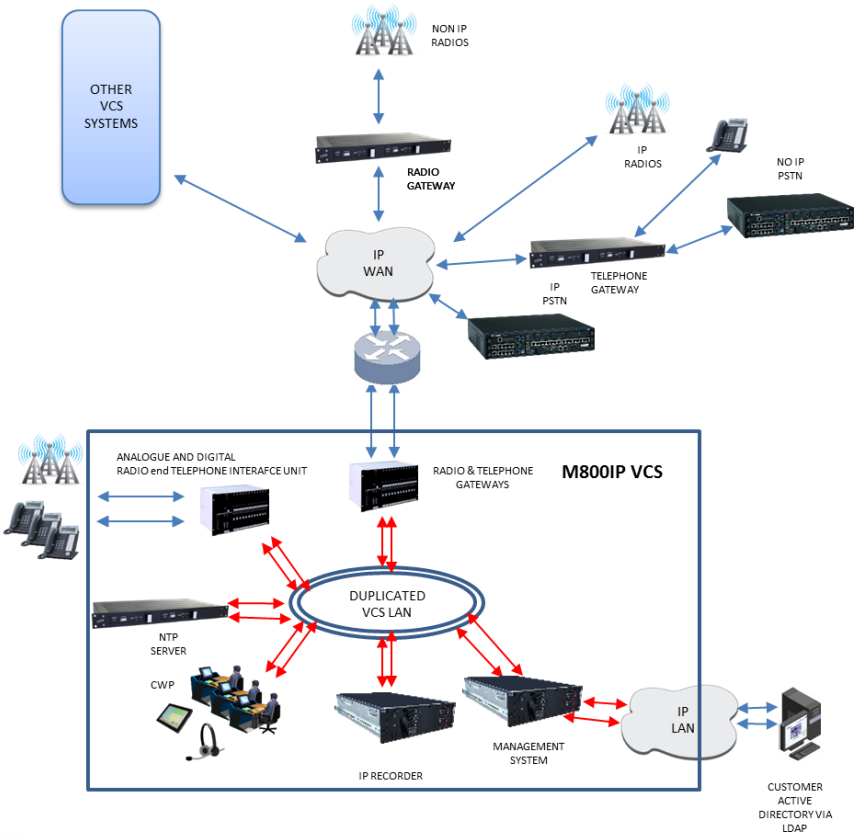
## 6. SITTI SOLUTION

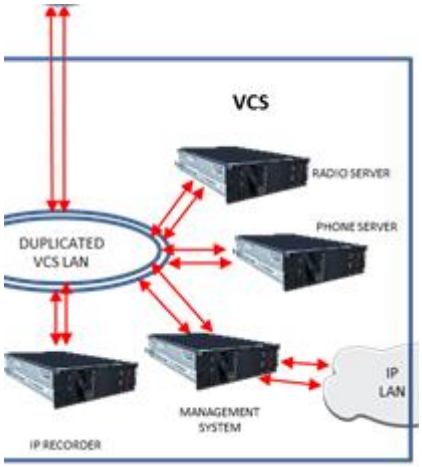
The architectural solution proposed by SITTI for its VCS systems envisages true gateways that are aimed at managing and segregating the interface between external (WAN or ACC general LAN) and internal VCS LAN communications.

Such gateways are hosted on one or more independent blades as part the standard VCS solution. Each radio gateway blade allows up to 16 radio connections, while telephone gateways provide up to 30 telephone connections. For redundancy reasons, gateways are normally duplicated to provide very fast recovery time.

Moreover, SITTI M800IP® allows the implementation of the M+N redundancy method (*M=number of gateways permanently required for the service; N=number of gateways available to replace any of the M, automatically*).

This application permits the system to overcome N failures without disrupting the service, which is much more performing and cost effective than simple duplication.




Sometimes, a different VCS architecture is looked for on the market, instead of blade gateways: the use of dedicated servers that are directly connected to the internal VCS LAN. Based on the large experience accumulated by SITTI, this solution is strongly discouraged, because it is exposing the internal LAN to the WAN. Furthermore, configuration of the server-based SBCs can be cumbersome.

## 7. BENEFITS TO THE CUSTOMER

The main features of SITTI's gateways are summarized as follows:

a) Radio Gateway:
- Dedicated CPU with real time, secure OS.
- Two Ethernet physical ports on the WAN side, physically separated from other two Ethernet physical ports on the internal LAN side.
- Management of radios with ED 137 unicast communication.
- Extension of the external radio ED 137 unicast communication to a separate multicast internal communication stream with negligible delay for both data and RTP.
- Connection to remote radios only for configured ones.
- Radio domain WAN addressing separate from internal LAN domain addressing.

b) Telephone Gateway
- Dedicated CPU with real time, secure OS.
- Two Ethernet physical ports on the WAN side, physically separated from other two Ethernet physical ports on the internal LAN side.
- Management of local Proxy and SIP communications.
- External telephone communication separate from internal communication with negligible delay for both data and RTP.
- Connection to external telephones only for configured users and limited number of calls.

## 8. CONCLUSION

The SBC function is important to ANSPs to separate internal and external communications in order to proactively prevent intentional and unintentional attacks like denial of service, unauthorized calls and malformed packets. SBCs can be standard devices, not specifically designed for ED137 purposes, protecting the general ANSP LAN rather than a VCS.

The MULTIFONO® M800IP® solution from SITTI includes radio and telephone gateways, allowing a better management of the voice and data streams with physical independence between external and internal LANs. This feature can be provided by dedicated blades acting as gateways as independent parts of the VCS, which represent a better solution as compared to a server-based architecture.

SITTI S.p.A.
Via Cadorna 73 – 20090 Vimodrone (MI) – Italy
www.sitti.it – commerciale@sitti.it - +39 02 2507121