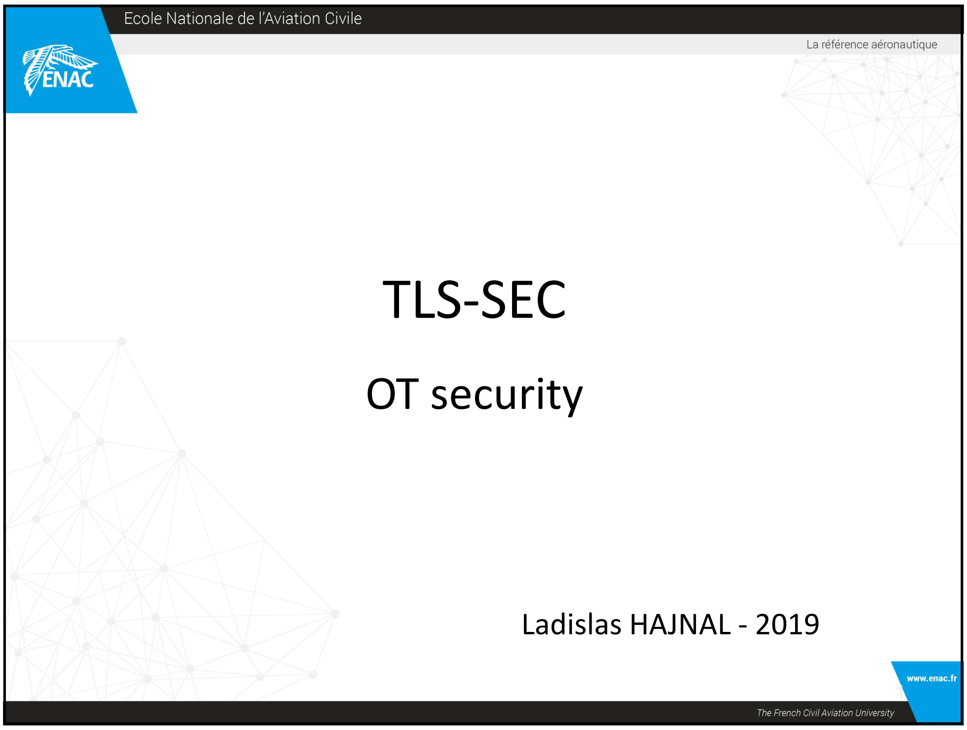


Ecole Nationale de l'Aviation Civile

La référence aéronautique

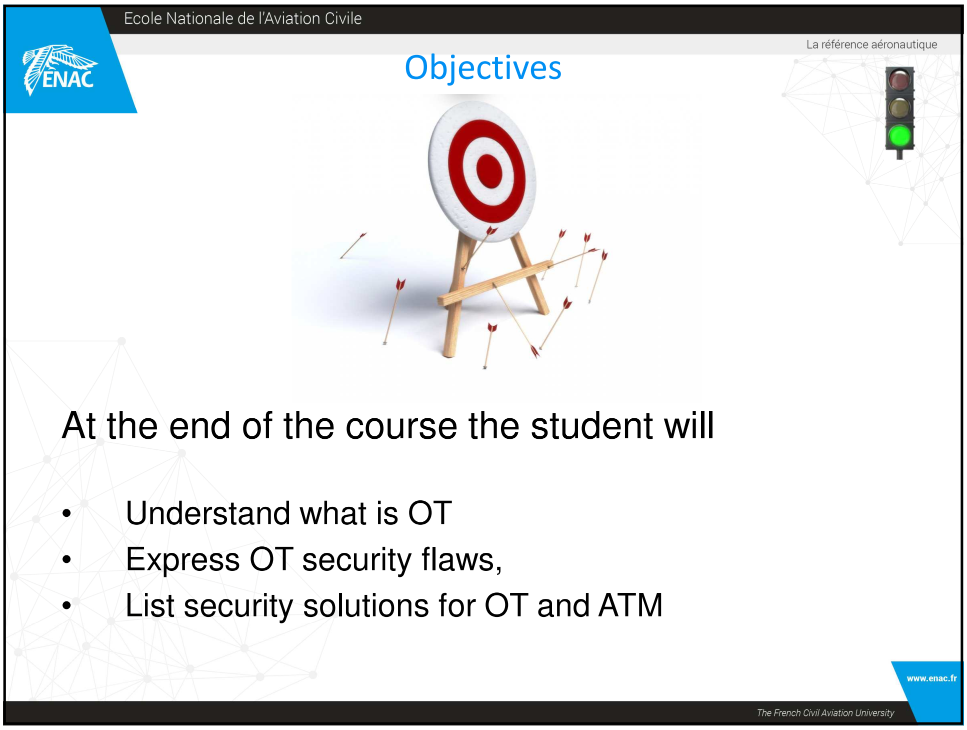
TLS-SEC

OT security

Ladislas HAJNAL - 2019

www.enac.fr

The French Civil Aviation University



Ecole Nationale de l'Aviation Civile

La référence aéronautique

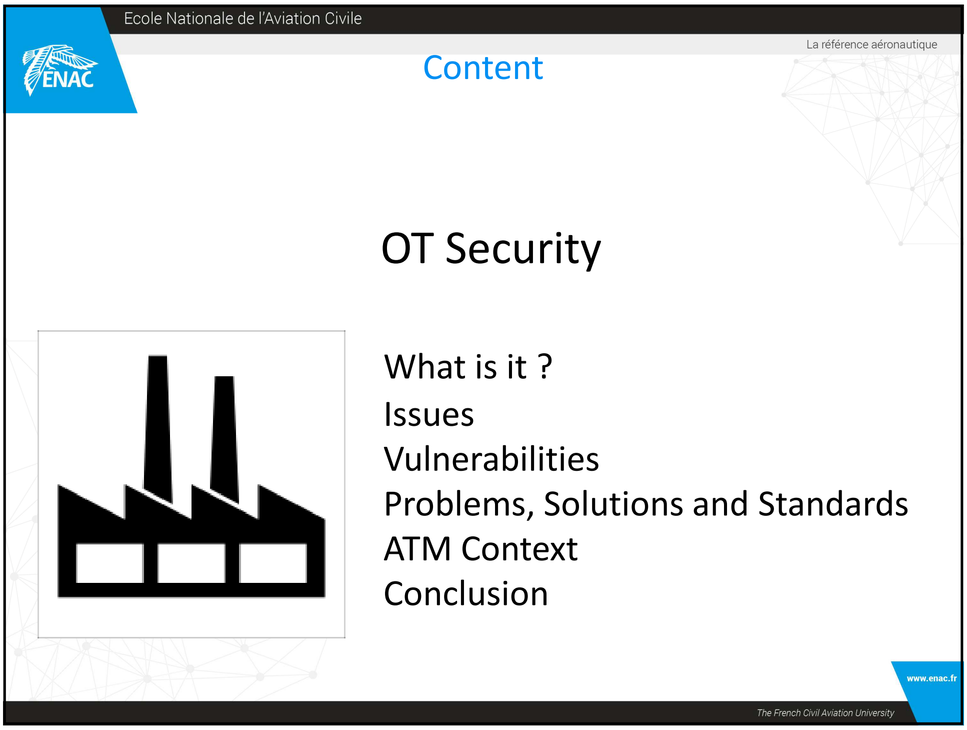
Objectives

At the end of the course the student will

- Understand what is OT
- Express OT security flaws,
- List security solutions for OT and ATM

www.enac.fr

The French Civil Aviation University



Ecole Nationale de l'Aviation Civile

La référence aéronautique

Content

OT Security

What is it ?
Issues
Vulnerabilities
Problems, Solutions and Standards
ATM Context
Conclusion

www.enac.fr

The French Civil Aviation University

Ecole Nationale de l'Aviation Civile

La référence aéronautique

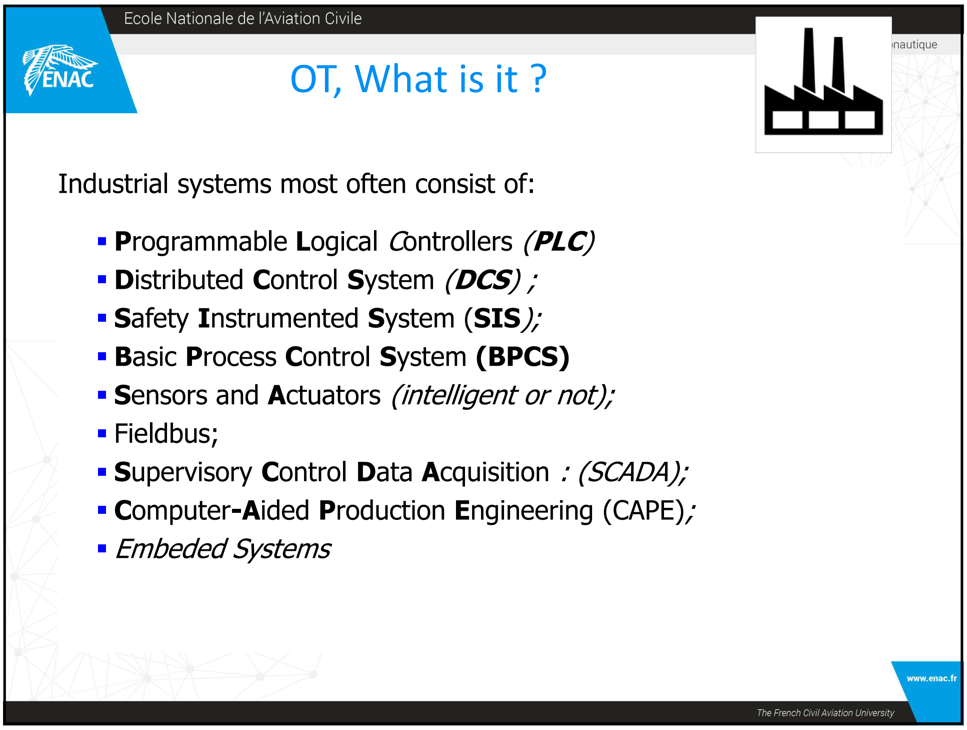
OT Security

What is OT ?

Issues
Vulnerabilities
Problems, Solutions and Standards
Civil Aviation Context
Conclusion

www.enac.fr

The French Civil Aviation University



Ecole Nationale de l'Aviation Civile

nautique

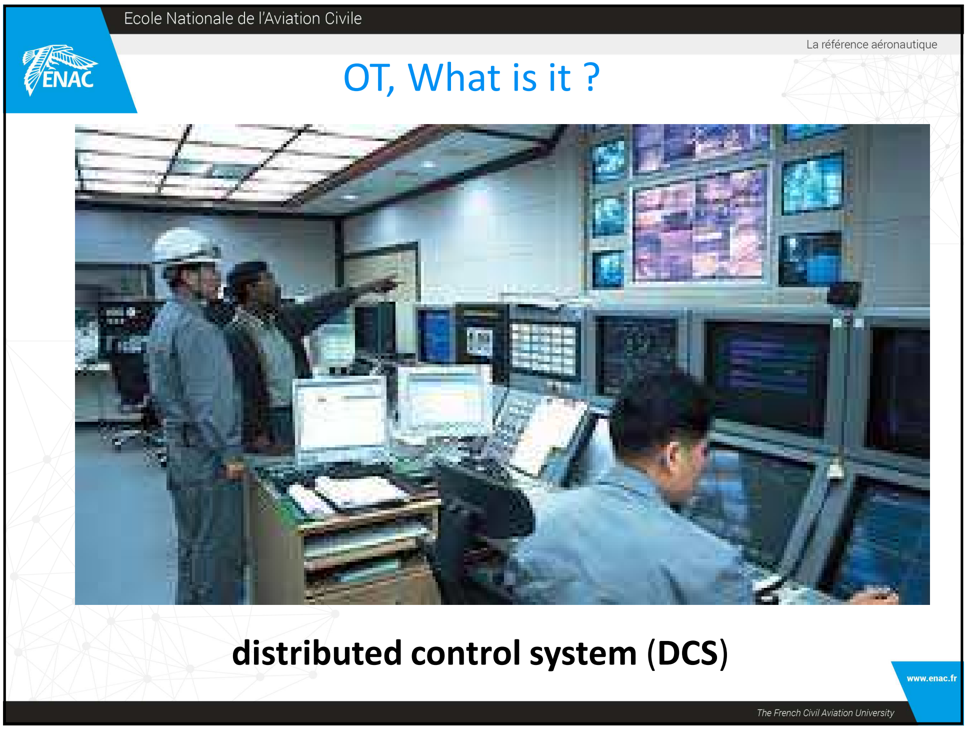
OT, What is it ?

Industrial systems most often consist of:

- **P**rogrammable **L**ogical *C*ontrollers ***(PLC)***
- **D**istributed **C**ontrol **S**ystem ***(DCS)*** *;*
- **S**afety **I**nstrumented **S**ystem (**SIS***);*
- **B**asic **P**rocess **C**ontrol **S**ystem **(BPCS)**
- **S**ensors and **A**ctuators *(intelligent or not);*
- Fieldbus;
- **S**upervisory **C**ontrol **D**ata **A**cquisition *: (SCADA);*
- **C**omputer-**A**ided **P**roduction **E**ngineering (CAPE)*;*
- *Embeded Systems*

www.enac.fr

The French Civil Aviation University



Ecole Nationale de l'Aviation Civile

La référence aéronautique

OT, What is it ?

distributed control system (DCS)

www.enac.fr

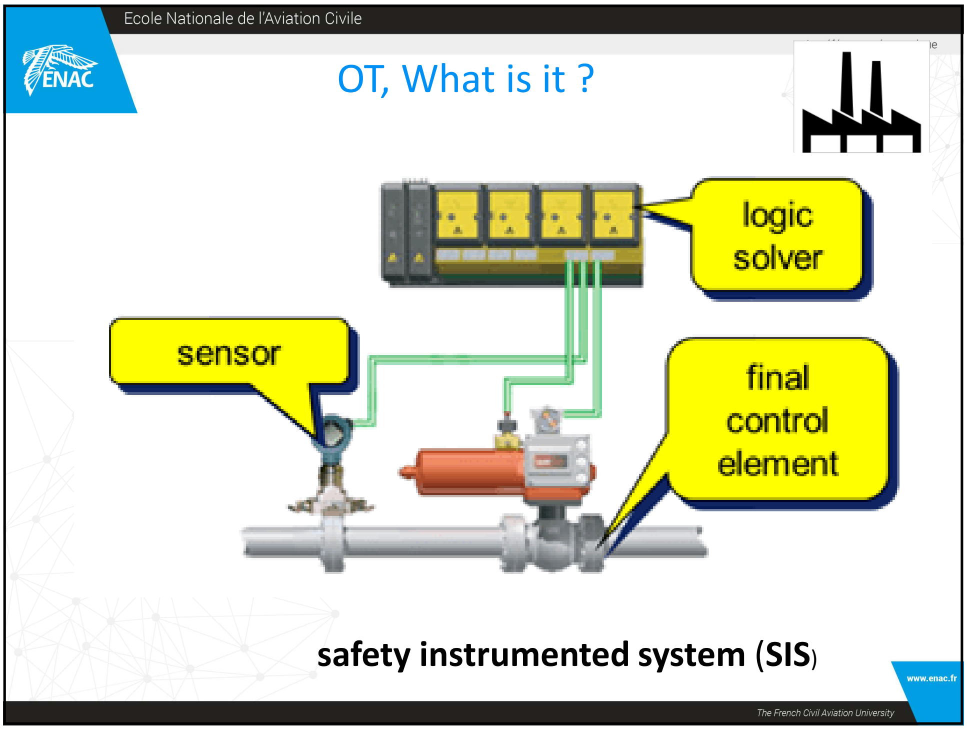
The French Civil Aviation University

Ecole Nationale de l'Aviation Civile

OT, What is it ?

www.enac.fr

The French Civil Aviation University



Ecole Nationale de l'Aviation Civile

OT, What is it ?

safety instrumented system (SIS)

www.enac.fr

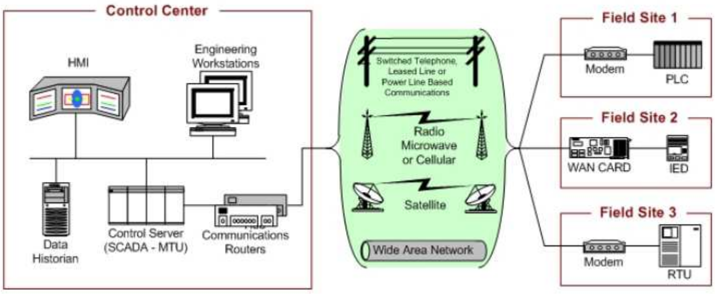
The French Civil Aviation University

Ecole Nationale de l'Aviation Civile

La référence aéronautique

OT, What is it ?

