

IFATSEA Cyber-SMC Technical Supervision Concept overview for the ATSEP Working Positions

SESAR, & the ATSEP Working Position

(An operational approach)

ENGAGE Workshop
SJU, 27 March 2018



Presented by:

Theodore Kiritsis
Vice President
IFATSEA

Related to A39-WP/370 presented in ICAO Assembly 2016



Figure 10: ATSEP SMC. Picture courtesy of Entry Point North.



CONOPS dissemination



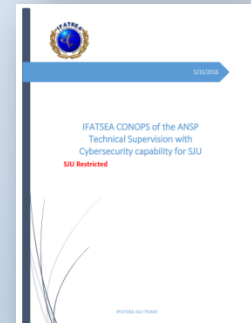
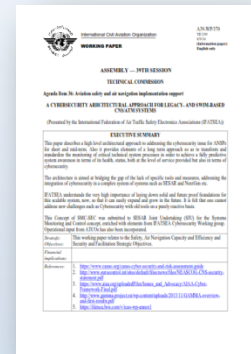
IFATSEA* has presented the Cyber-SMC Technical Supervision Concept to the ICAO Assembly 2016 as an IP under the title:

Agenda Item 36: Aviation safety and air navigation implementation support with the title
“A CYBERSECURITY ARCHITECTURAL APPROACH FOR LEGACY- AND SWIM-BASED CNS/ATM SYSTEMS”, (A39-WP/370)

A CONOPS description was also submitted to SJU and to ICAO Cybersecurity working group chair

The concept was also presented to:

- ENISA together with input for the ENISA study on **Smart airports**.
- ICB as an input for the ICB Cybersecurity paper
- EASA in 2018 in view of the Related regulatory work
- EGHD in 2018 as an integral part for the ATSEP WP
- Activities in ICAO Training(NGAP) and also in AMC for ATSEP Training in EU 2017/373



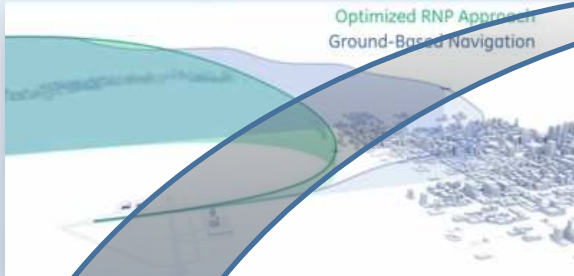
*INTERNATIONAL FEDERATION OF AIR TRAFFIC SAFETY ELECTRONIC ASSOCIATIONS

MOVING TO THE NEW ERA - NEW TECHNOLOGIES /CONCEPTS



PBN (RNP) - ADS-B – DATA COMS
4D Trajectory

SATELITE COMS/NAV/SUR



**New Business
models**

**CYBERSECURITY Threats
over SWIM**



FDP (flight object) - remote FDP- SoA

REMOTE TOWERS

Virtual Centers & ADSPs



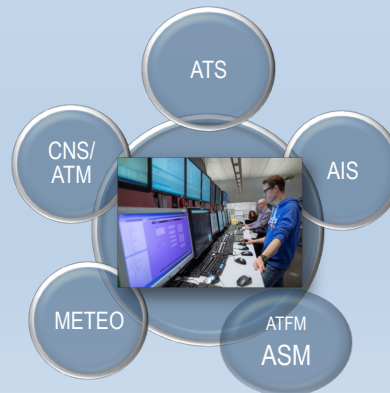
SWIM

Definition of ATSEP

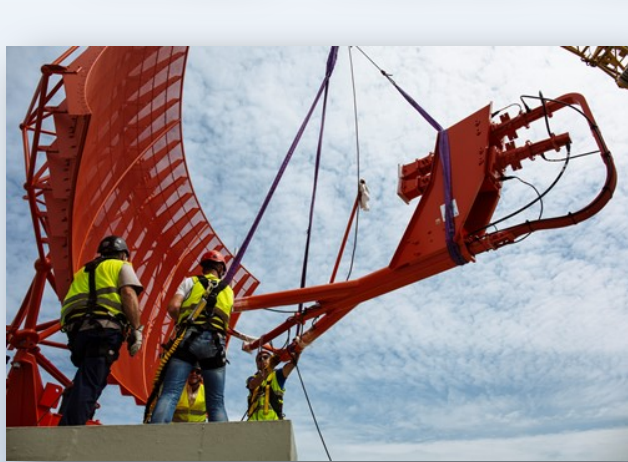
‘Air traffic safety electronics personnel (ATSEP)’ means any authorised personnel who are competent to operate, maintain, release from, and return into operations equipment of the **functional system** ;

‘Functional system’ means a combination of procedures, human resources and equipment, including hardware and software, organised to perform a function within the context of ATM/ANS and other ATM network functions;

AAS *“The proposed target architecture and associated evolution of service provision will generate changes in the work, skills, and therefore training, of the staff and in particular ATCOs and ATSEPs”*



ATSEP TASKS-Please note the different working environments



Functional systems & elements to be monitored and controlled by ATSEP personnel

ATM systems/functions

CNS installations

AIS Systems/functions

SoA — non Geographically co-located

Cyber sec alerts for ANS-SWIM



**One screen per system
No holistic picture**

**(cannot be used for
distributed systems over
SWIM)**



Possible ATM/ANS and other network functions and related systems:

They all need to be monitored and controlled !

Air Traffic Services (ATS):

- Air Traffic Control (ATC) Area Control Service, Approach Control Service, Aerodrome Control Service
- Flight Information Service (FIC)
- Aerodrome Flight Information Service (AFIS)
- En-route Flight Information Service (En-route FIS) Advisory Service

Communication, navigation or surveillance services (CNS)

Communications (C)

- Aeronautical Mobile Service (air-ground communication)
- Aeronautical **Fixed Service** (ground-ground communications)
- Aeronautical Mobile Satellite Service (AMSS)

Navigation (N)

- Provision of NDB , VOR/DME, ILS signal in space. Provision of MLS signal in space.
- Provision of GNSS signal in space

Surveillance (S)

- Primary Surveillance (PS)
- Secondary Surveillance (SS)
- Automatic Dependent Surveillance (ADS/B)

Aeronautical Information Services (AIS)

- Provision of the whole AIS service

Meteorological Services (MET)

