



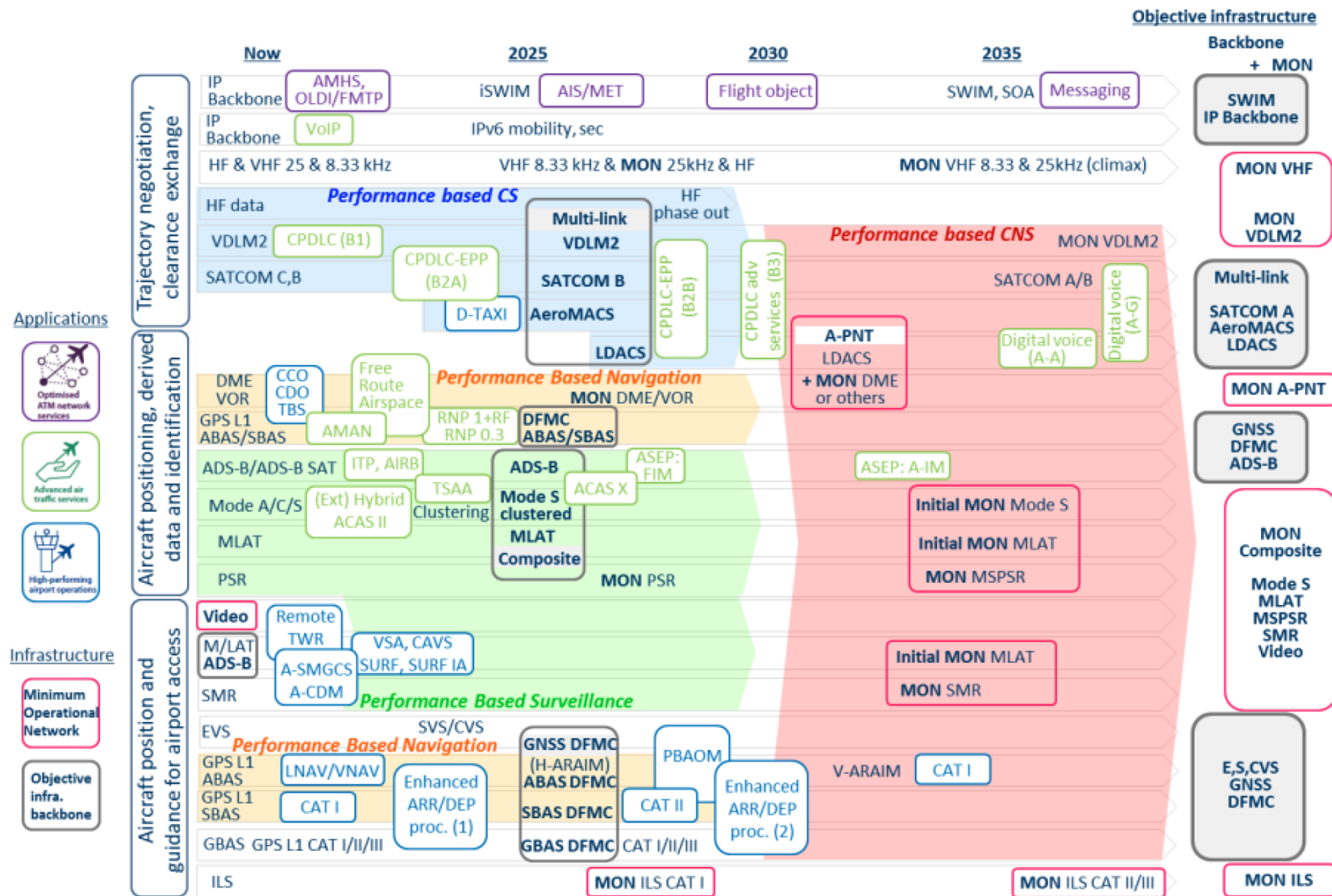
# STATE OF PLAY OF CNS SECURITY

27 MARCH 2019

EXTRACT FOR PUBLICATION

HELIOS  
an  egis company

# THE ROAD AHEAD FOR CNS SHOWS LEGACY AND FUTURE SOLUTIONS





# SUMMARY OF KEY CNS SOLUTIONS

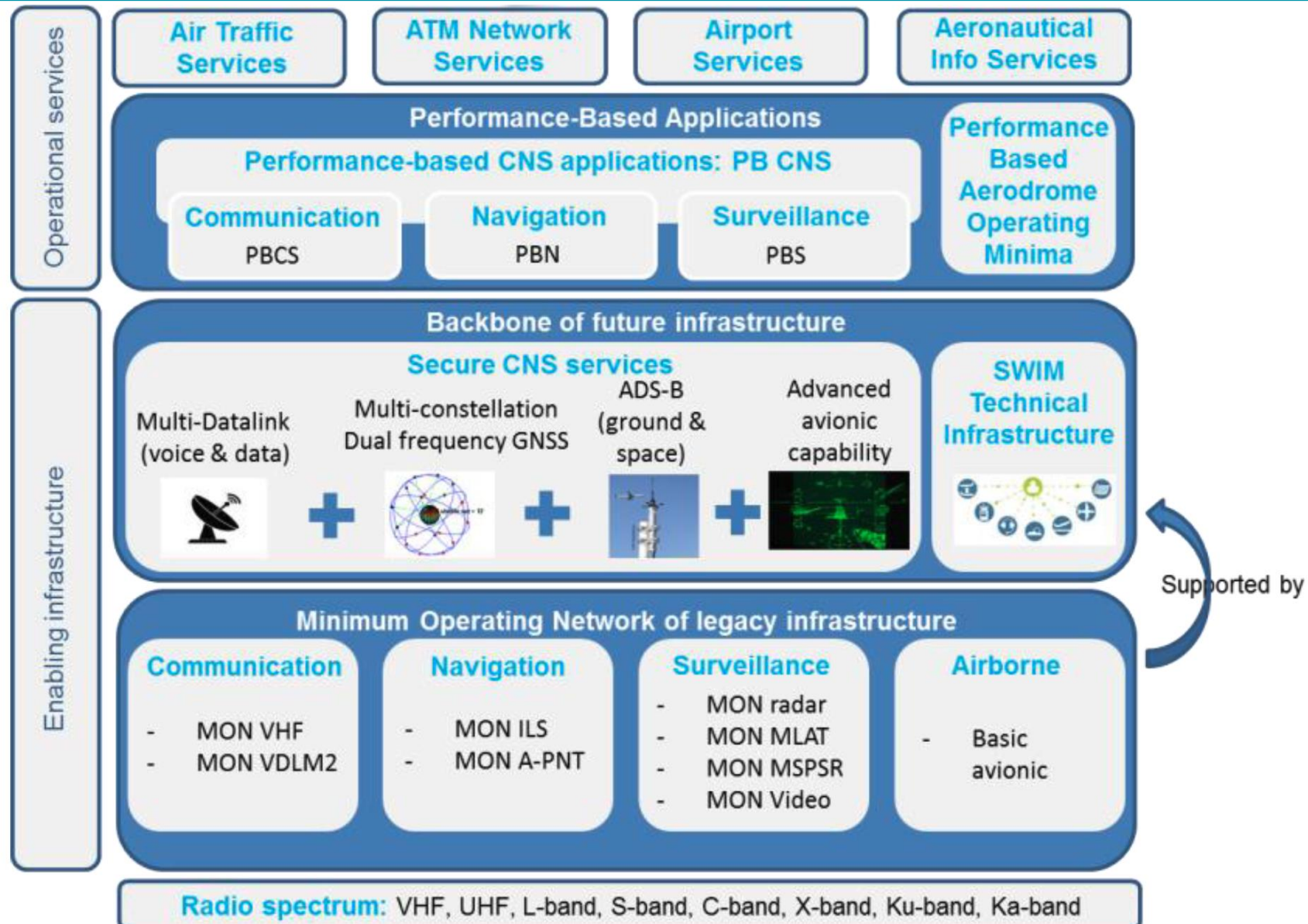
	VDLM2/ CPDLC	PENS/ NewPENS	NDB, DME, VOR	ADS-B	ASTERIX	SWIM Yellow	SWIM Blue
<b>Threats</b>	Denial of Service, Spoofing	Sophisticated attackers, Endpoint compromise	Sophisticated attackers, Spoofing	Privacy, Denial of Service, Spoofing	Denial of Service, Spoofing, MITM Attacks	The Internet, IT solution complacency	Spoofing, MITM Attacks

Diverse sets of weaknesses, similar sets of threats, wide range of mitigations with some common themes

Summary messages:

1. Historic ATM trust model undermines today's security
2. Many security risks well mitigated by operational procedures, but beware of social engineering attacks
3. Huge reliance on GNSS, but DFMC from mid-2020s should help
4. General concentration into fewer CNS assets puts 'more eggs in fewer baskets'
5. 'New' solutions should be securable, especially if suppliers respond to security requirements

# SESAR CNS ARCHITECTURE RETAINS LEGACY AS MIN OPERATING NETWORK



# FINAL THOUGHTS ON RESEARCH

1. Very long lead times for CNS solutions are the root problem
2. Civil aviation not trying to defend against MIL electronic warfare capabilities
3. No published systematic review of security of CNS solutions
4. Need to ramp-up efforts for security in CNS standardisation activities
5. Insufficient fundamental research being done on system-of-systems aspects

**How do we urgently address critical vulnerabilities in a concerted way?**