SCADA



Scada General Layout

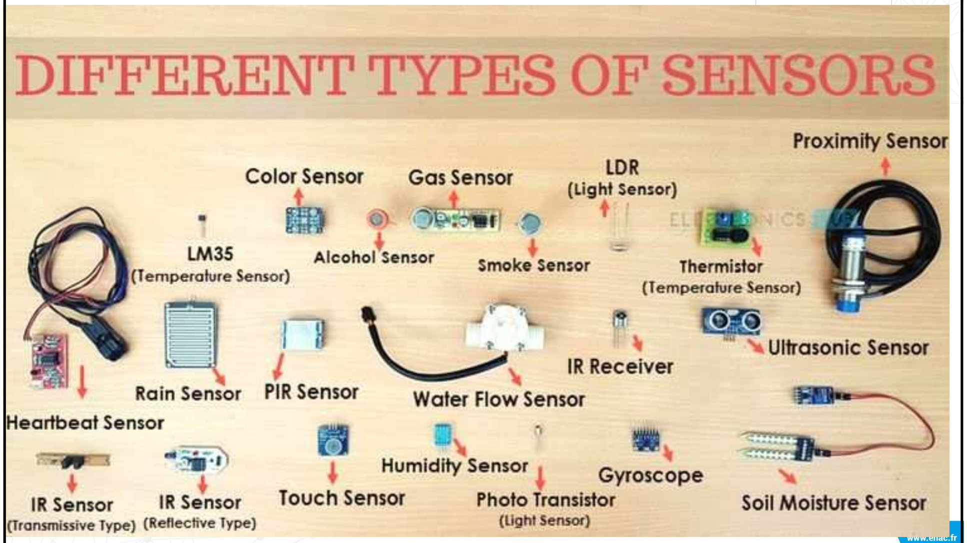
www.enac.fr

The French Civil Aviation University

Ecole Nationale de l'Aviation Civile

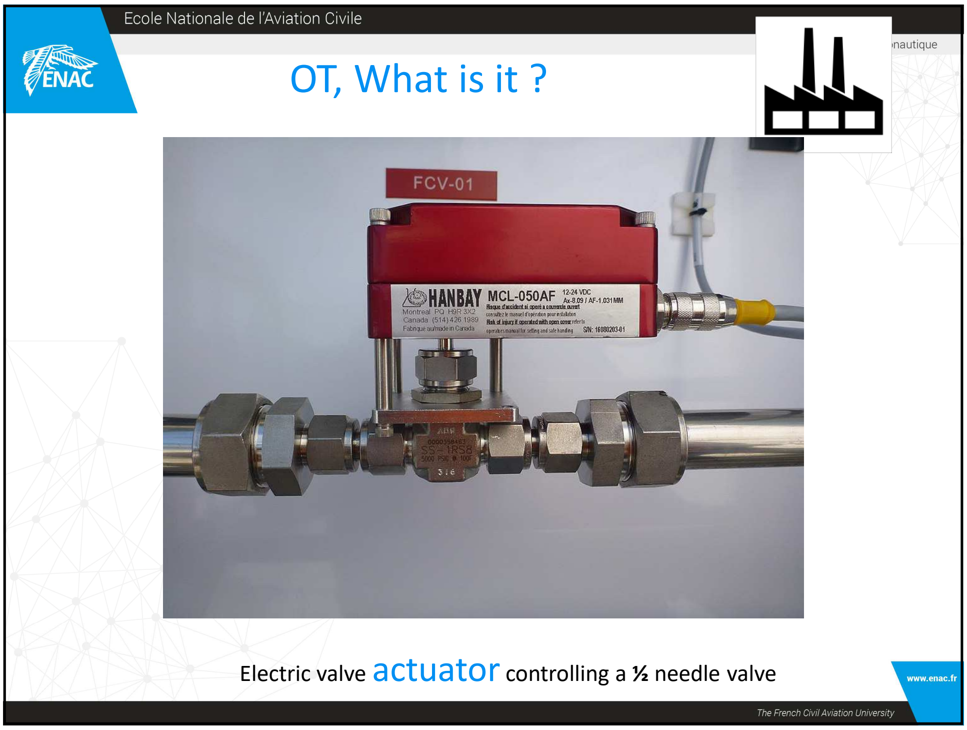
nautique

OT, What is it ?



www.enac.fr

The French Civil Aviation University



Ecole Nationale de l'Aviation Civile

nautique

OT, What is it ?

Electric valve actuator controlling a ½ needle valve

www.enac.fr

The French Civil Aviation University

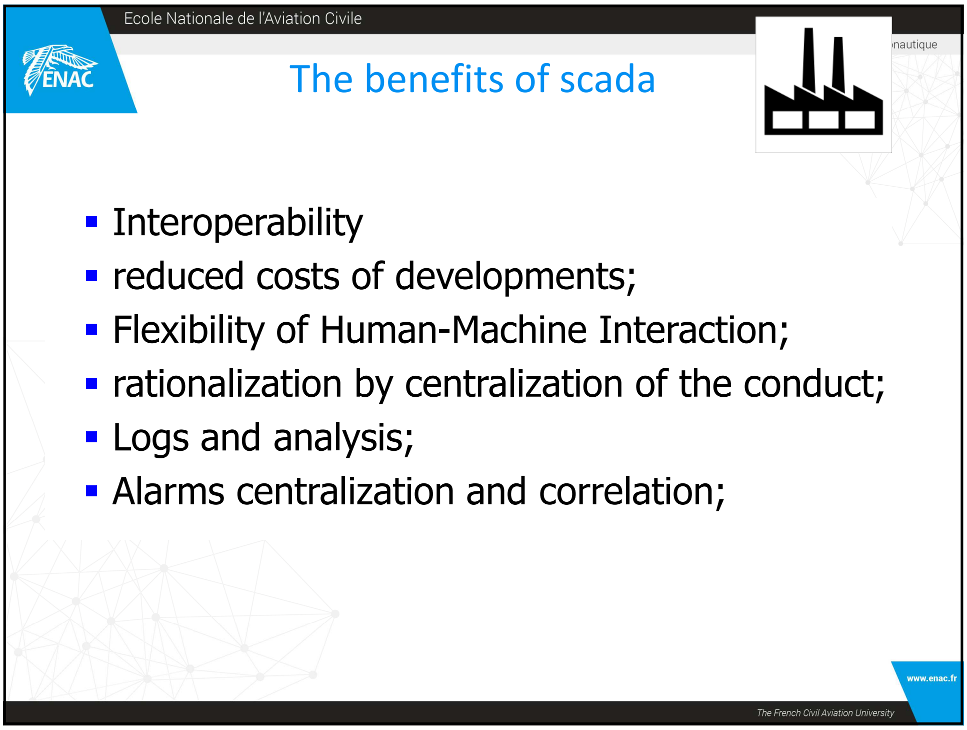
Ecole Nationale de l'Aviation Civile

nautique

OT, What is it ?

www.enac.fr

The French Civil Aviation University



Ecole Nationale de l'Aviation Civile

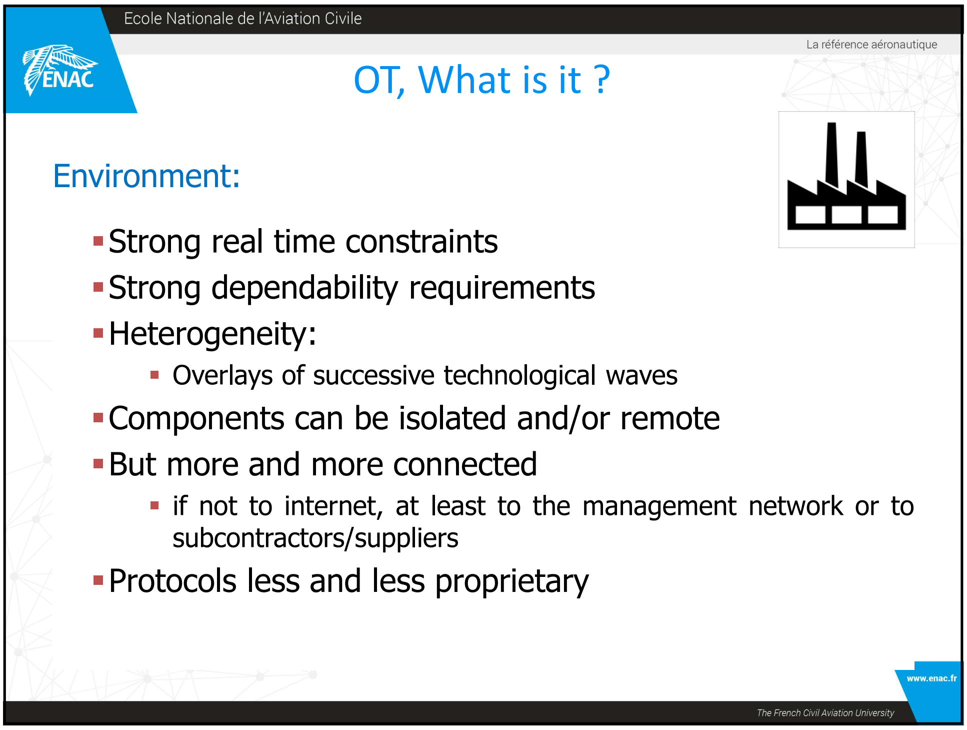
nautique

The benefits of scada

- Interoperability
- reduced costs of developments;
- Flexibility of Human-Machine Interaction;
- rationalization by centralization of the conduct;
- Logs and analysis;
- Alarms centralization and correlation;

www.enac.fr

The French Civil Aviation University



Ecole Nationale de l'Aviation Civile

La référence aéronautique

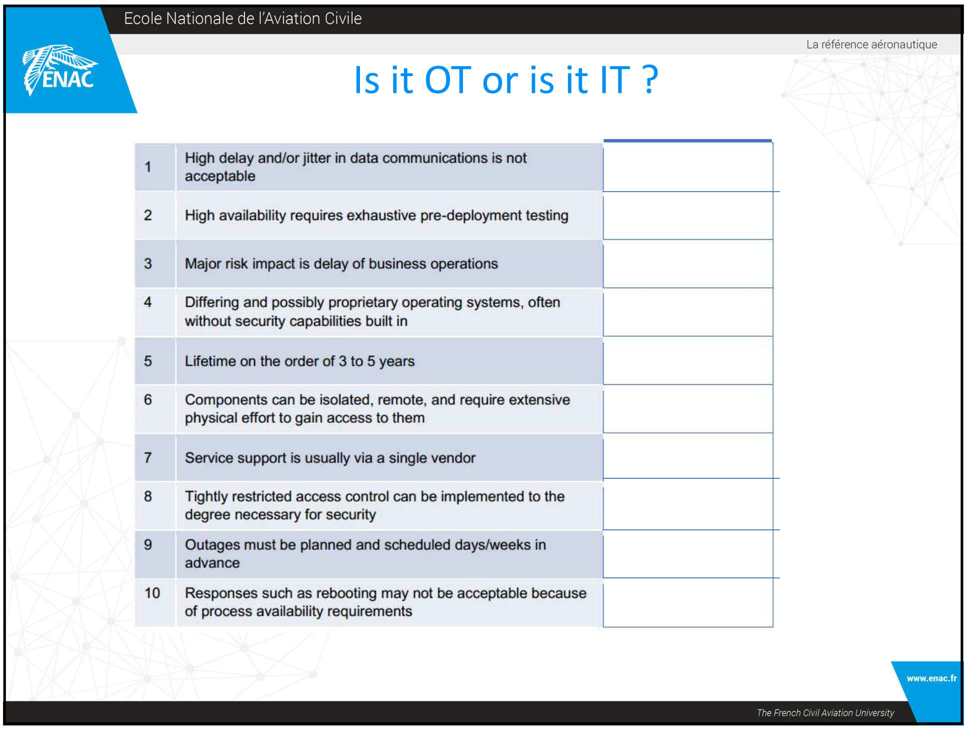
OT, What is it ?

Environment:

- Strong real time constraints
- Strong dependability requirements
- Heterogeneity:
  - Overlays of successive technological waves
- Components can be isolated and/or remote
- But more and more connected
  - if not to internet, at least to the management network or to subcontractors/suppliers
- Protocols less and less proprietary

www.enac.fr

The French Civil Aviation University



Ecole Nationale de l'Aviation Civile

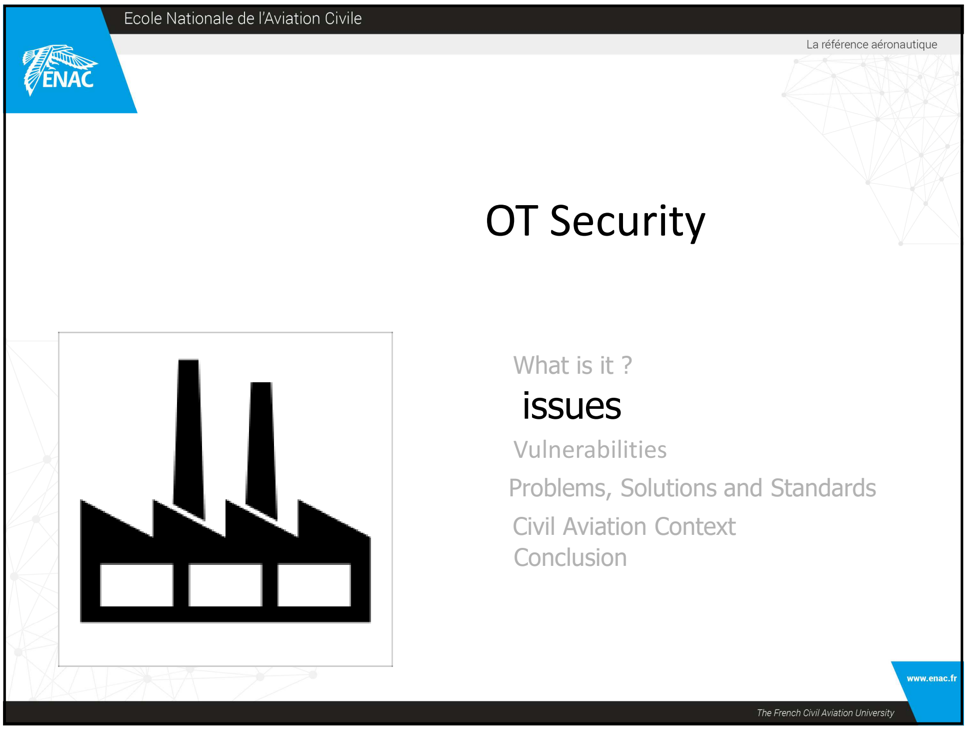
La référence aéronautique

Is it OT or is it IT ?