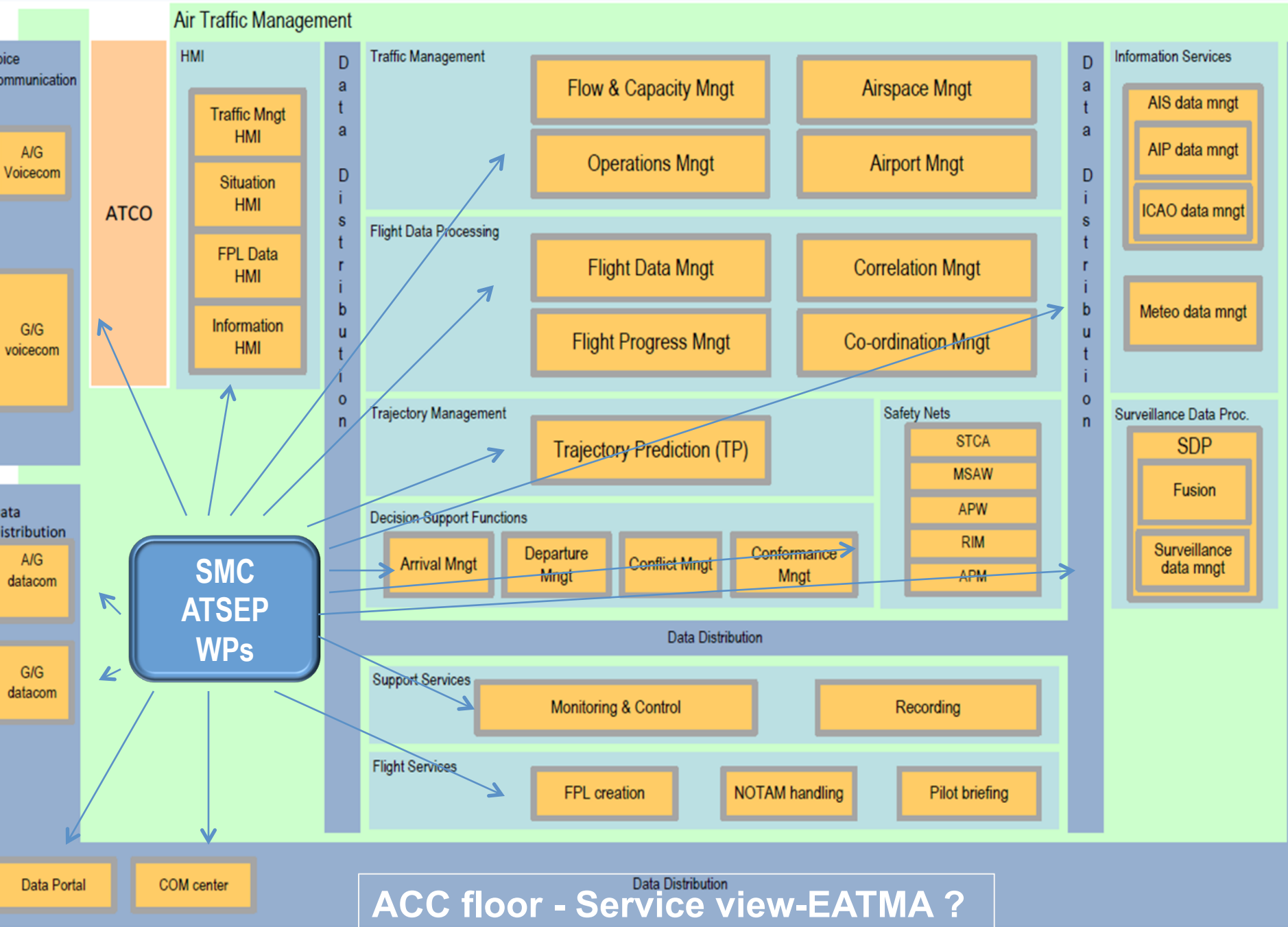
Meteorological Watch Office Aerodrome Meteorological Offices Meteorological Stations

Air Traffic Flow Management (ATFM)

- Provision of the local ATFM
- Provision of the central ATFM

Air Space Management (ASM)

- Provision of the local ASM (Pre-tactical/ASM Level 2 and tactical/ASM Level 3) service



Cyber security in CNS/ATM-

A Technological Toolset for the ATSEP WP

- The issue of **Cybersecurity** for ATM is complex* as it includes the physical security at **local and remote CNS mission critical installations**, the networking elements (space and ground) , the **ATM specific attack vectors** e.g. on Surveillance (i.e. **spoofing**), jamming of space navigation or RPAS, and **any potential combination of the above**
- IFATSEA proposes a *Technical Supervision model instantiated in each ATSEP WP, that refers to a beyond state of the art HOLISTIC concept of **an event object**. This will be **build in individual new CNS/ATM systems feeding information** , deducted/collected from specific sensors (s/w and h/w), **centrally**.*
- ***This will allow** , after processing , to inform of **their specific health status (incl Cyber)**, with predictive capabilities, in the SMC domain on the ATSEP WP.*
- This architectural element will provide an interoperable **ANSP (level) Total ANS systems situational awareness** , with Cyber-Security capability, **in a cost effective way**.
- It will be capable of addressing legacy and SWIM based systems and processes.

*CNS System specifications are public!



Description of the IFATSEA SMC-Cyber Concept for the ATSEP Working Position

It describes a **high level architectural approach** to addressing the cybersecurity issue for ANSPs for short and mid-term (also for Legacy).

The architecture is aimed at :

- **bridging the current gap of the lack of specific tools and procedural measures,**
- **addressing the integration of cybersecurity in a complex system** of systems such as SESAR and NextGen etc.

It provides elements of a long term approach so as to:

- transform and standardize the monitoring and control of critical system Technical processes
- achieve a predictive system awareness in terms of its health status, both at the level of service provided but also in performance of all system functions in terms of cybersecurity.
- Achieving the monitoring of all the Operational systems

Description continued..

The IFATSEA approach takes into account **the safety and time criticality of ANS services**. It is **not addressed as a purely IT Security project** but with a **holistic approach** encompassing :

- Airspace related(*signal in space*),
- IT related and Infrastructure/installations or access control systems
- **Operational impact on ATCO and Pilots**
- the ANS environment **both for Legacy and SESAR systems**.

SESAR and NextGen being **Sociotechnical System of Systems**, it will be very difficult to address issues like **cascade failures**.

Cascade failures are a potential reality due to the tight coupling, interoperability and interrelation of the new processes (*especially under Time pressure*) .

What does it do?