1	High delay and/or jitter in data communications is not acceptable	
2	High availability requires exhaustive pre-deployment testing	
3	Major risk impact is delay of business operations	
4	Differing and possibly proprietary operating systems, often without security capabilities built in	
5	Lifetime on the order of 3 to 5 years	
6	Components can be isolated, remote, and require extensive physical effort to gain access to them	
7	Service support is usually via a single vendor	
8	Tightly restricted access control can be implemented to the degree necessary for security	
9	Outages must be planned and scheduled days/weeks in advance	
10	Responses such as rebooting may not be acceptable because of process availability requirements	

www.enac.fr

The French Civil Aviation University



Ecole Nationale de l'Aviation Civile

La référence aéronautique

OT Security

What is it ?

issues

Vulnerabilities

Problems, Solutions and Standards

Civil Aviation Context

Conclusion

www.enac.fr

The French Civil Aviation University

Ecole Nationale de l'Aviation Civile

La référence aéronautique

OT ISS
What is at stake (1)

- 1982 - Russie - Piégeage d'un logiciel SCADA avec un cheval de Troie qui en s'exécutant a créé des dysfonctionnements et des erreurs de mesure qui ont engendré l'explosion d'un oléoduc.
- 2000 – Australie - Un employé licencié utilise ses codes d'accès encore actifs pour se connecter au SI industriel et provoque un désastre industriel en déversant 800 000 litres d'eau usées dans la nature

www.enac.fr

The French Civil Aviation University

Ecole Nationale de l'Aviation Civile

La référence aéronautique

OT ISS
What is at stake (1)

- 2003 : USA Ohio Centrale nucléaire Davis-Besse – Le vers SQL Slammer se propage du réseau d'enterprise vers l'ensemble du réseau industriel,

- 2008 – Pologne - Un adolescent polonais fait dérailler in tramway après avoir pris le contrôle du système d'aiguillage.

www.enac.fr

The French Civil Aviation University

Ecole Nationale de l'Aviation Civile

La référence aéronautique

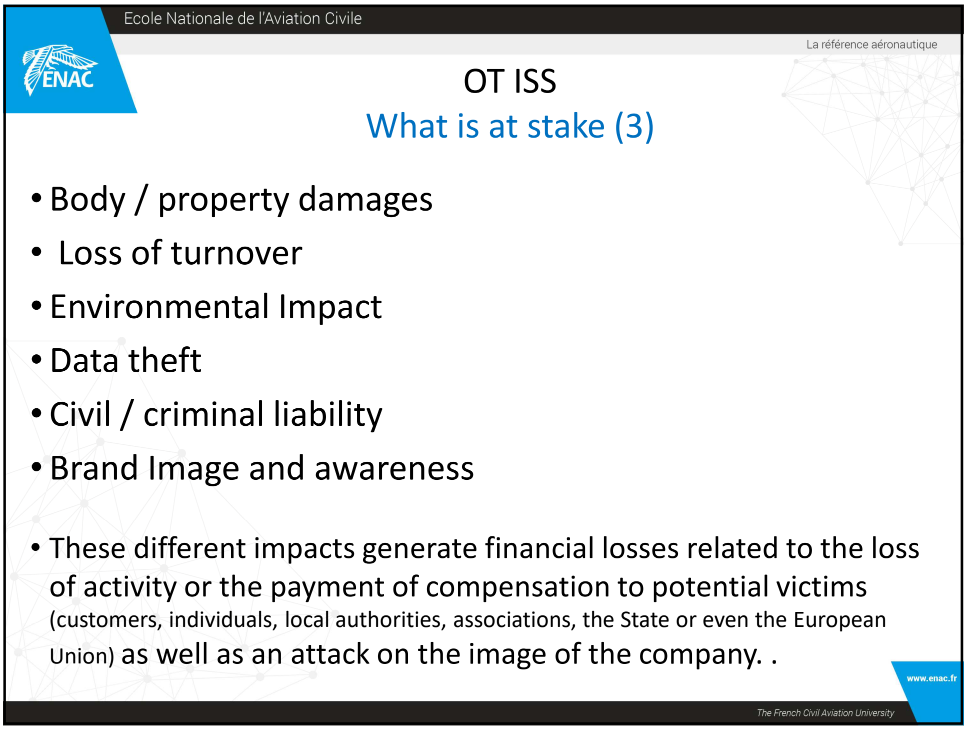
OT ISS

What is at stake (2)

- 2010 – Iran – Opération Olympic Games – Le vers stuxnet ralentit le programme iranien d' enrichissement d'uranium en détruisant les centrifuges.
- 2012 – Canada – des Hackers Chinois tenu responsables d'une Intrusion sur les systèmes de Telvent, le géant de la production d'énergie

www.enac.fr

The French Civil Aviation University



Ecole Nationale de l'Aviation Civile

La référence aéronautique

OT ISS

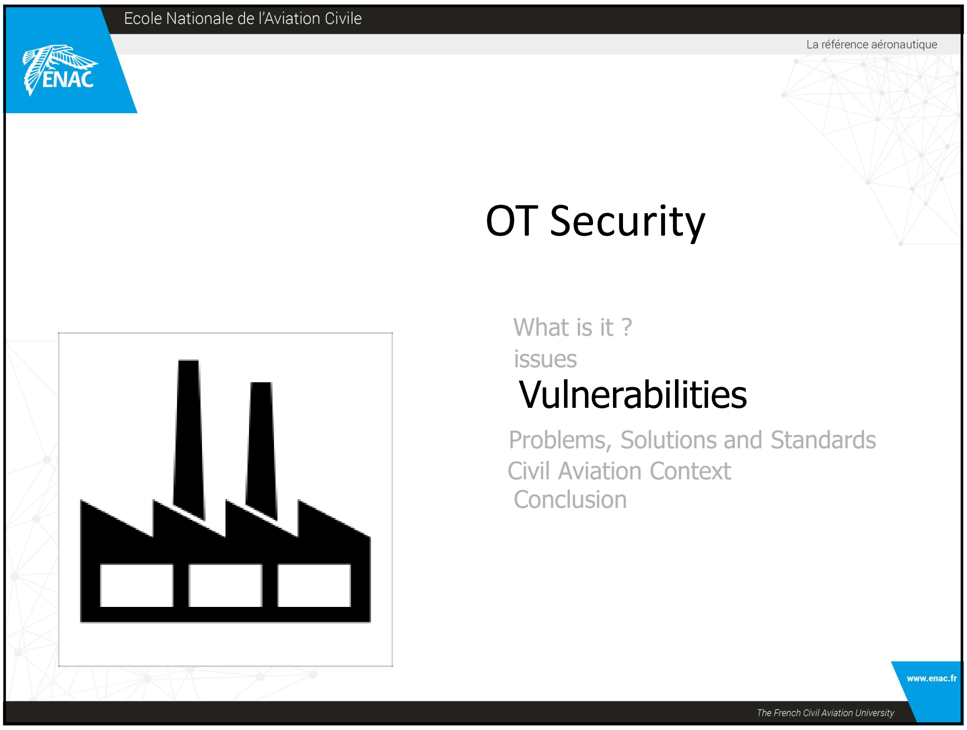
What is at stake (3)

- Body / property damages
- Loss of turnover
- Environmental Impact
- Data theft
- Civil / criminal liability
- Brand Image and awareness

- These different impacts generate financial losses related to the loss of activity or the payment of compensation to potential victims (customers, individuals, local authorities, associations, the State or even the European Union) as well as an attack on the image of the company. .

www.enac.fr

The French Civil Aviation University



Ecole Nationale de l'Aviation Civile

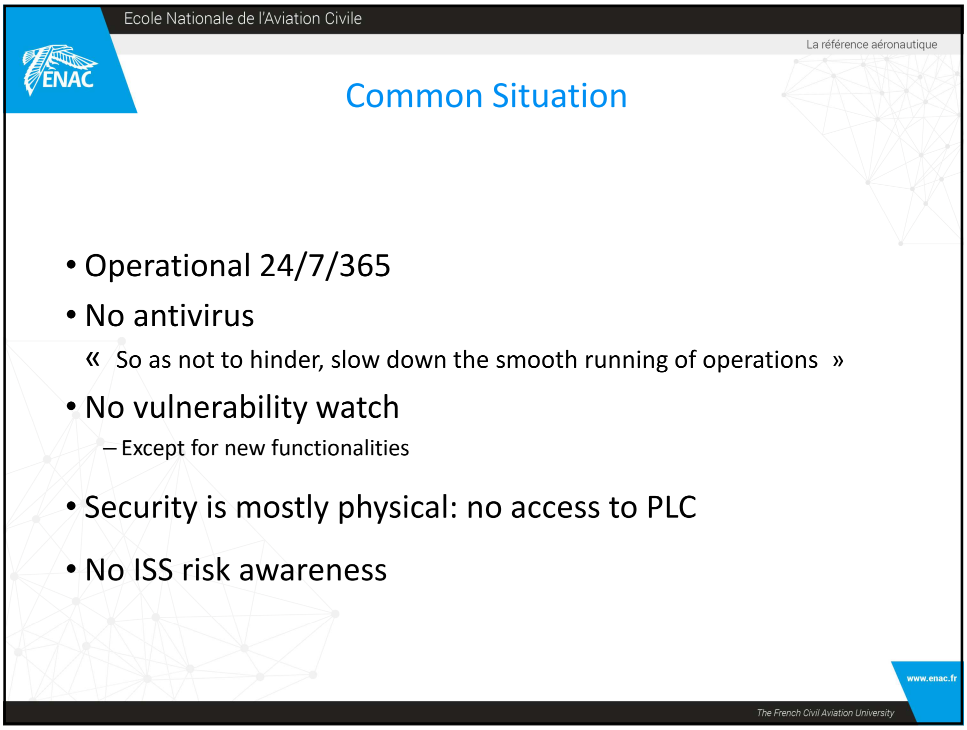
La référence aéronautique

OT Security

What is it ?
issues
Vulnerabilities
Problems, Solutions and Standards
Civil Aviation Context
Conclusion

www.enac.fr

The French Civil Aviation University



Ecole Nationale de l'Aviation Civile

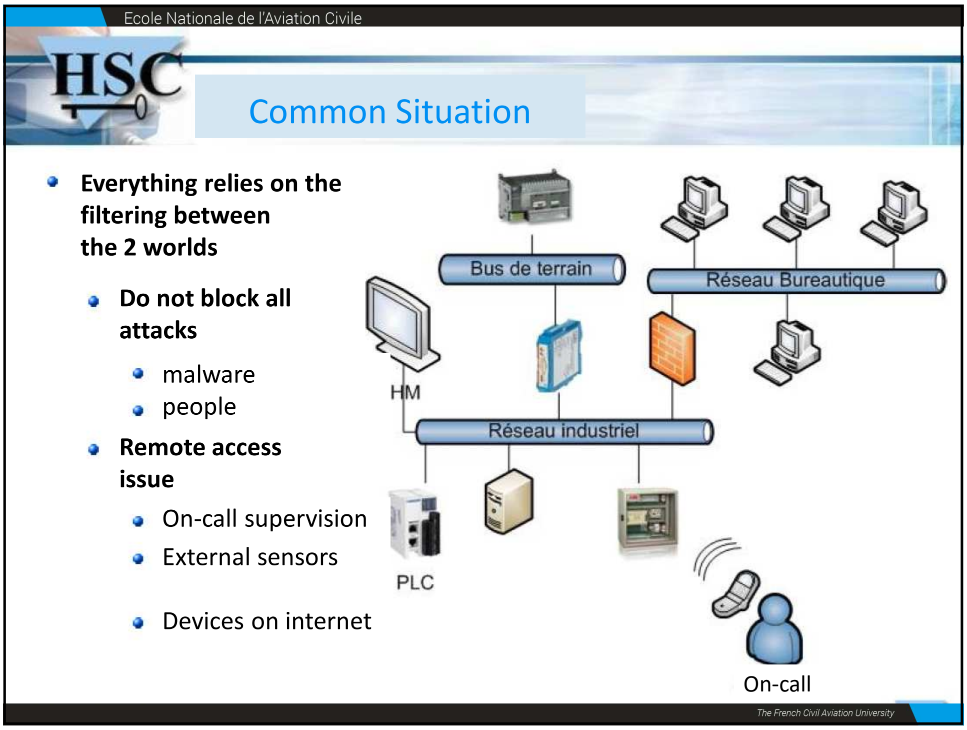
La référence aéronautique

Common Situation

- Operational 24/7/365
- No antivirus
  « So as not to hinder, slow down the smooth running of operations »
- No vulnerability watch
  – Except for new functionalities
- Security is mostly physical: no access to PLC
- No ISS risk awareness

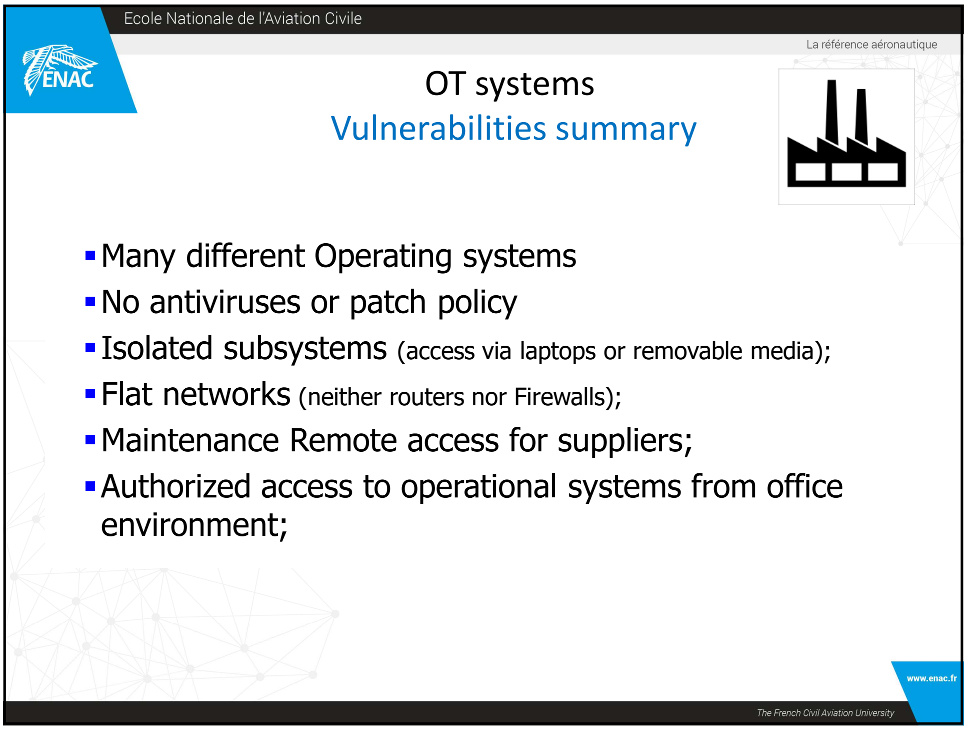
www.enac.fr

The French Civil Aviation University



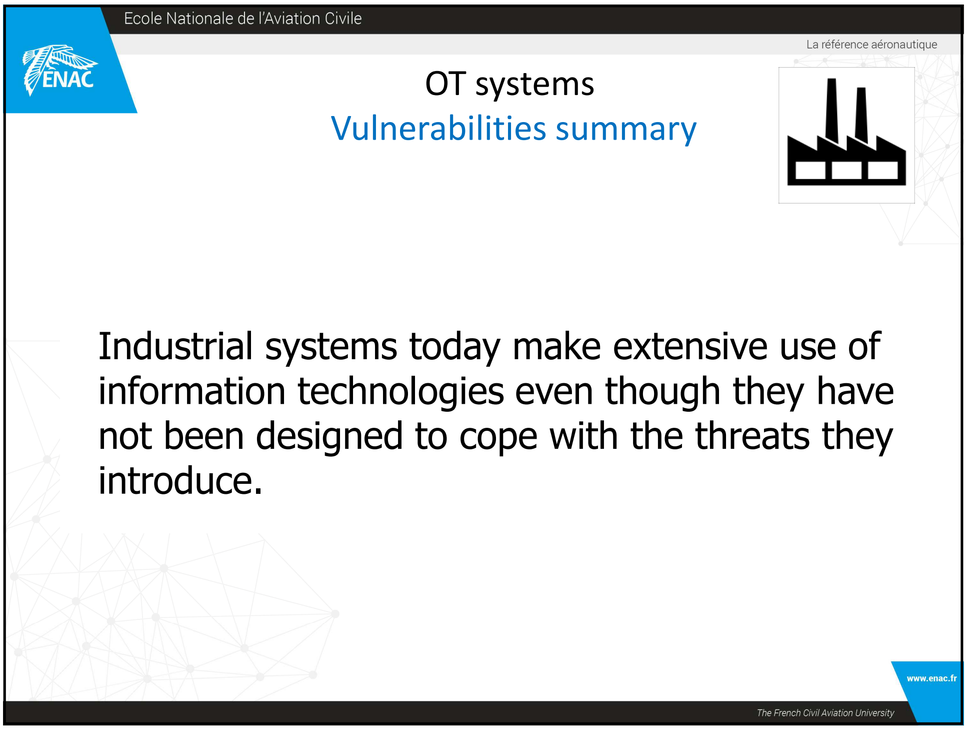
Common Situation

- Everything relies on the filtering between the 2 worlds
  - Do not block all attacks
    - malware
    - people
  - Remote access issue
    - On-call supervision
    - External sensors
    - Devices on internet



OT systems
Vulnerabilities summary

- Many different Operating systems
- No antiviruses or patch policy
- Isolated subsystems (access via laptops or removable media);
- Flat networks (neither routers nor Firewalls);
- Maintenance Remote access for suppliers;
- Authorized access to operational systems from office environment;



Ecole Nationale de l'Aviation Civile

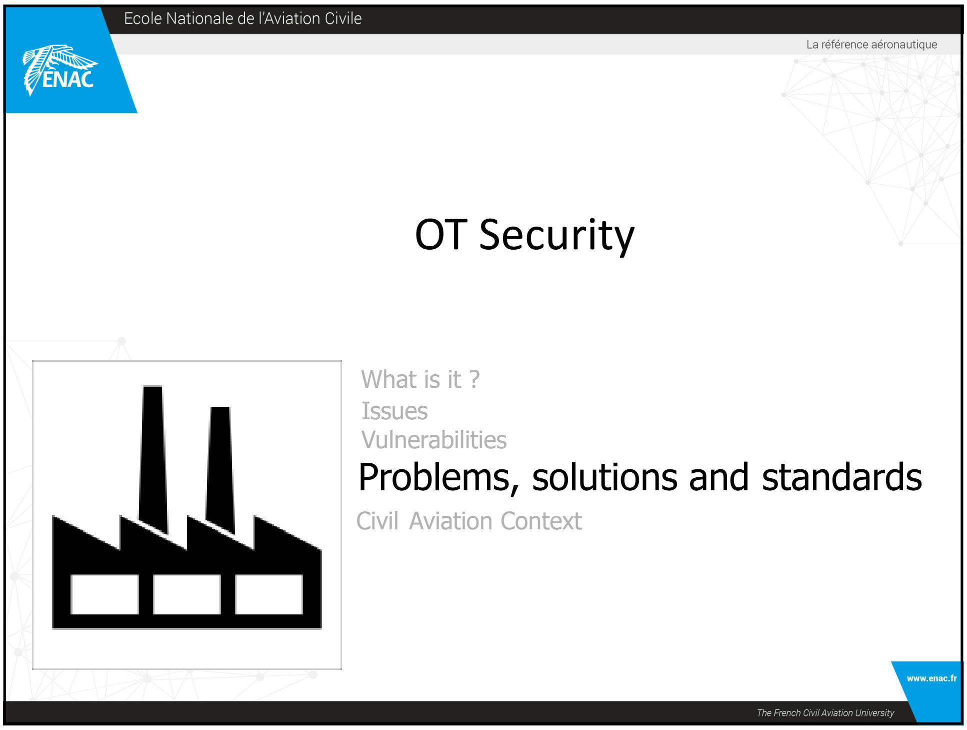
La référence aéronautique

OT systems
Vulnerabilities summary

Industrial systems today make extensive use of information technologies even though they have not been designed to cope with the threats they introduce.

www.enac.fr

The French Civil Aviation University



Ecole Nationale de l'Aviation Civile

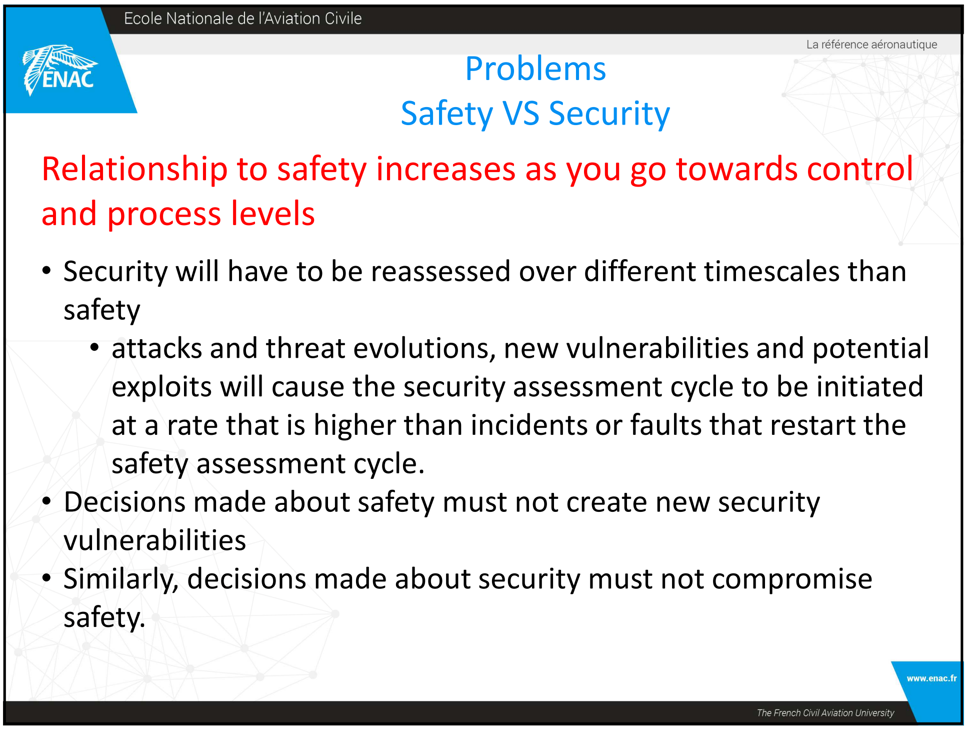
La référence aéronautique

OT Security

What is it ?
Issues
Vulnerabilities
Problems, solutions and standards
Civil Aviation Context

www.enac.fr

The French Civil Aviation University



Ecole Nationale de l'Aviation Civile

La référence aéronautique

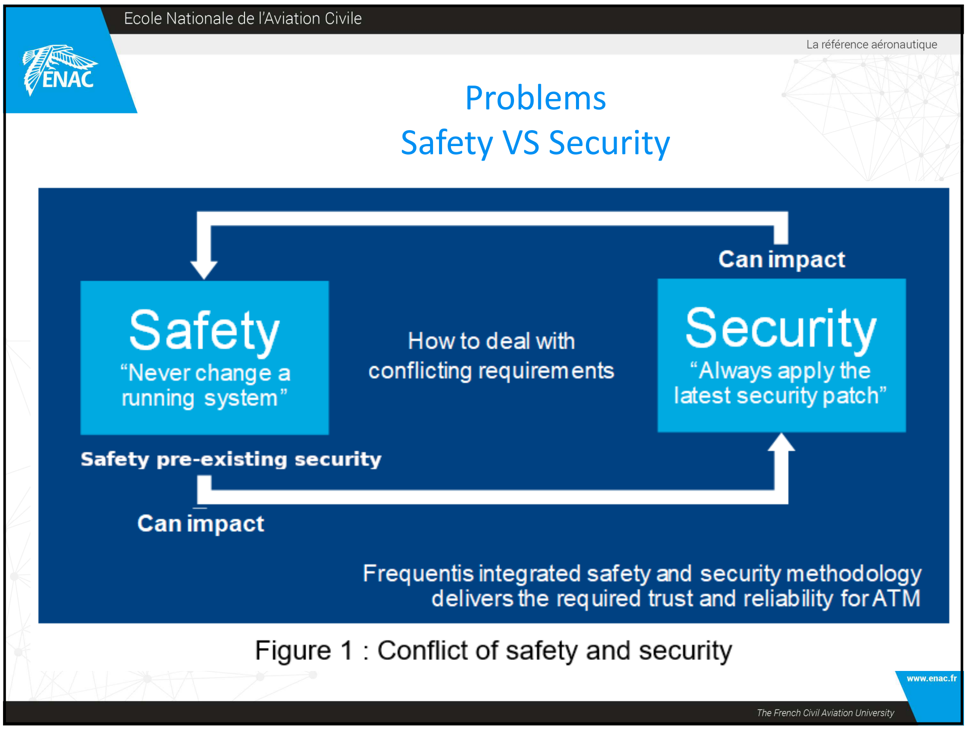
Problems
Safety VS Security

Relationship to safety increases as you go towards control and process levels

- Security will have to be reassessed over different timescales than safety
  - attacks and threat evolutions, new vulnerabilities and potential exploits will cause the security assessment cycle to be initiated at a rate that is higher than incidents or faults that restart the safety assessment cycle.
- Decisions made about safety must not create new security vulnerabilities
- Similarly, decisions made about security must not compromise safety.

www.enac.fr

The French Civil Aviation University



Ecole Nationale de l'Aviation Civile

La référence aéronautique

Problems
Safety VS Security

Can impact

Safety
"Never change a running system"

How to deal with conflicting requirements

Security
"Always apply the latest security patch"

Safety pre-existing security

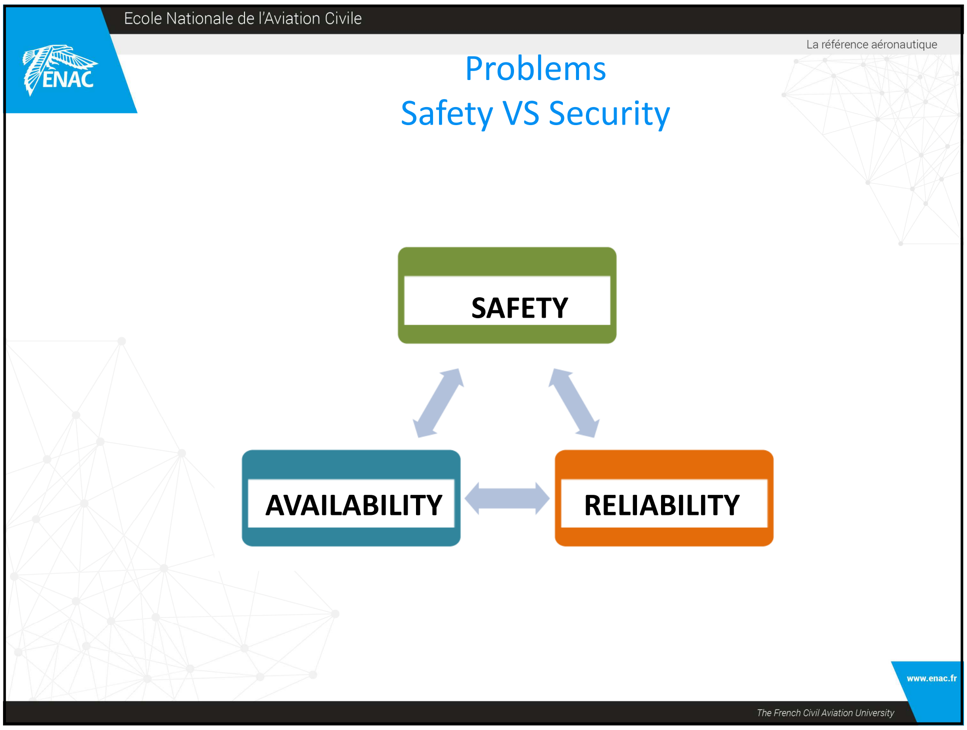
Can impact

Frequentis integrated safety and security methodology delivers the required trust and reliability for ATM

Figure 1 : Conflict of safety and security

www.enac.fr

The French Civil Aviation University



Ecole Nationale de l'Aviation Civile

La référence aéronautique

Problems
Safety VS Security

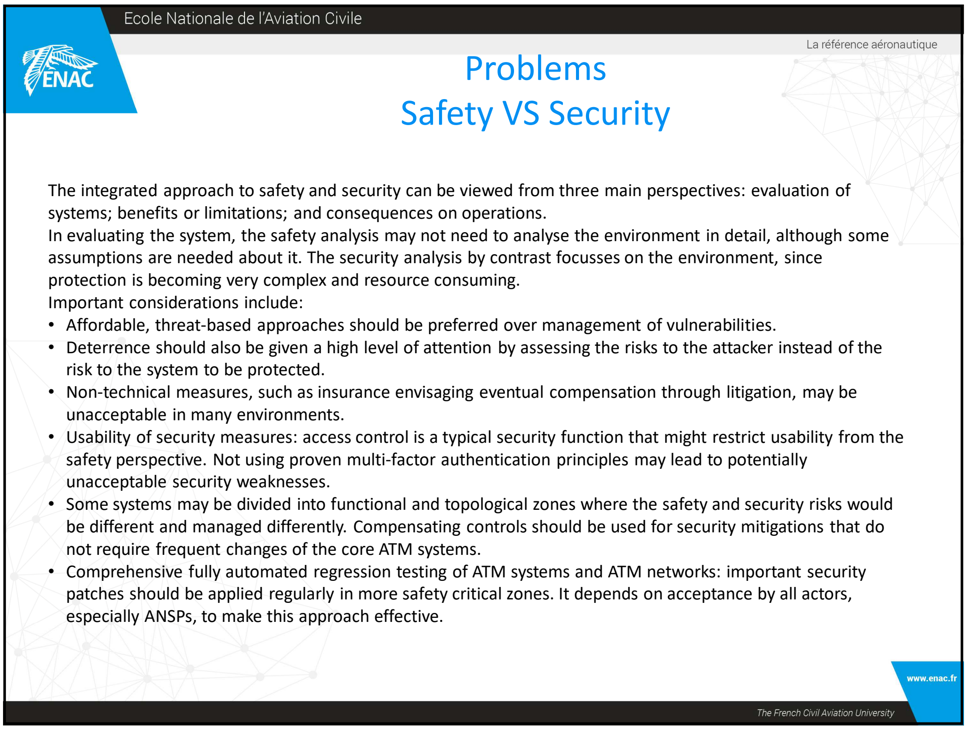
SAFETY

AVAILABILITY

RELIABILITY

www.enac.fr

The French Civil Aviation University



Ecole Nationale de l'Aviation Civile

La référence aéronautique

Problems
Safety VS Security

The integrated approach to safety and security can be viewed from three main perspectives: evaluation of systems; benefits or limitations; and consequences on operations.

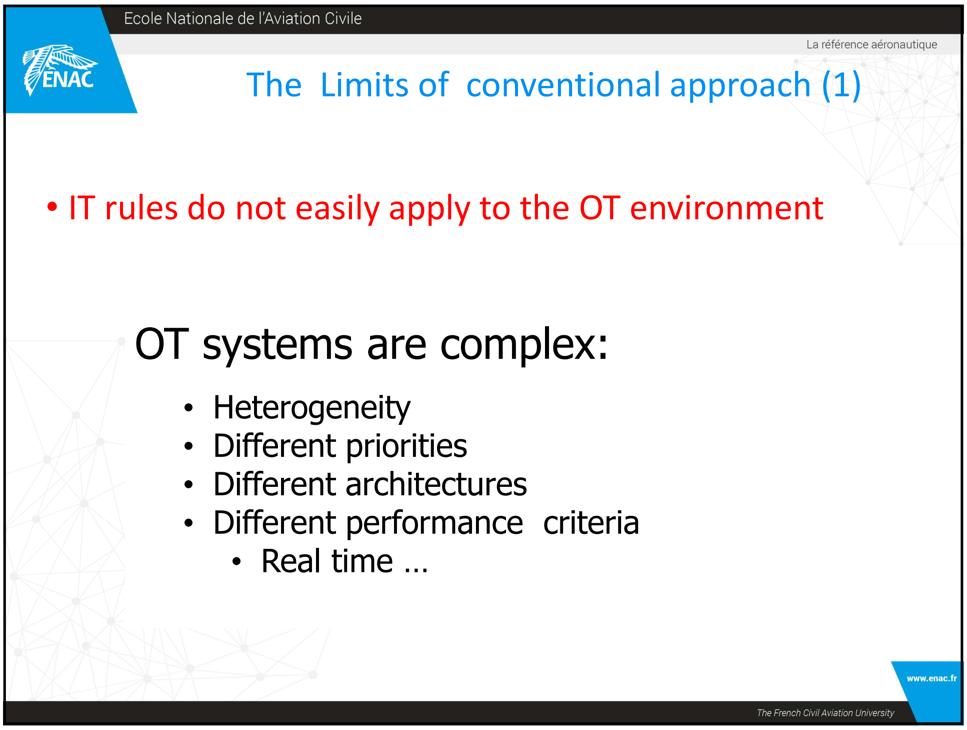
In evaluating the system, the safety analysis may not need to analyse the environment in detail, although some assumptions are needed about it. The security analysis by contrast focusses on the environment, since protection is becoming very complex and resource consuming.