Main functionalities of SMC-Sec ATSEP working positions

- Monitor the **performance of systems and services**
- **Presentation** of system **health** including Cybersecurity alert levels (CDM with ATCO e.g. Security threat level)
- **Combines multiple failures** due to either malfunction or Cybersecurity
- **Enables Incident resolution and attribution to technical failure or Cyber attack**
- **Isolated event/incident** (cyber-technical) handling
- **Provides build in Resilience for pro and post incident** (through configuration management) and or Decision support tools
- **Incident reconstruction**
- **Fusion** of all the above data by evaluating continuously based on rules in order to produce/identify new patterns/events
- Manage a network of **geographically distributed** systems/sensors
- **Recording and replay**

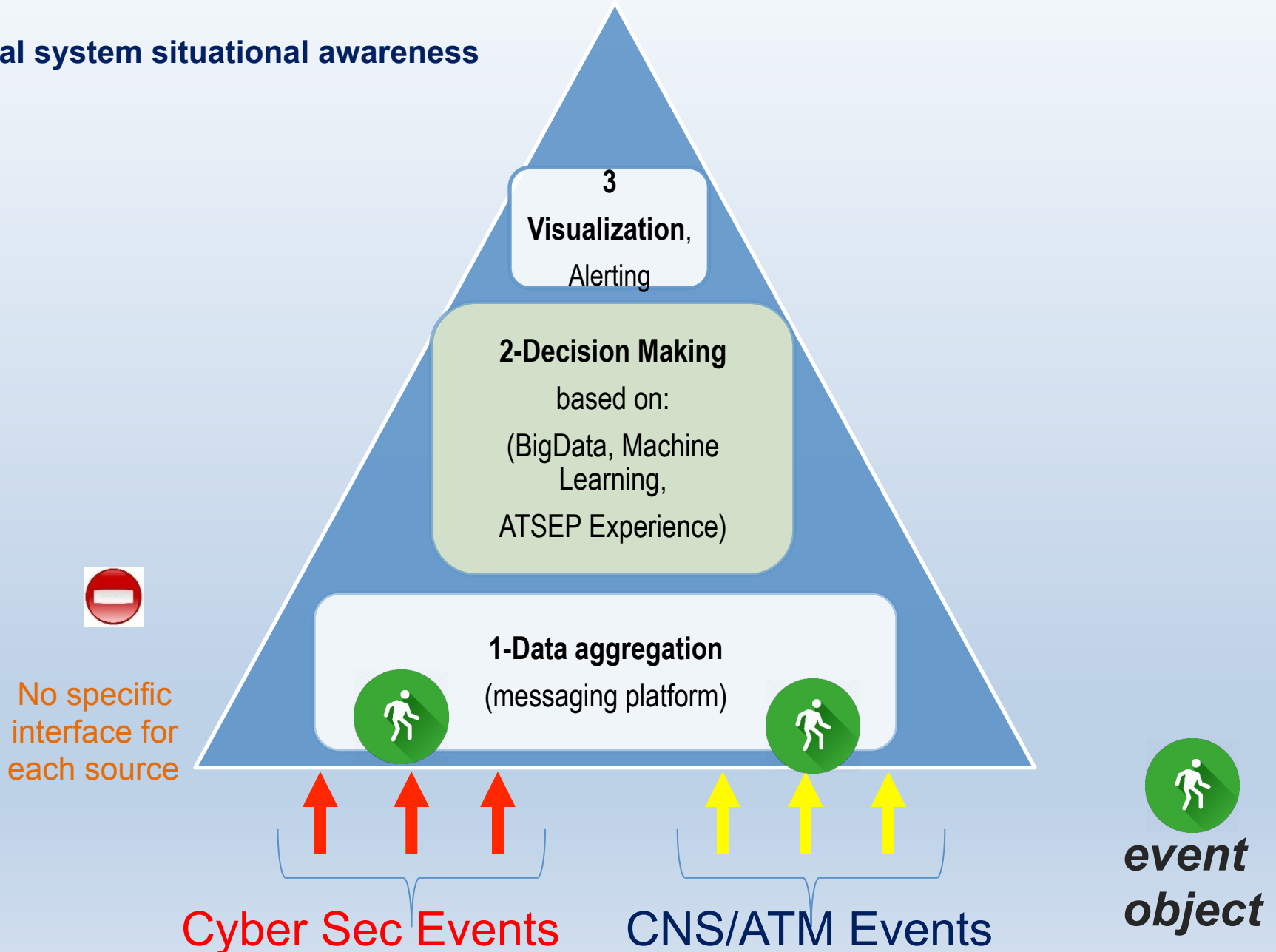
Principles of Concept design



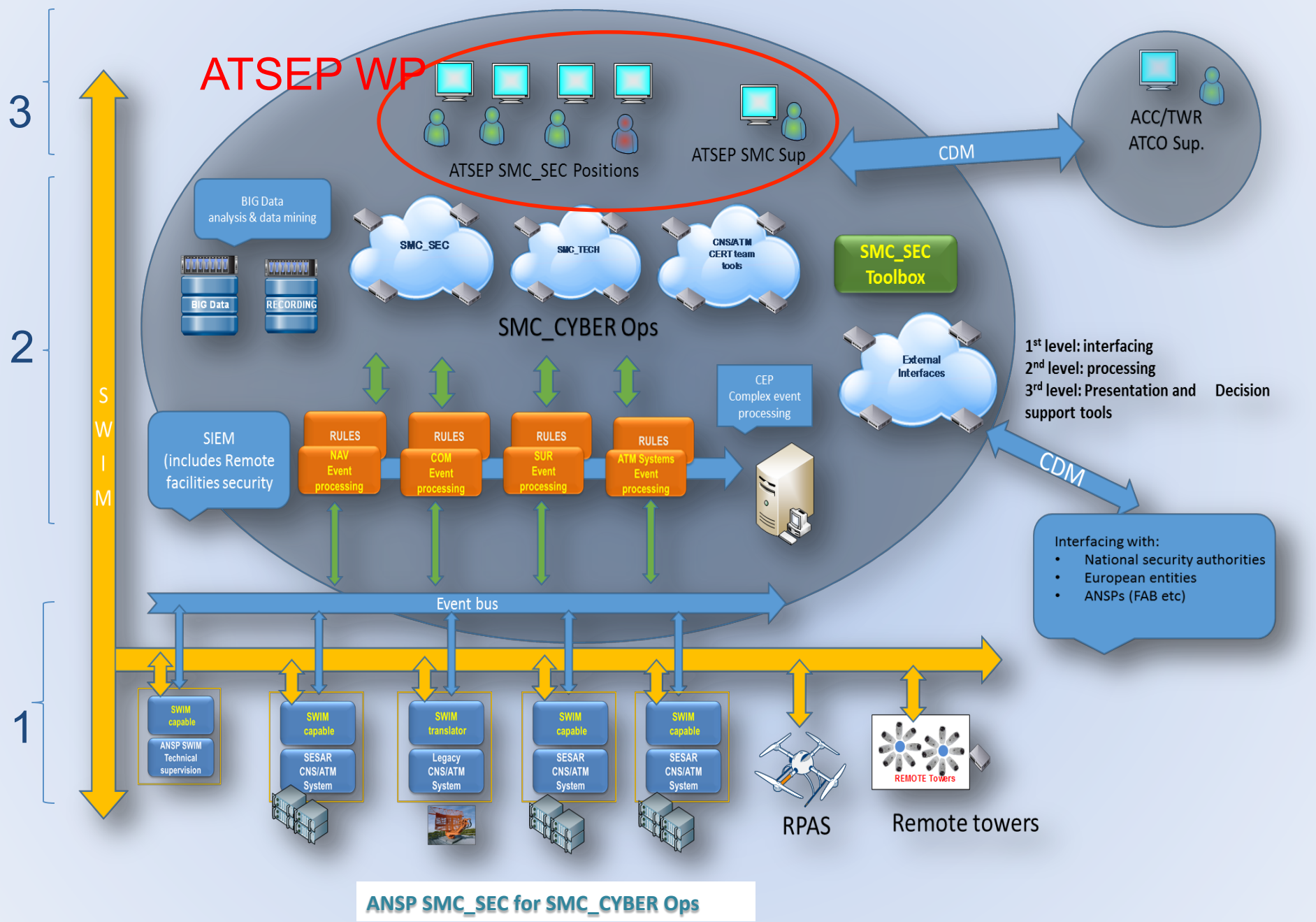
- The event effect must **not** reach the Controller or Pilot (if at all possible).
(Note: Navigation info is transmitted directly to the pilot).
 - *We consider that when this happens the system has failed to protect the ops actor*
- Cybersecurity events are treated as **any other technical event**. These events are not only IT but may include physical elements such as '**signal in space**', RPAS, DoS, or procedures.
- ATSEP on duty must have the **tools** and **training** to **distinguish** whether the event is technical failure or security (**this will require research and standardization activity*)
- Concepts such as Remote towers must integrate C&C in SMC/Cyber (concept must be future proof including new Business models and Service Oriented Architecture).
- Cyber-attack vector and pattern recognition and analysis is done locally and integrated in a Pan-European image or global image although at different levels.