Important considerations include:

- Affordable, threat-based approaches should be preferred over management of vulnerabilities.
- Deterrence should also be given a high level of attention by assessing the risks to the attacker instead of the risk to the system to be protected.
- Non-technical measures, such as insurance envisaging eventual compensation through litigation, may be unacceptable in many environments.
- Usability of security measures: access control is a typical security function that might restrict usability from the safety perspective. Not using proven multi-factor authentication principles may lead to potentially unacceptable security weaknesses.
- Some systems may be divided into functional and topological zones where the safety and security risks would be different and managed differently. Compensating controls should be used for security mitigations that do not require frequent changes of the core ATM systems.
- Comprehensive fully automated regression testing of ATM systems and ATM networks: important security patches should be applied regularly in more safety critical zones. It depends on acceptance by all actors, especially ANSPs, to make this approach effective.

www.enac.fr

The French Civil Aviation University



Ecole Nationale de l'Aviation Civile

La référence aéronautique

The Limits of conventional approach (1)

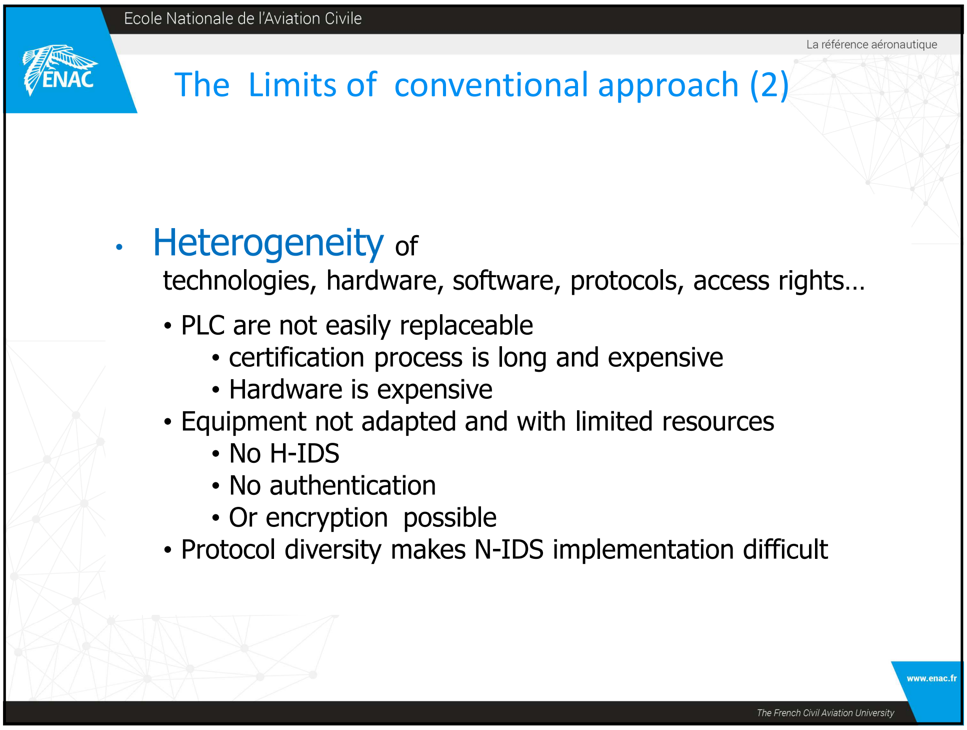
- IT rules do not easily apply to the OT environment

OT systems are complex:

- Heterogeneity
- Different priorities
- Different architectures
- Different performance criteria
  - Real time …

www.enac.fr

The French Civil Aviation University



Ecole Nationale de l'Aviation Civile

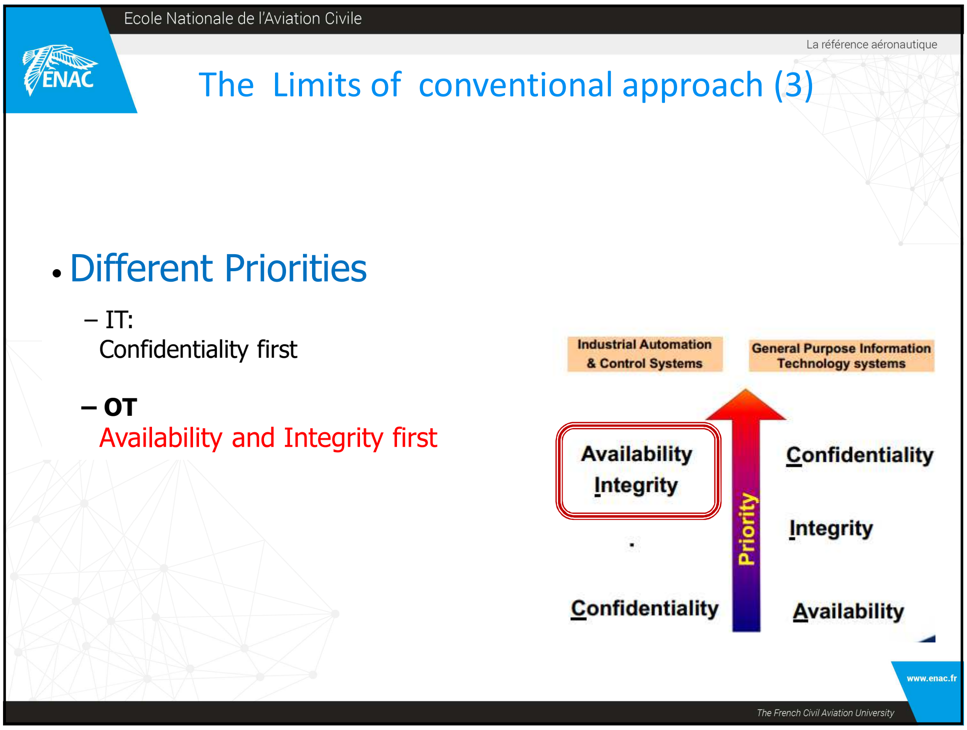
La référence aéronautique

The Limits of conventional approach (2)

- Heterogeneity of technologies, hardware, software, protocols, access rights…
  - PLC are not easily replaceable
    - certification process is long and expensive
    - Hardware is expensive
  - Equipment not adapted and with limited resources
    - No H-IDS
    - No authentication
    - Or encryption possible
  - Protocol diversity makes N-IDS implementation difficult

www.enac.fr

The French Civil Aviation University



Ecole Nationale de l'Aviation Civile

La référence aéronautique

The Limits of conventional approach (3)

- Different Priorities
  - – IT:
    Confidentiality first
  - **– OT**
    Availability and Integrity first

Industrial Automation & Control Systems

General Purpose Information Technology systems

Availability
Integrity

Confidentiality

Priority

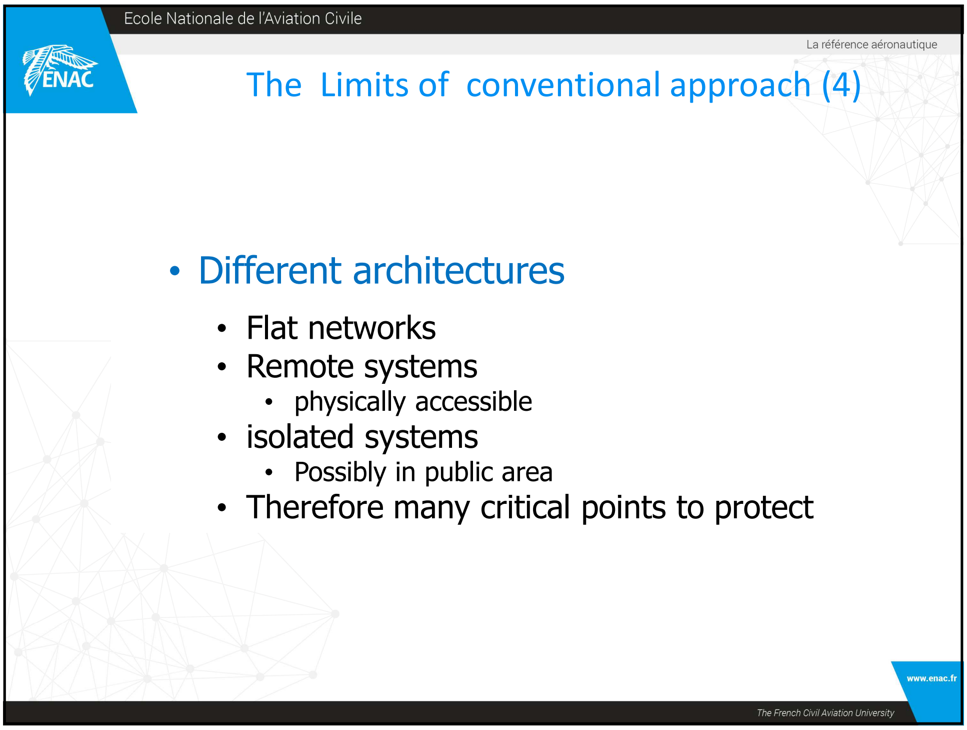
Confidentiality

Integrity

Availability

www.enac.fr

The French Civil Aviation University



Ecole Nationale de l'Aviation Civile

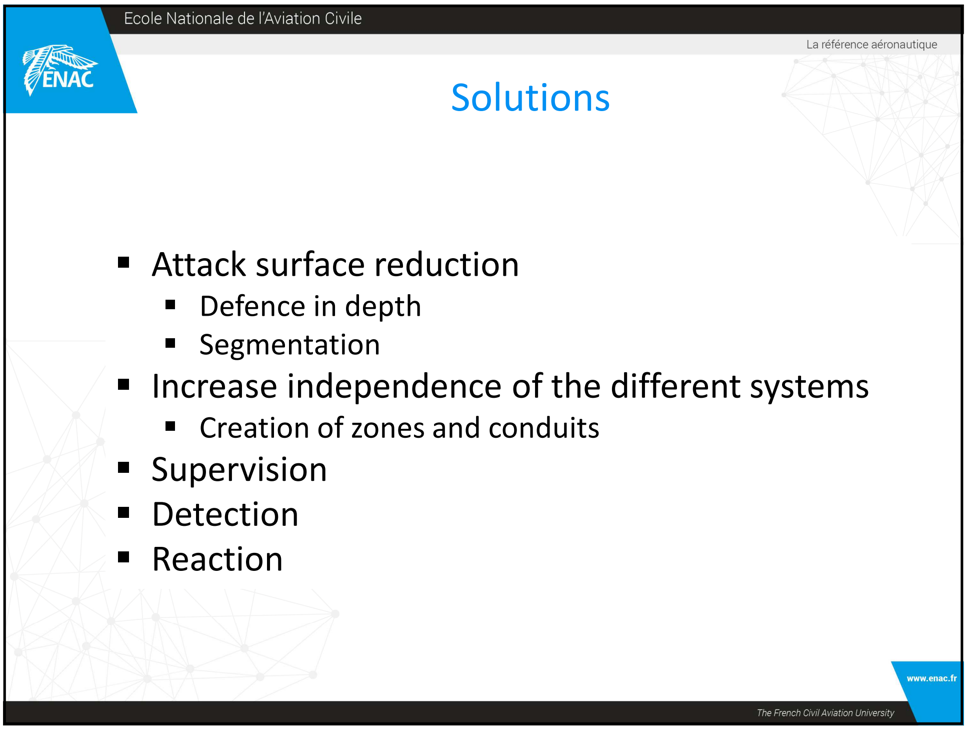
La référence aéronautique

The Limits of conventional approach (4)

- Different architectures
  - Flat networks
  - Remote systems
    - physically accessible
  - isolated systems
    - Possibly in public area
  - Therefore many critical points to protect

www.enac.fr

The French Civil Aviation University



Ecole Nationale de l'Aviation Civile

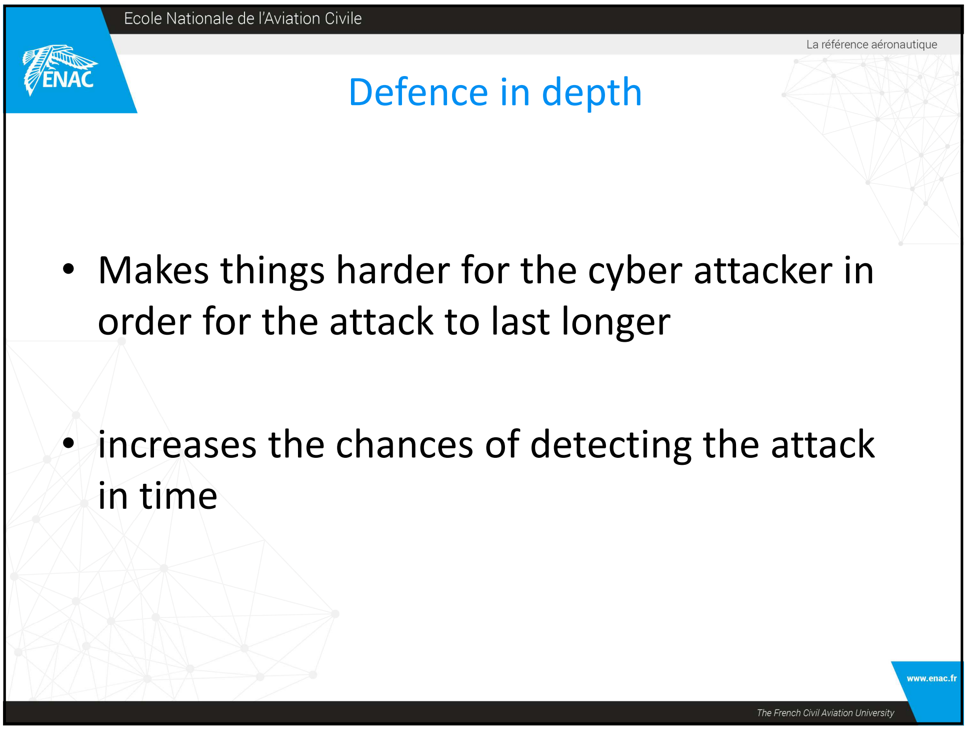
La référence aéronautique

Solutions

- Attack surface reduction
  - Defence in depth
  - Segmentation
- Increase independence of the different systems
  - Creation of zones and conduits
- Supervision
- Detection
- Reaction

www.enac.fr

The French Civil Aviation University



Ecole Nationale de l'Aviation Civile

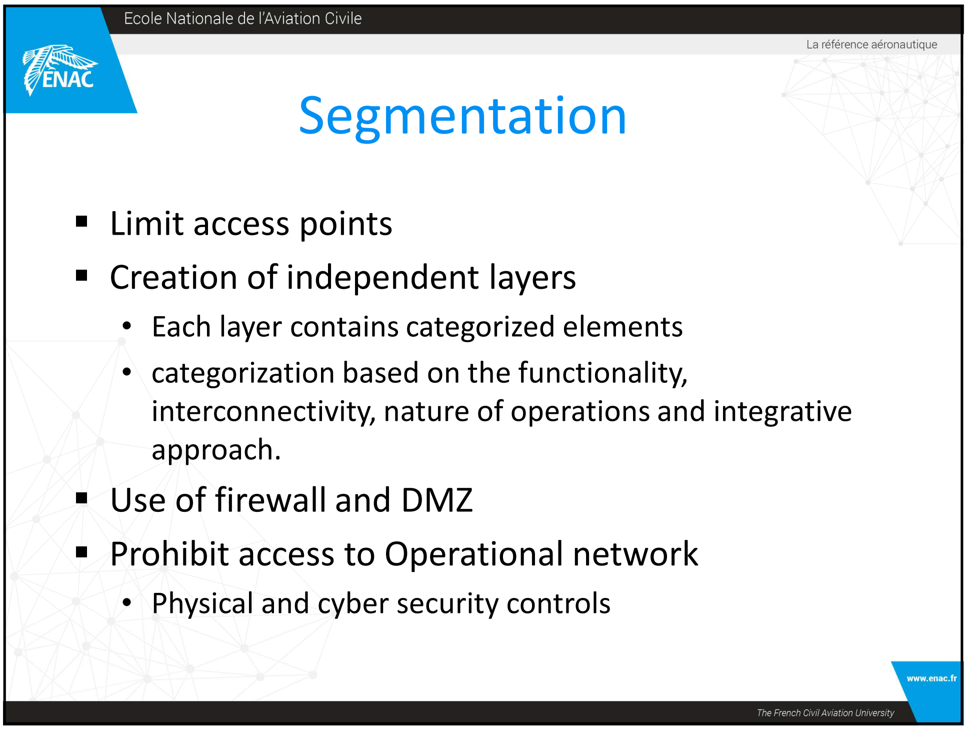
La référence aéronautique

Defence in depth

- Makes things harder for the cyber attacker in order for the attack to last longer
- increases the chances of detecting the attack in time

www.enac.fr

The French Civil Aviation University



Ecole Nationale de l'Aviation Civile

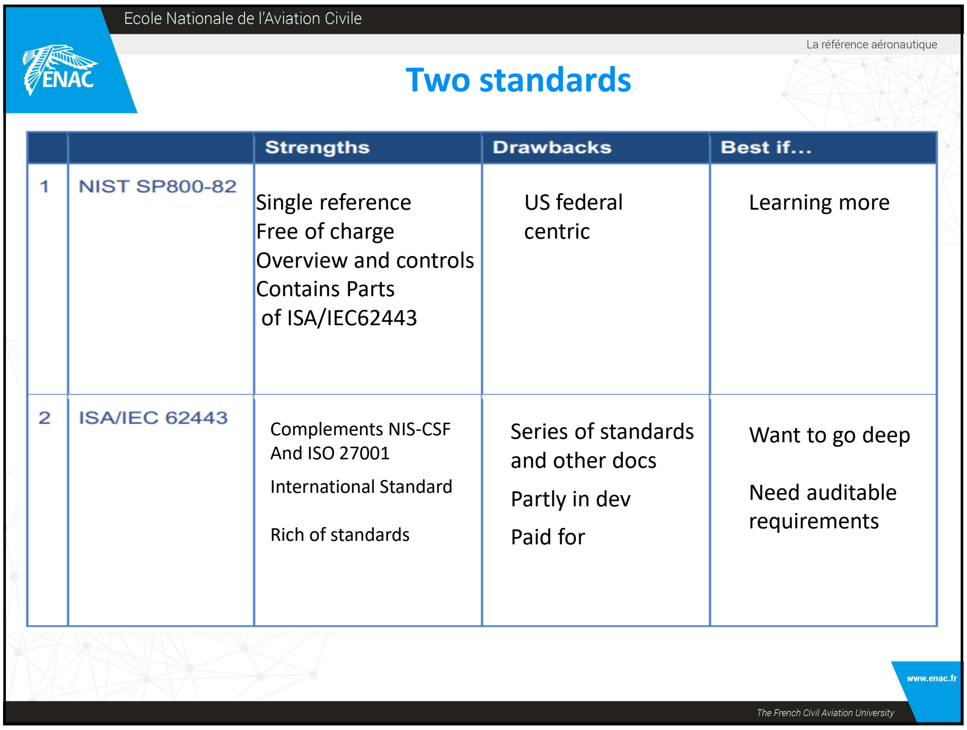
La référence aéronautique

Segmentation

- Limit access points
- Creation of independent layers
    - Each layer contains categorized elements
    - categorization based on the functionality, interconnectivity, nature of operations and integrative approach.
- Use of firewall and DMZ
- Prohibit access to Operational network
    - Physical and cyber security controls

www.enac.fr

The French Civil Aviation University



Ecole Nationale de l'Aviation Civile

La référence aéronautique

Two standards

		Strengths	Drawbacks	Best if…
1	NIST SP800-82	Single reference Free of charge Overview and controls Contains Parts of ISA/IEC62443	US federal centric	Learning more
2	ISA/IEC 62443	Complements NIS-CSF And ISO 27001 International Standard Rich of standards	Series of standards and other docs Partly in dev Paid for	Want to go deep Need auditable requirements

www.enac.fr

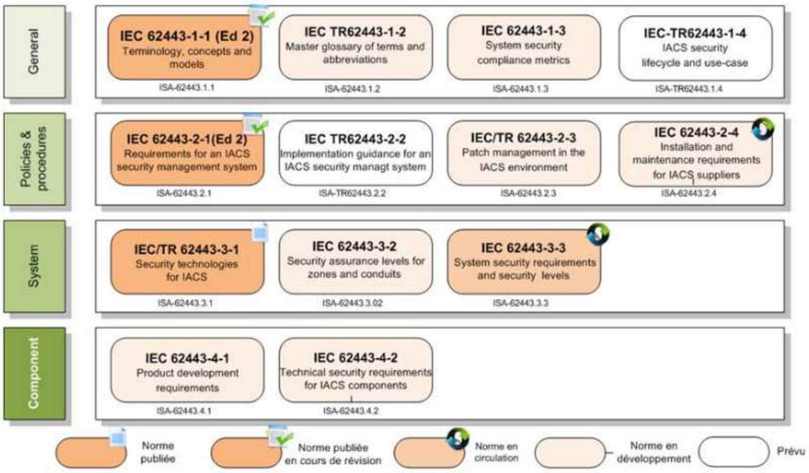
The French Civil Aviation University

ISA/IEC-62443 Standard

- ISA/IEC-62443: series of standards, technical reports and information that assist in the implementation of electronically secure Industrial Automation and Control Systems (IACS).