IFATSEA SMC-Cyber Concept for the ATSEP WP

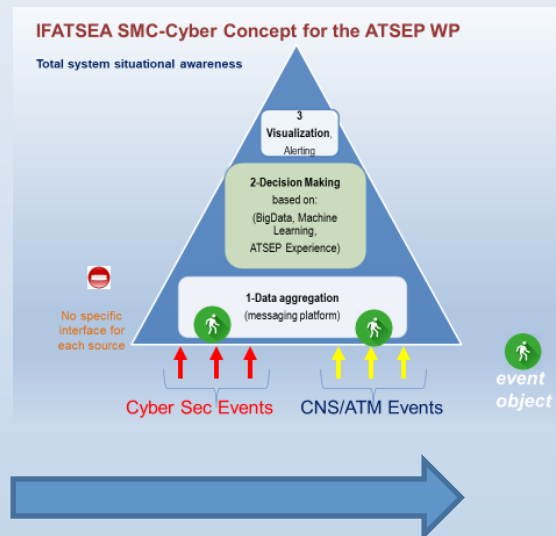
Total system situational awareness



IFATSEA SMC-Cyber Concept in depth



ATSEP Working position evolution



ATSEP Working position





Technical description and operation

- A cybersecurity related event, is **considered as any other event**, taking of course into account the type may be of a transversal nature, impacting more than one process or service in the ANS environment. (**....Cascade failures*)
- The system's technical health events including Cyber events will feed a Complex Event Processing (CEP) to be implemented at Local ANSP level.
- According to the Cyber and System's health related predefined criteria (rules), the outcome of this CEP has to be treated accordingly and in any case as **close as possible to real time**.
- Cyber threats or suspicious activities or patterns of activities detected will be immediately addressed locally and communicated to a higher level (National) or further through to supranational entities.
- ATSEP Cybersec specialist must **understand the impact of mitigation measures of a Security event handling on the Total system**.

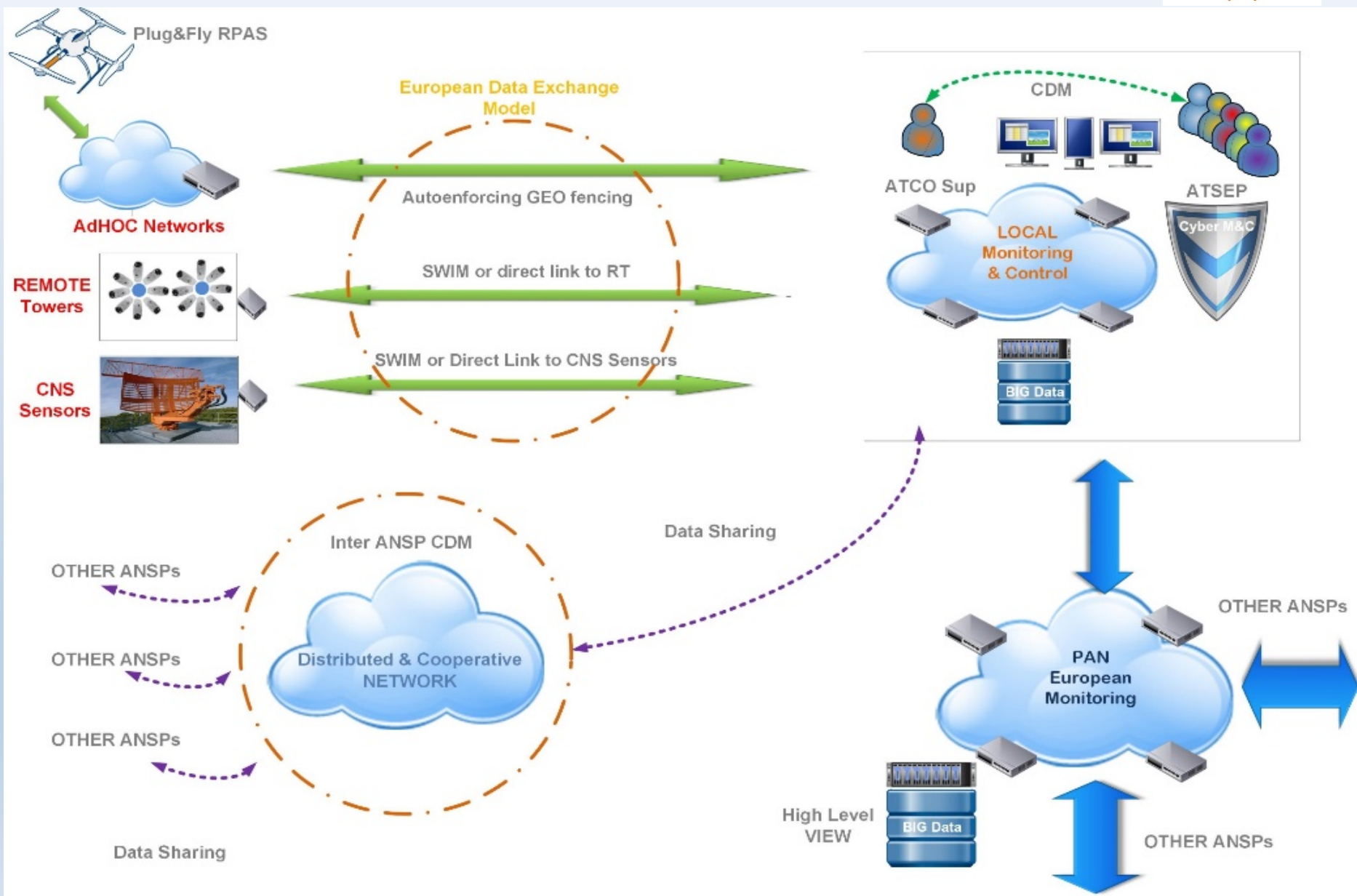
Beyond the state of the art-*to be researched*



- IFATSEA proposes the **definition of a System Health SMC_XML Object*** concept to be researched in the context of Security by design.
 - An instance of this object will be running in every CNS&ATM system communicating centrally with the **Systems Monitoring and Control function (SMC)** and results appearing on the ATSEP_WP
 - This object will integrate a **Security Data Object** so as to build up a continuous holistic picture of the 'real time' system status, leading to an in depth system wide awareness.
 - The filtered output of the events created by these objects will be displayed post-processing on the screen of the ATSEP_WP on duty supported by decision making tools*.
 - The **Complex Event Processing & Analysis*** will be incorporated incrementally into ATSEP SMC duties, making it very **cost effective**.
- Designing systems with Cybersecurity in mind from the onset, enhanced with **SMC_SEC Object*** within a **SMC_XML object** over secure protocols will constitute a paradigm shift and create a robust Cybersecurity Capability for ANSPs.

**To be Researched -not existing today.*

IFATSEA High level abstract model of ANSP SMC_SEC INTEROPERABILITY



EU Framework ensuring Cybersecurity in ATM

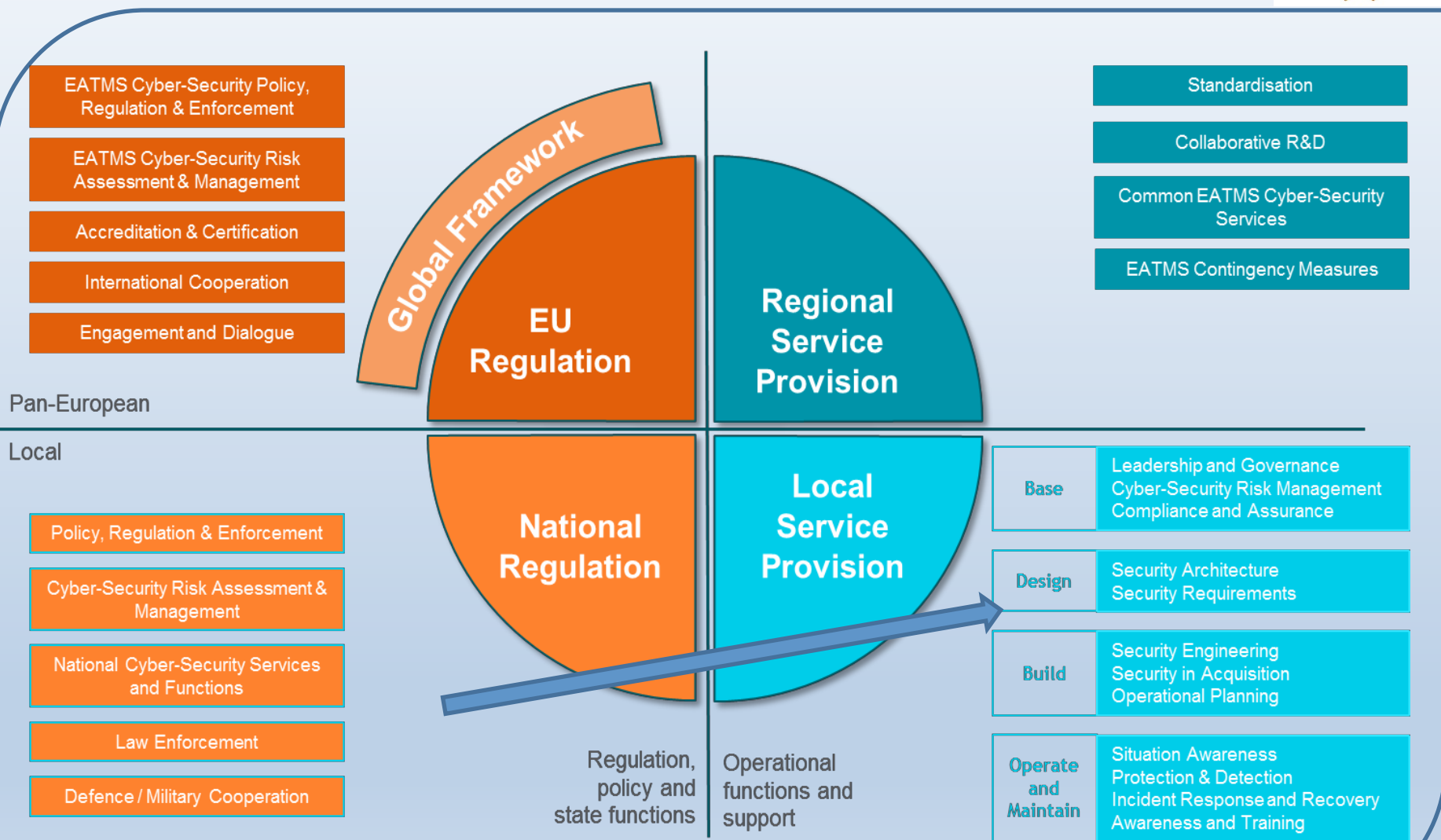
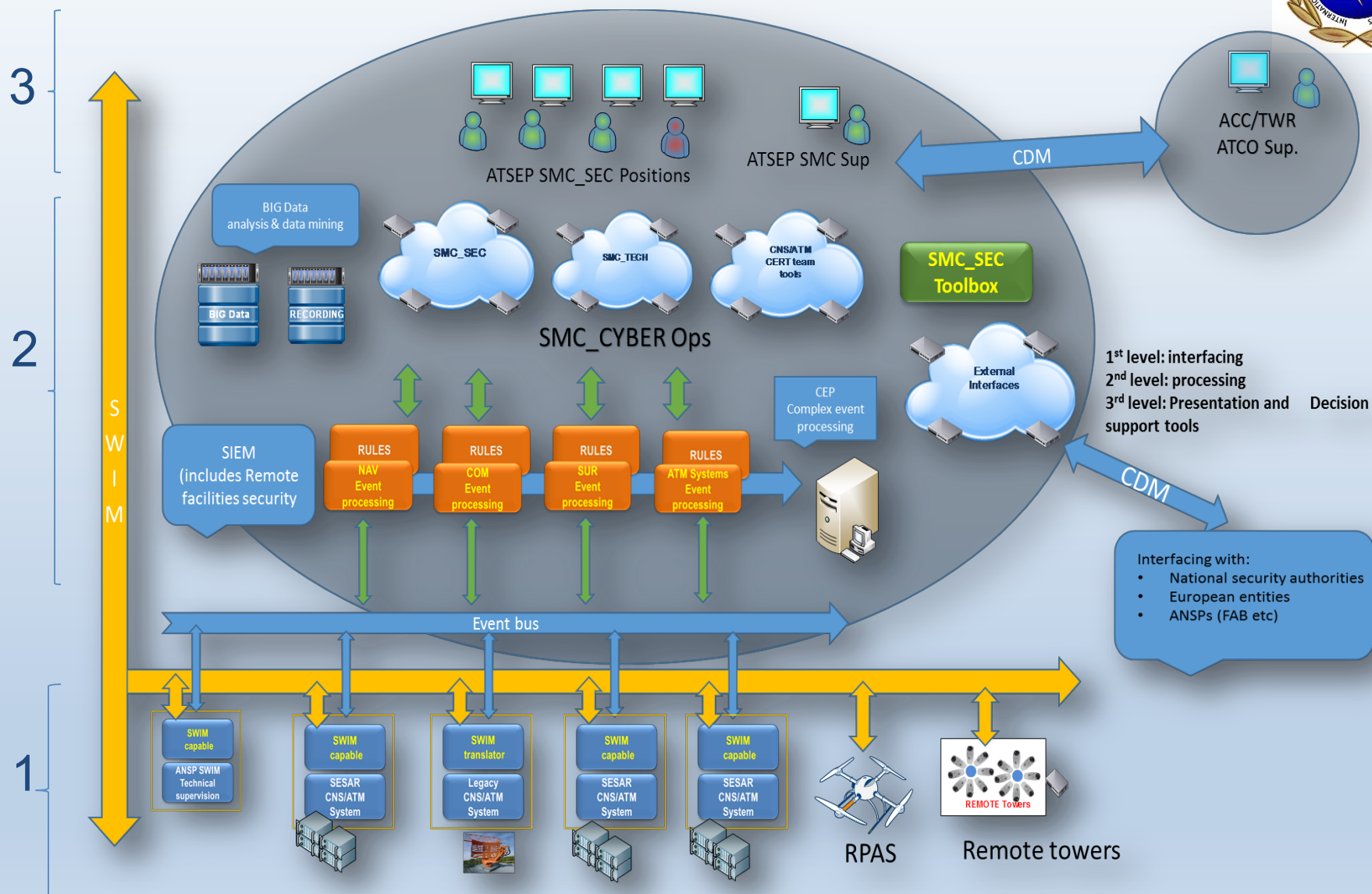
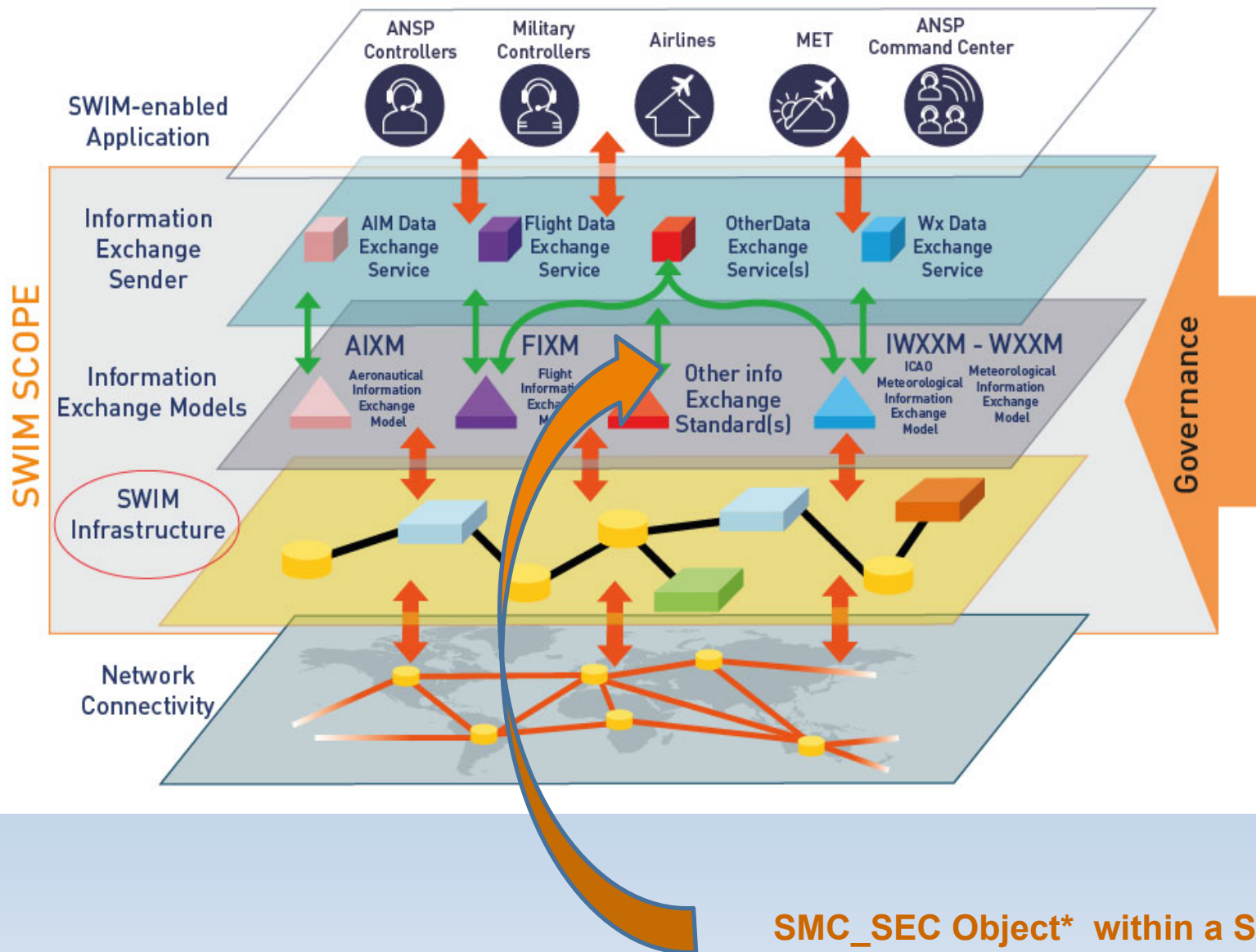


Figure 3: EU Framework for ensuring the Cyber-Security of ATM

ANSP SMC_SEC for SMC_CYBER Ops ARCHITECTURE



The SWIM based ATM information exchange concept



Main points on the **Human** element



One thing is for sure, all these new concepts are not without challenges for all the ATM actors.