- These guidelines apply to end-users (i.e. asset owner), system integrators, security practitioners, and control systems manufacturers responsible for manufacturing, designing, implementing, or managing industrial automation and control systems.

IEC 62443 – Documents structure



General	**IEC 62443-1-1 (Ed 2)** Terminology, concepts and models ISA-62443.1.1	**IEC TR62443-1-2** Master glossary of terms and abbreviations ISA-62443.1.2	**IEC 62443-1-3** System security compliance metrics ISA-62443.1.3	**IEC-TR62443-1-4** IACS security lifecycle and use-case ISA-TR62443.1.4
Policies & procedures	**IEC 62443-2-1(Ed 2)** Requirements for an IACS security management system ISA-62443.2.1	**IEC TR62443-2-2** Implementation guidance for an IACS security managt system ISA-TR62443.2.2	**IEC/TR 62443-2-3** Patch management in the IACS environment ISA-62443.2.3	**IEC 62443-2-4** Installation and maintenance requirements for IACS suppliers ISA-62443.2.4
System	**IEC/TR 62443-3-1** Security technologies for IACS ISA-62443.3.1	**IEC 62443-3-2** Security assurance levels for zones and conduits ISA-62443.3.02	**IEC 62443-3-3** System security requirements and security levels ISA-62443.3.3	
Component	**IEC 62443-4-1** Product development requirements ISA-62443.4.1	**IEC 62443-4-2** Technical security requirements for IACS components ISA-62443.4.2		

Norme publiée

Norme publiée en cours de révision

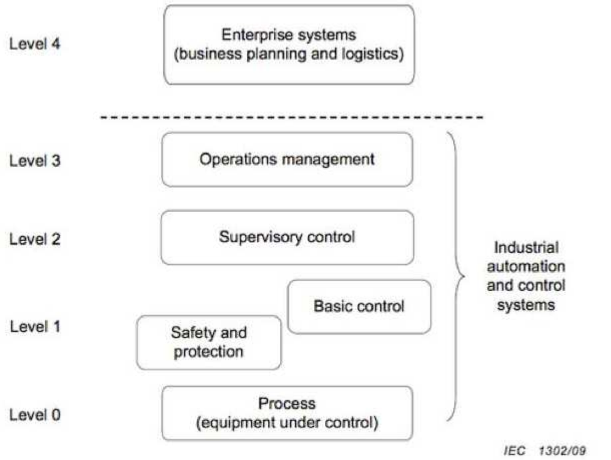
Norme en circulation

Norme en développement

Prévu

IEC 62443 Industrial Control System Reference model

5 Layers SEGREGATION


Level 4
Enterprise systems (business planning and logistics)
Level 3
Operations management
Level 2
Supervisory control
Level 1
Basic control
Safety and protection
Level 0
Process (equipment under control)
Industrial automation and control systems
IEC 1302/09

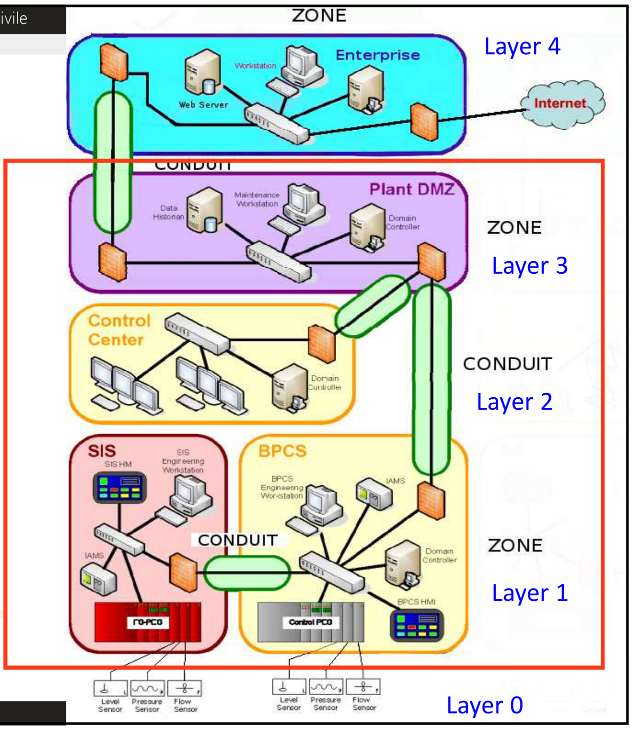
- Chaque couche possède des entités système spécifiques.
  - La plupart d'entre eux seront intégrés par l'environnement en réseau, mais certains d'entre eux peuvent être encore autonome.

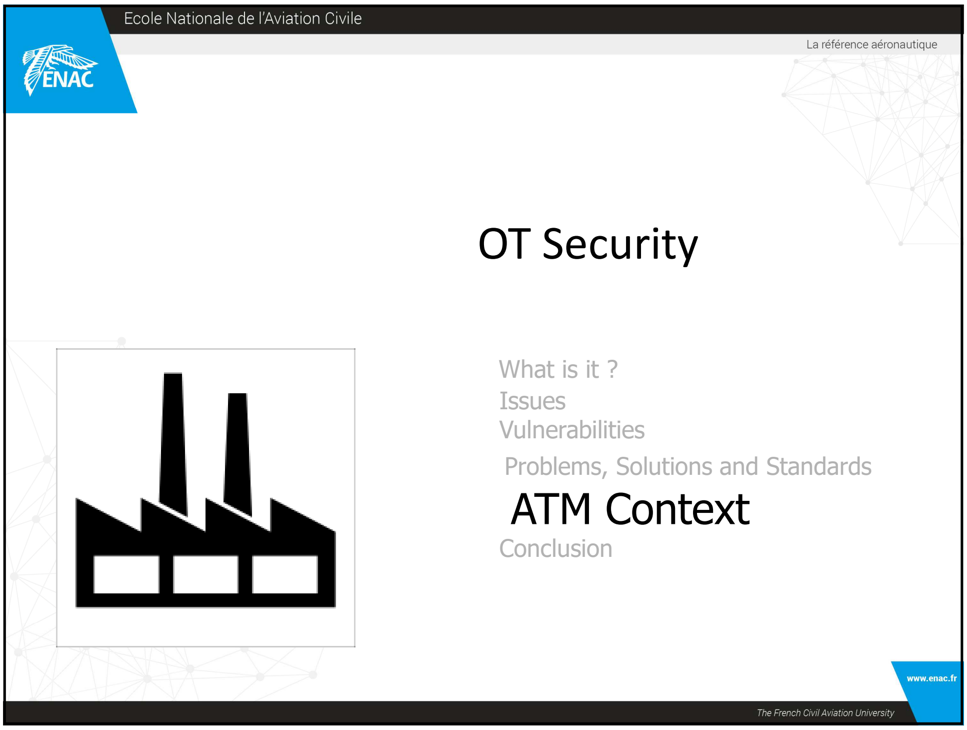
Defence-in-Depth / Layer Segregation

IEC 62443

- ZONES: groups of logical or physical assets that share the same security requirements
- CONDUIT: each communication between zones is carried out by a conduit

ICS ENVIRONMENT





Ecole Nationale de l'Aviation Civile

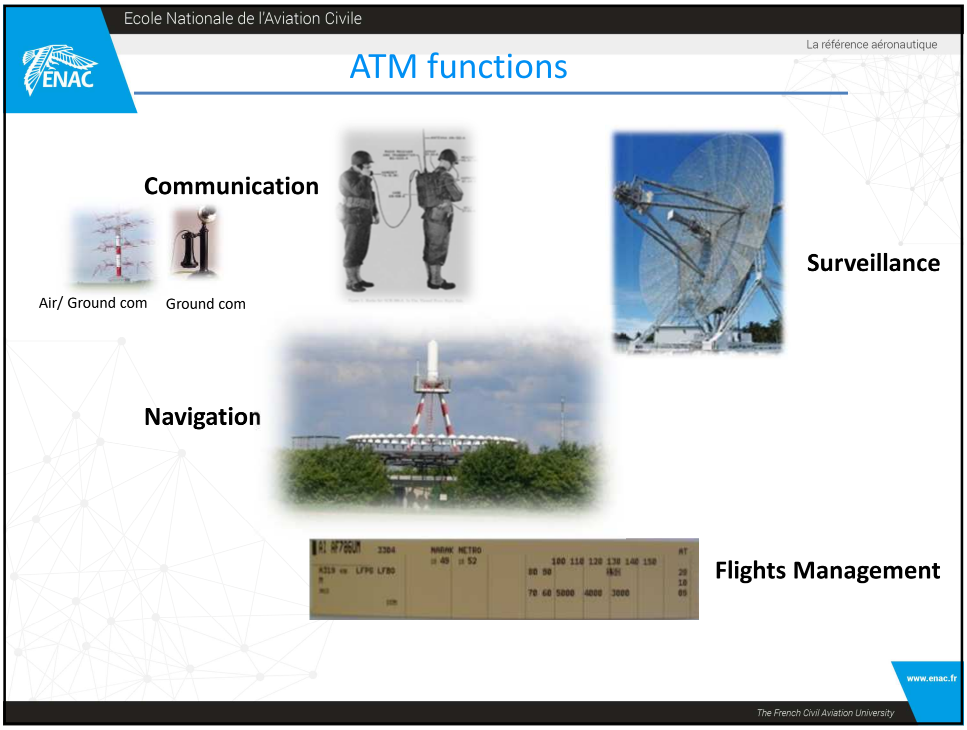
La référence aéronautique

OT Security

What is it ?
Issues
Vulnerabilities
Problems, Solutions and Standards
ATM Context
Conclusion

www.enac.fr

The French Civil Aviation University



Ecole Nationale de l'Aviation Civile

La référence aéronautique

ATM functions

Communication

Air/ Ground com

Ground com

Surveillance

Navigation

Flights Management

www.enac.fr

The French Civil Aviation University

ATM environment is OT

- Strong real time constraints
  - Availability and integrity of Air Trafic Control
- Strong dependability requirements
  - systems must run properly
- Heterogeneity:
  - Overlays of successive technological waves
- Components can be isolated and/or remote
  - Radio navigation ground stations, approach lightning ….
- But more and more connected
  - Airliners, airport service provider, Meteorological service…
- Protocols less and less proprietary
  - Ethernet, Internet protocol …

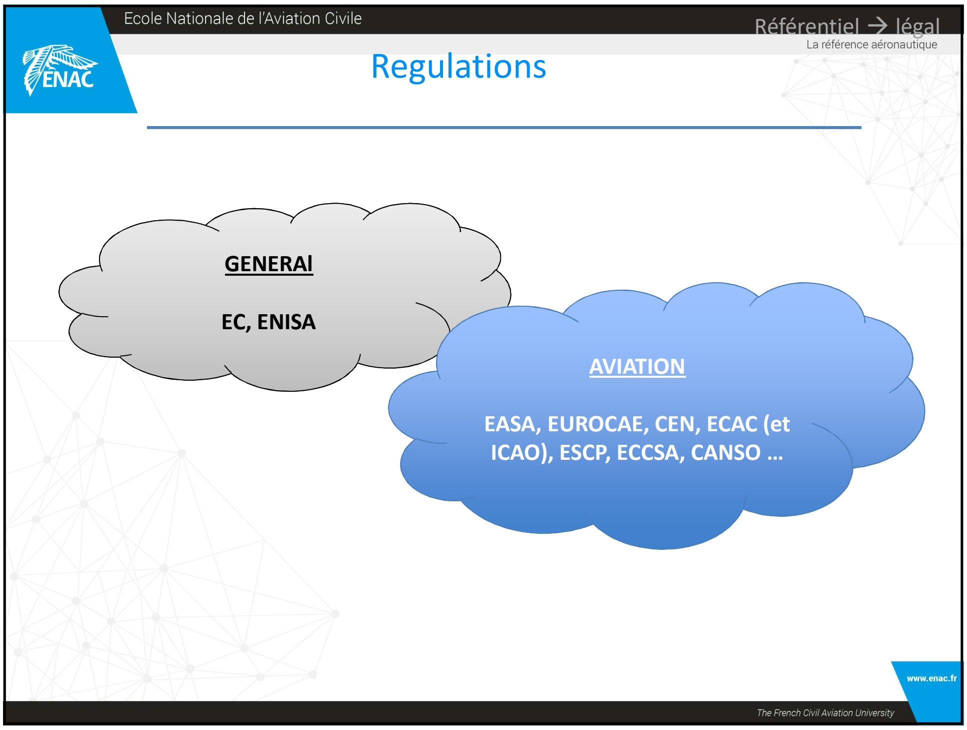
Connections with OT

***Initially,** ICS had little resemblance to IT systems in that ICS were **isolated systems running proprietary control protocols using specialized hardware and software**.*

*Widely available, low-cost **Internet Protocol (IP) devices are now replacing proprietary solutions**, [..].*

*As ICS […] are **being designed** and implemented using **industry standard** computers, operating systems (OS) and network protocols, they are **starting to resemble IT systems**.*

NIST SP 800-82 « Guide to Industrial Control Systems (ICS) Security »



Ecole Nationale de l'Aviation Civile

Référentiel → légal

La référence aéronautique

Regulations

GENERAl

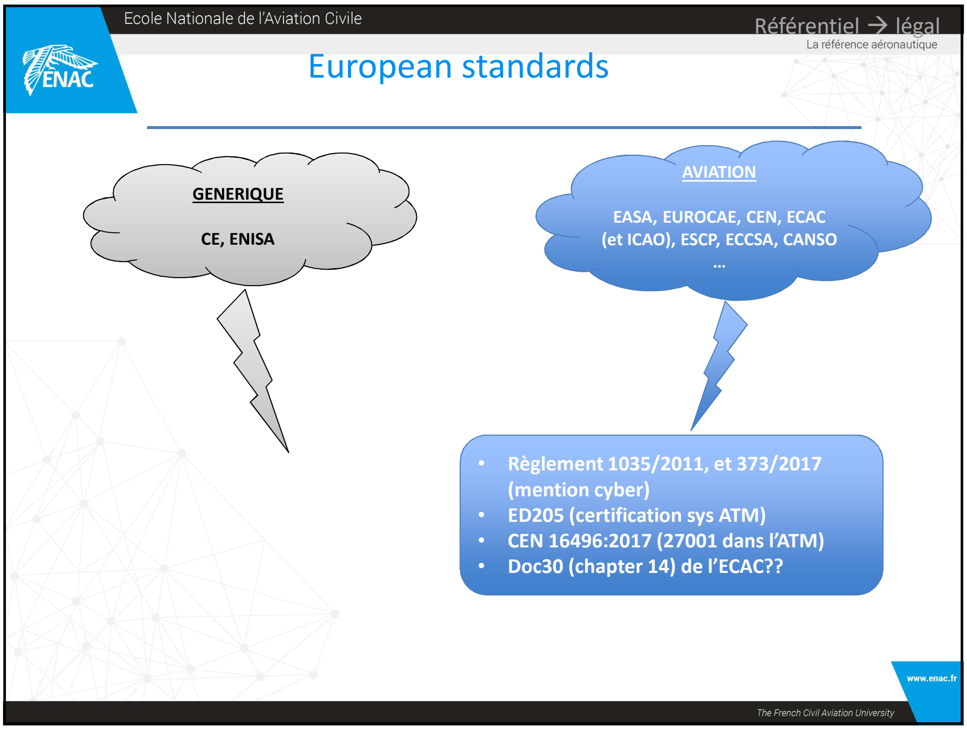
EC, ENISA

AVIATION

EASA, EUROCAE, CEN, ECAC (et ICAO), ESCP, ECCSA, CANSO …

www.enac.fr

The French Civil Aviation University



Ecole Nationale de l'Aviation Civile

Référentiel → légal

La référence aéronautique

European standards

GENERIQUE

CE, ENISA

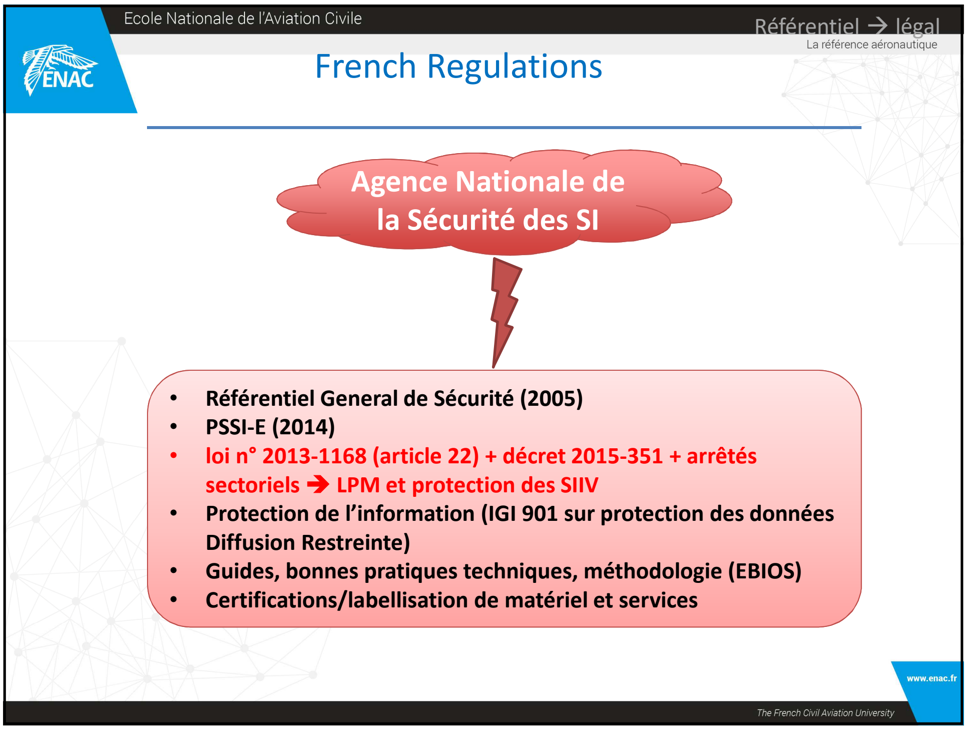
AVIATION

EASA, EUROCAE, CEN, ECAC (et ICAO), ESCP, ECCSA, CANSO …

- **Règlement 1035/2011, et 373/2017 (mention cyber)**
- **ED205 (certification sys ATM)**
- **CEN 16496:2017 (27001 dans l'ATM)**
- **Doc30 (chapter 14) de l'ECAC??**

www.enac.fr

The French Civil Aviation University



Ecole Nationale de l'Aviation Civile

Référentiel → légal

La référence aéronautique

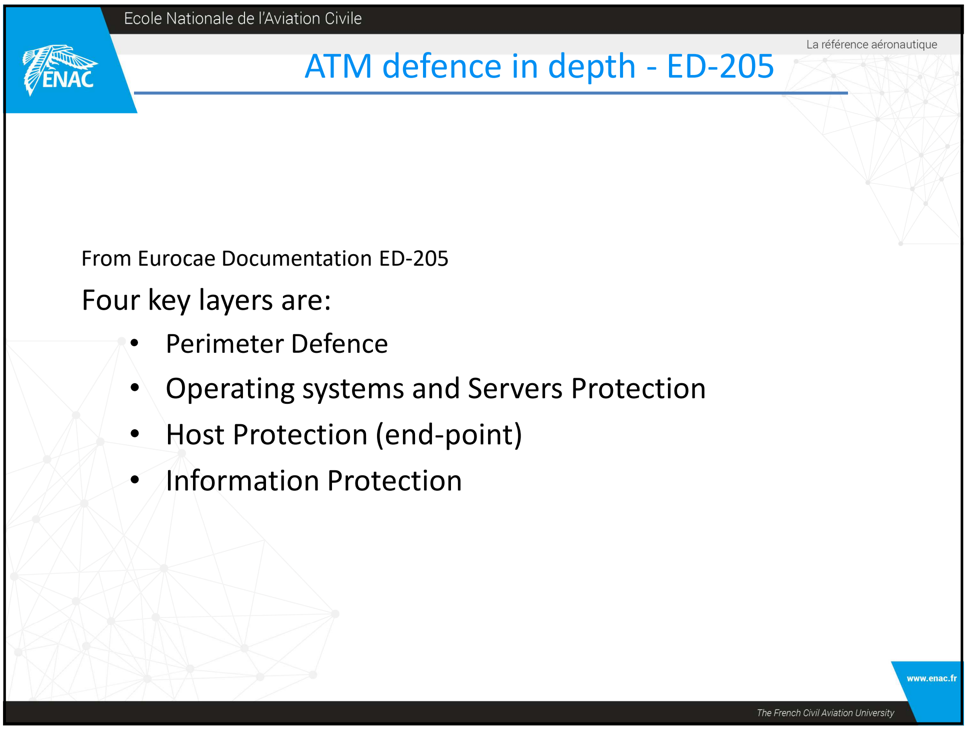
French Regulations

Agence Nationale de la Sécurité des SI

- Référentiel General de Sécurité (2005)
- PSSI-E (2014)
- loi n° 2013-1168 (article 22) + décret 2015-351 + arrêtés sectoriels ➔ LPM et protection des SIIV
- Protection de l'information (IGI 901 sur protection des données Diffusion Restreinte)
- Guides, bonnes pratiques techniques, méthodologie (EBIOS)
- Certifications/labellisation de matériel et services

www.enac.fr

The French Civil Aviation University



Ecole Nationale de l'Aviation Civile

La référence aéronautique

ATM defence in depth - ED-205

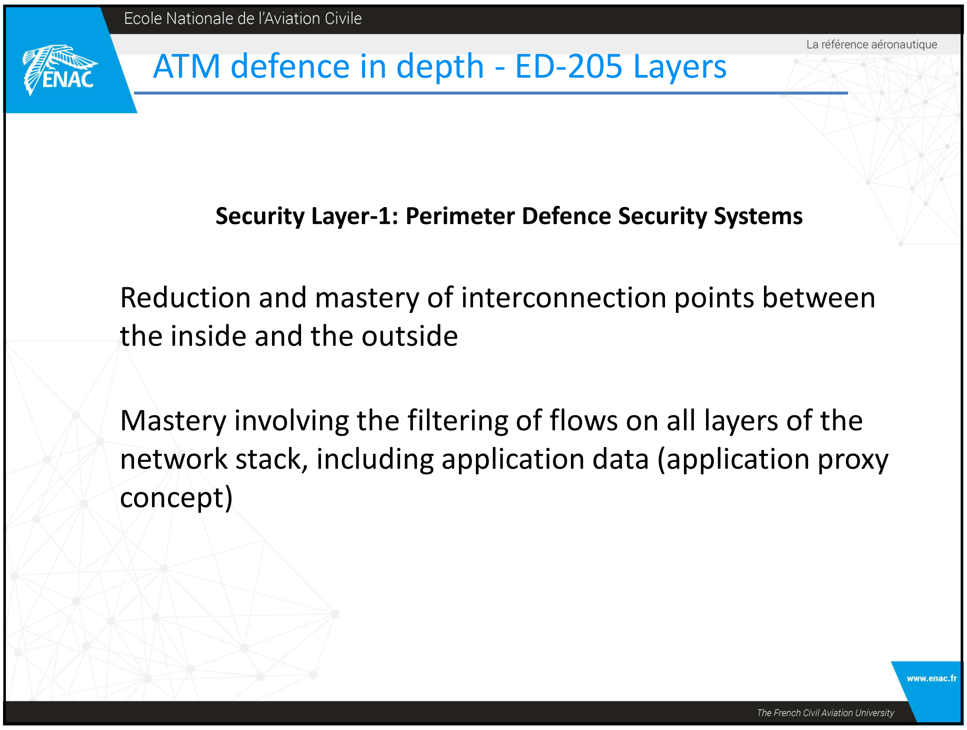
From Eurocae Documentation ED-205

Four key layers are:

- Perimeter Defence
- Operating systems and Servers Protection
- Host Protection (end-point)
- Information Protection

www.enac.fr

The French Civil Aviation University



Ecole Nationale de l'Aviation Civile

La référence aéronautique

ATM defence in depth - ED-205 Layers

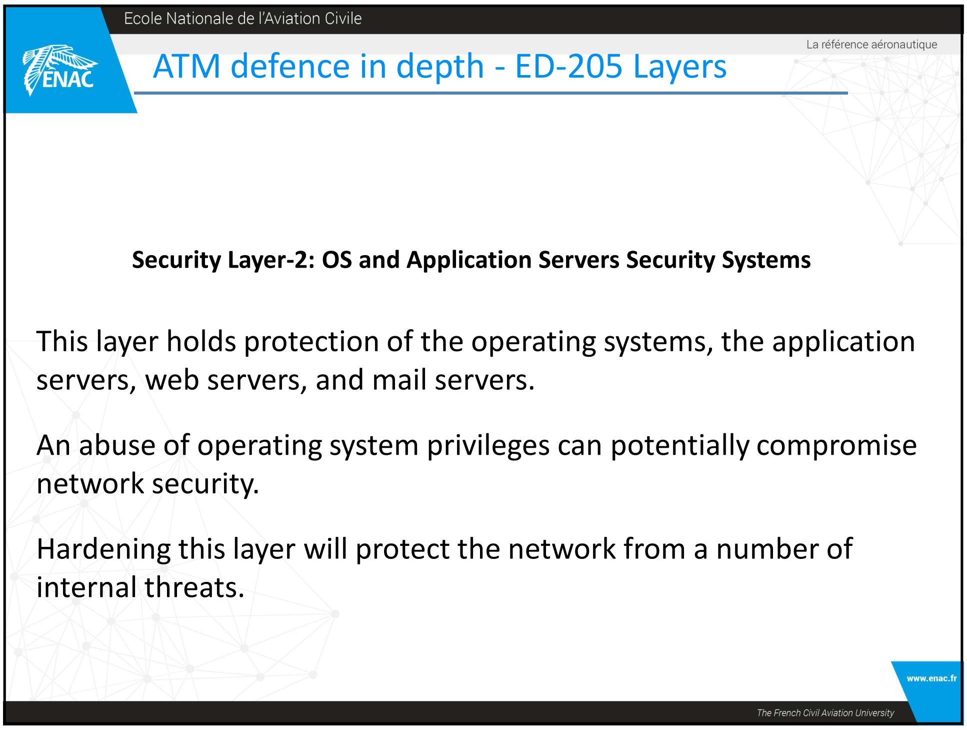
Security Layer-1: Perimeter Defence Security Systems

Reduction and mastery of interconnection points between the inside and the outside

Mastery involving the filtering of flows on all layers of the network stack, including application data (application proxy concept)

www.enac.fr

The French Civil Aviation University



Ecole Nationale de l'Aviation Civile

La référence aéronautique

ATM defence in depth - ED-205 Layers

Security Layer-2: OS and Application Servers Security Systems

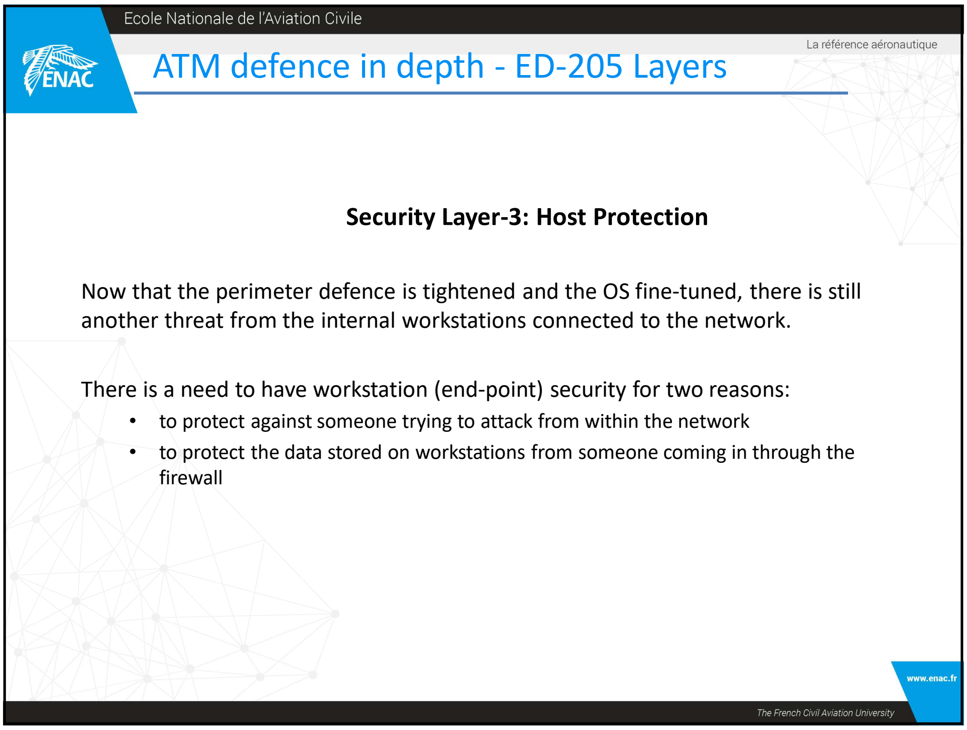
This layer holds protection of the operating systems, the application servers, web servers, and mail servers.

An abuse of operating system privileges can potentially compromise network security.

Hardening this layer will protect the network from a number of internal threats.

www.enac.fr

The French Civil Aviation University



Ecole Nationale de l'Aviation Civile

La référence aéronautique

ATM defence in depth - ED-205 Layers

Security Layer-3: Host Protection

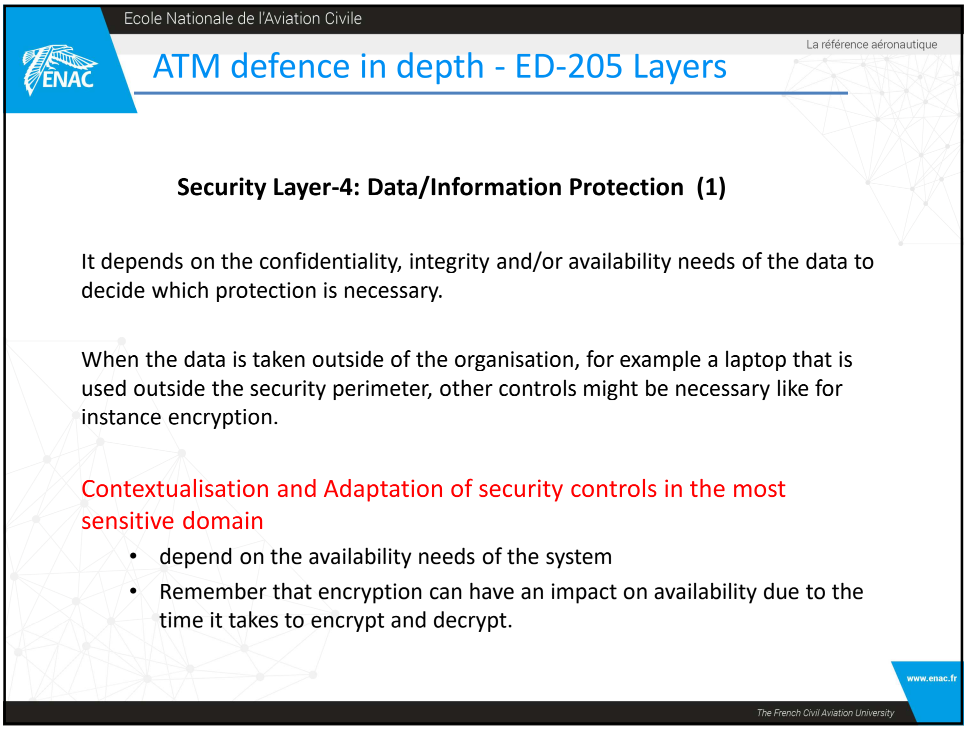
Now that the perimeter defence is tightened and the OS fine-tuned, there is still another threat from the internal workstations connected to the network.