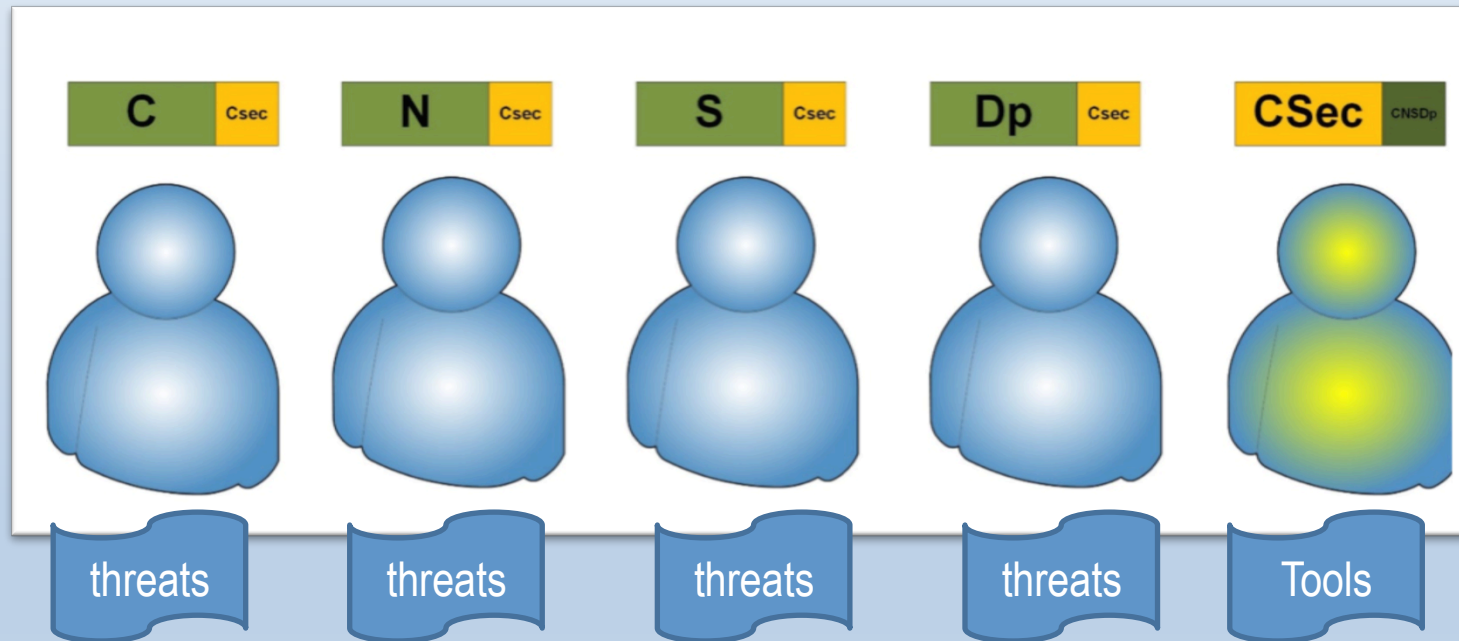
- 1) However, **ATSEP will require to run the Legacy systems beyond 2025** while working towards the implementation and integration of all new systems.
- 2) There will be:
 - New roles/duties and competences for ATSEP, driven by the new Technologies and **Automation, Digitalization** and even new **Business models**.
 - New Actors like RT, Virtual Centers (separated geographically)
 - New teaching disciplines to fulfill these new competences
- 4) Security and integrity wise, “Bullet proof” and resilient SYSTEMS , together with trained and competent personnel (ATSEP & ATCO) in order to avoid situations that will impact Safety and damage the image of Aviation Industry.

AAS

*“ Virtualization and distributed architecture will have a significant effect on the role of the ATSEP. Data and service assurance from third parties will require **new monitoring tools and an even greater emphasis on cyber security**. The ATSEP role will evolve to acquire new skills and take on these new responsibilities”.*

Impact on ATSEP Training (EU 2018/373) + AMC

- All are ATSEP and have received ATSEP Basic Training
- Cybersec specialist receives CNS basic training
- CNS/ATM ATSEP (specialists) receive CyberSEC training

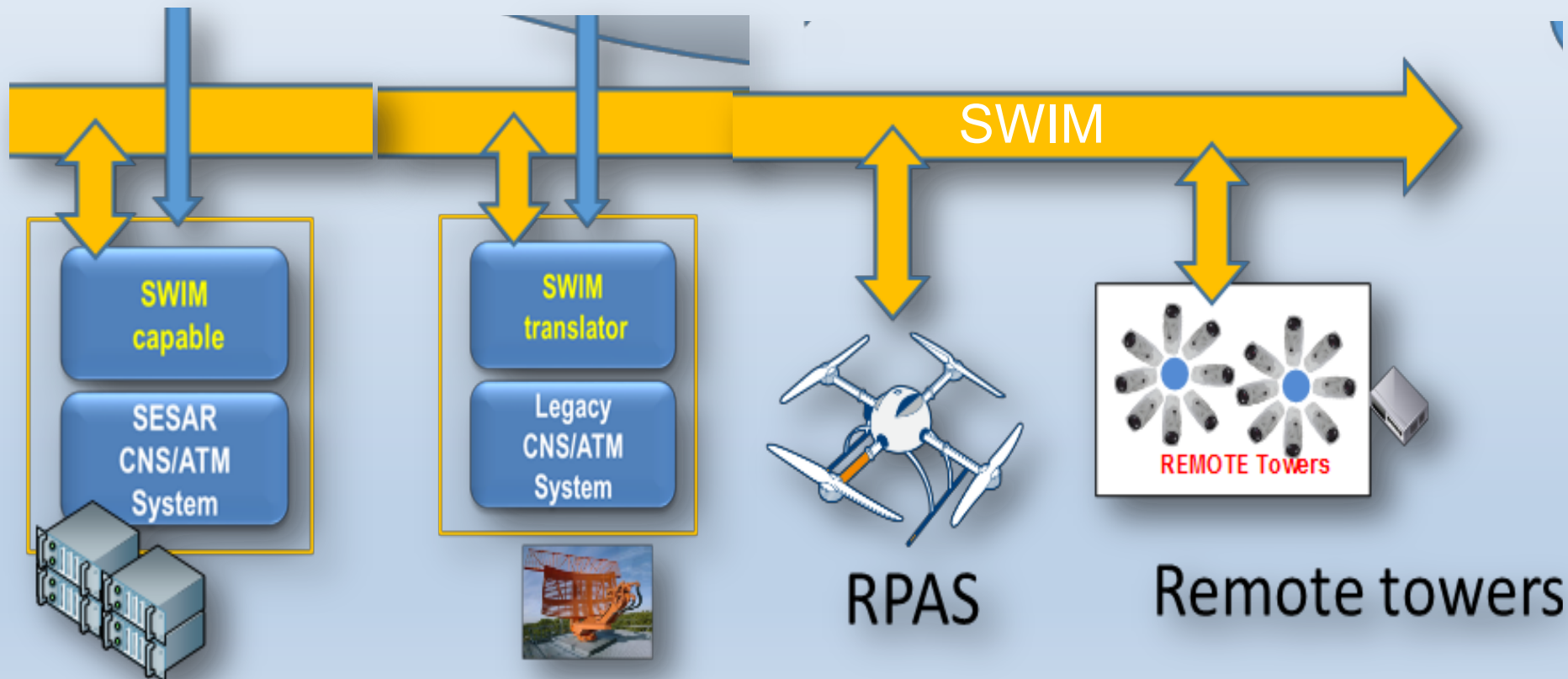




finally is the human!
(and the tools!)

Thank you for your attention
Any questions?

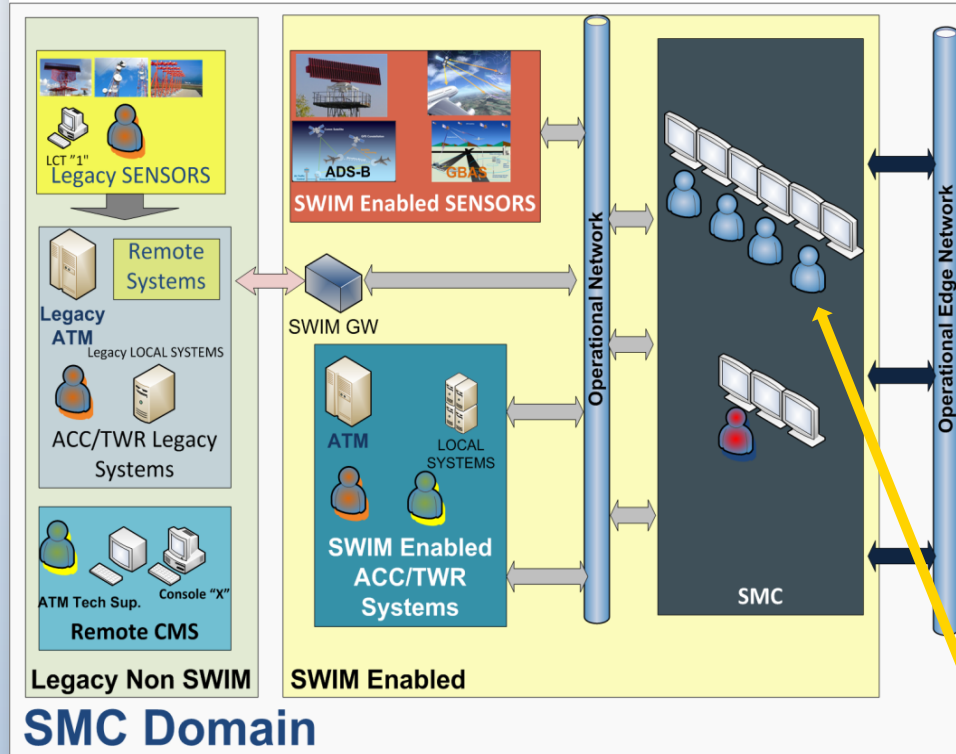
Connecting Legacy and Swim enabled systems to a common bus



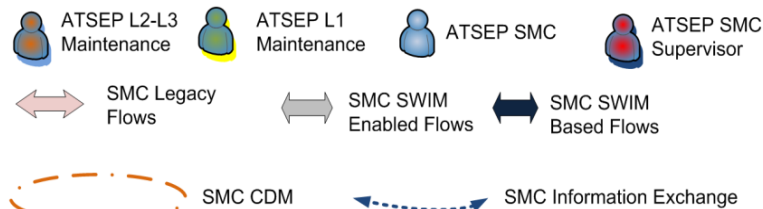
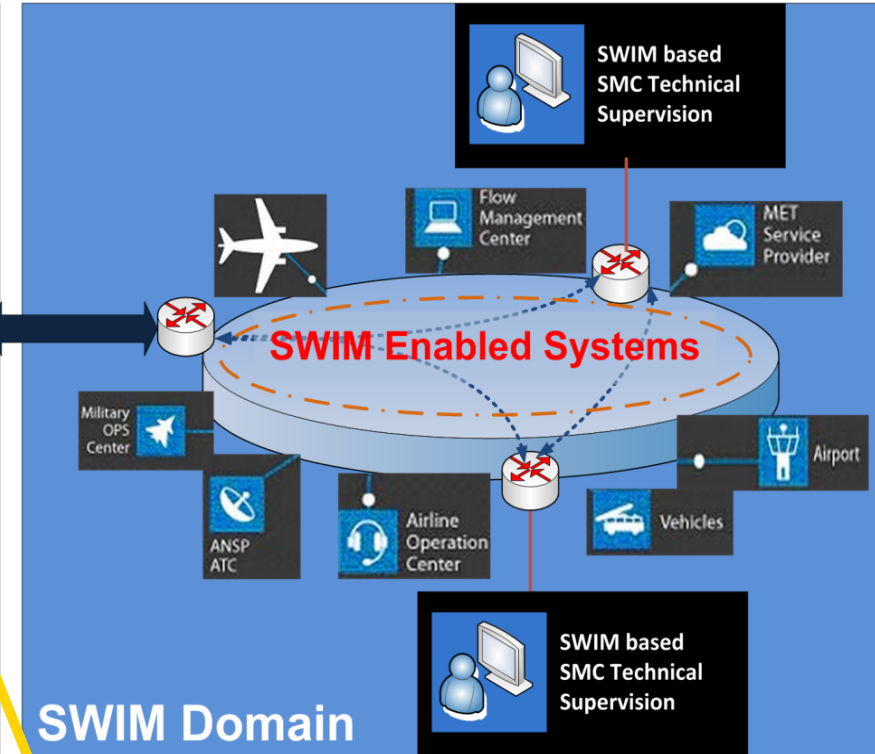
Legacy and SWIM based SMC of CNS/ATM systems for ANSPs



SWIM based SMC Technical Supervision



SWIM



SESAR Key Benefits Enablers:

- Full 4D trajectory
- Continuous descent and climb procedures
- Efficient taxi technologies and procedures
- Better flight profiles
- Optimized speed adjustments

ATSEP Cybersecurity specialist on duty