There is a need to have workstation (end-point) security for two reasons:

- to protect against someone trying to attack from within the network
- to protect the data stored on workstations from someone coming in through the firewall

www.enac.fr

The French Civil Aviation University



Ecole Nationale de l'Aviation Civile

La référence aéronautique

ATM defence in depth - ED-205 Layers

Security Layer-4: Data/Information Protection (1)

It depends on the confidentiality, integrity and/or availability needs of the data to decide which protection is necessary.

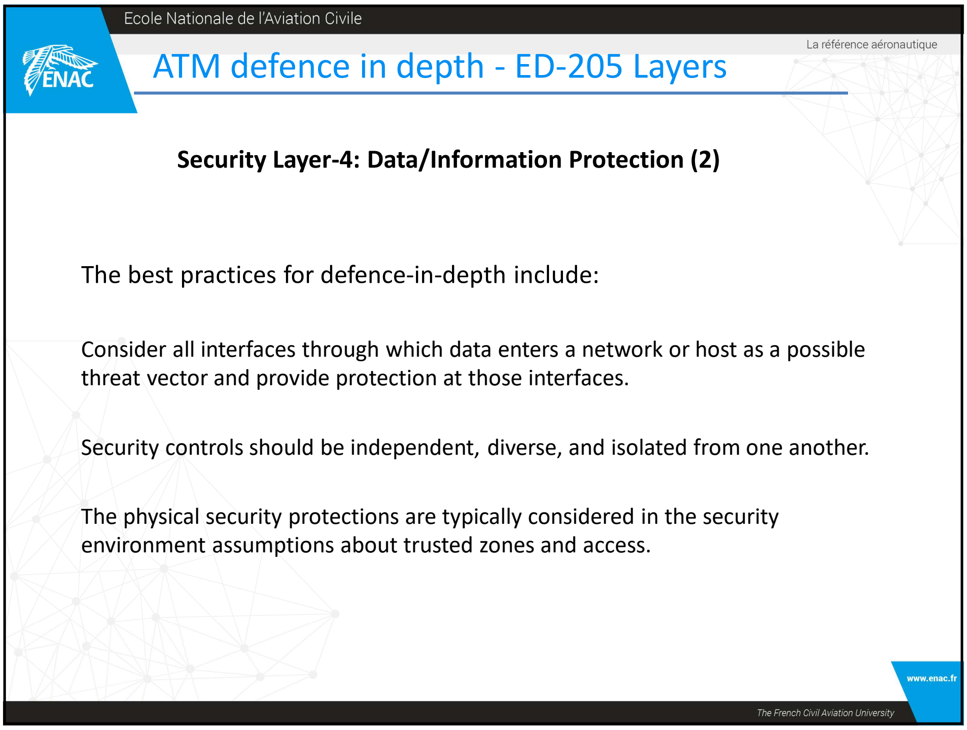
When the data is taken outside of the organisation, for example a laptop that is used outside the security perimeter, other controls might be necessary like for instance encryption.

Contextualisation and Adaptation of security controls in the most sensitive domain

- depend on the availability needs of the system
- Remember that encryption can have an impact on availability due to the time it takes to encrypt and decrypt.

www.enac.fr

The French Civil Aviation University



Ecole Nationale de l'Aviation Civile

La référence aéronautique

ATM defence in depth - ED-205 Layers

Security Layer-4: Data/Information Protection (2)

The best practices for defence-in-depth include:

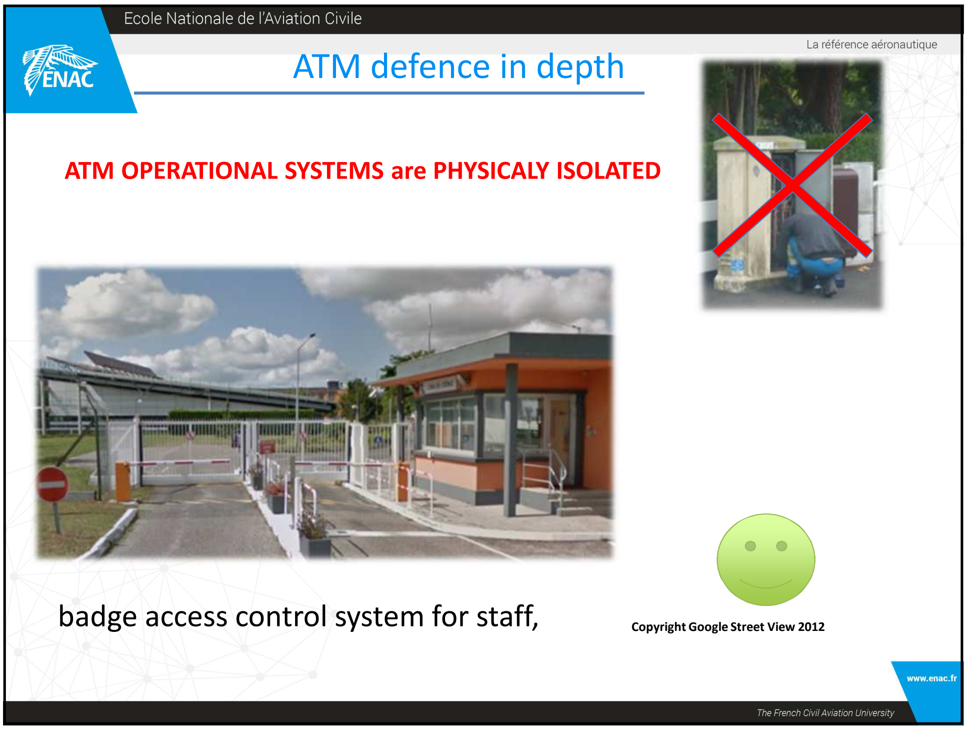
Consider all interfaces through which data enters a network or host as a possible threat vector and provide protection at those interfaces.

Security controls should be independent, diverse, and isolated from one another.

The physical security protections are typically considered in the security environment assumptions about trusted zones and access.

www.enac.fr

The French Civil Aviation University



Ecole Nationale de l'Aviation Civile

La référence aéronautique

ATM defence in depth

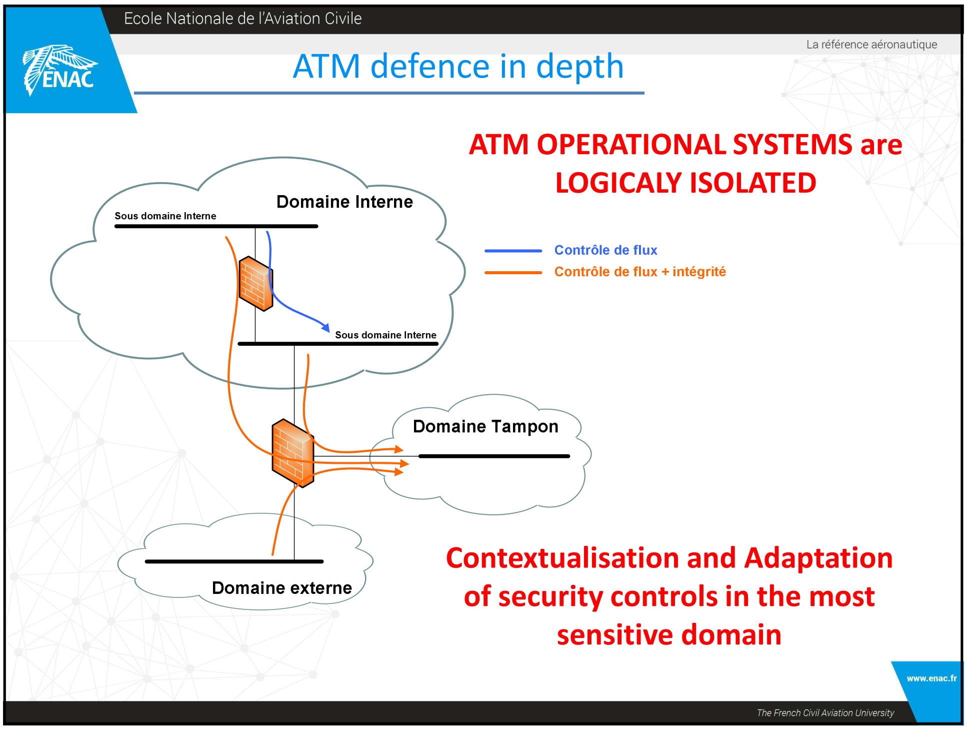
ATM OPERATIONAL SYSTEMS are PHYSICALY ISOLATED

badge access control system for staff,

Copyright Google Street View 2012

www.enac.fr

The French Civil Aviation University



Ecole Nationale de l'Aviation Civile

La référence aéronautique

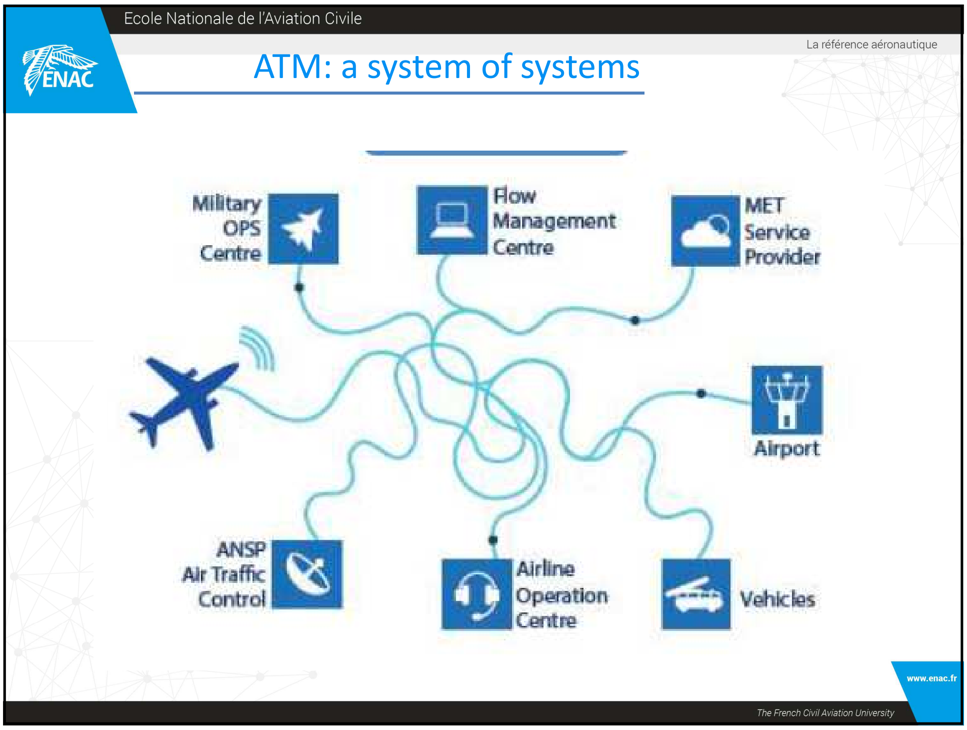
ATM defence in depth

ATM OPERATIONAL SYSTEMS are LOGICALY ISOLATED

Contextualisation and Adaptation of security controls in the most sensitive domain

www.enac.fr

The French Civil Aviation University



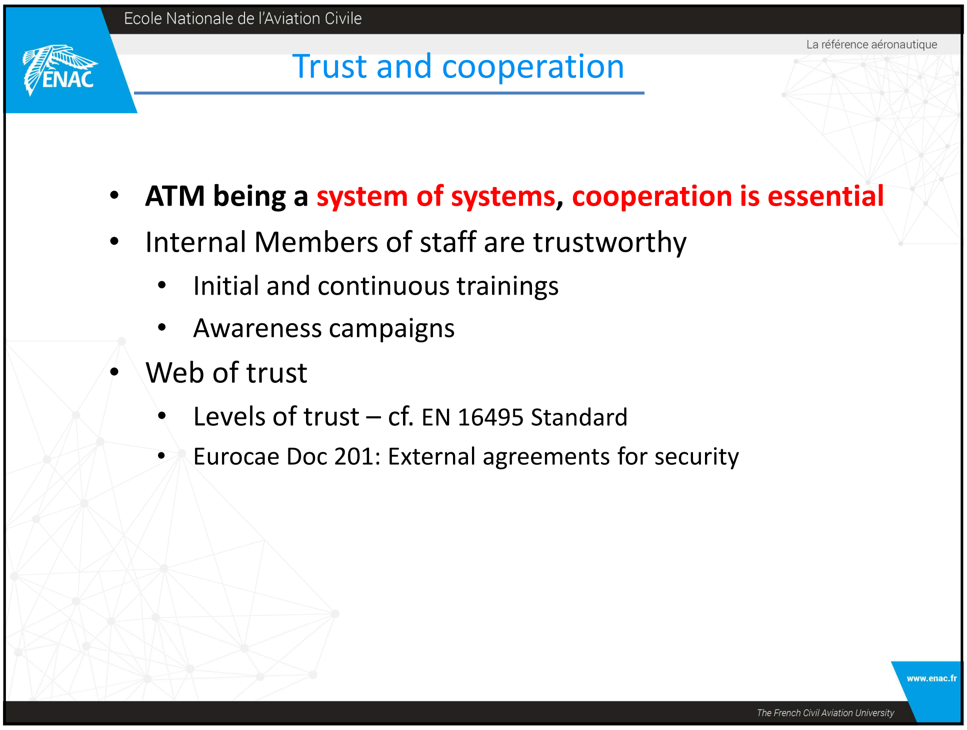
Ecole Nationale de l'Aviation Civile

La référence aéronautique

ATM: a system of systems

www.enac.fr

The French Civil Aviation University



Ecole Nationale de l'Aviation Civile

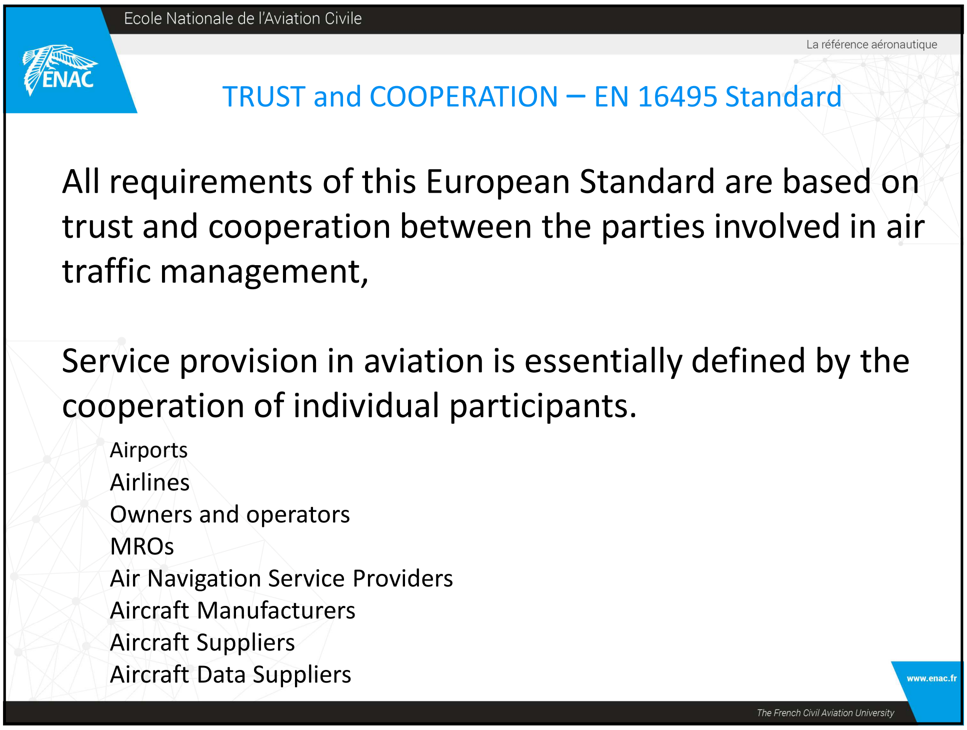
La référence aéronautique

Trust and cooperation

- **ATM being a system of systems, cooperation is essential**
- Internal Members of staff are trustworthy
  - Initial and continuous trainings
  - Awareness campaigns
- Web of trust
  - Levels of trust – cf. EN 16495 Standard
  - Eurocae Doc 201: External agreements for security

www.enac.fr

The French Civil Aviation University



Ecole Nationale de l'Aviation Civile

La référence aéronautique

TRUST and COOPERATION – EN 16495 Standard

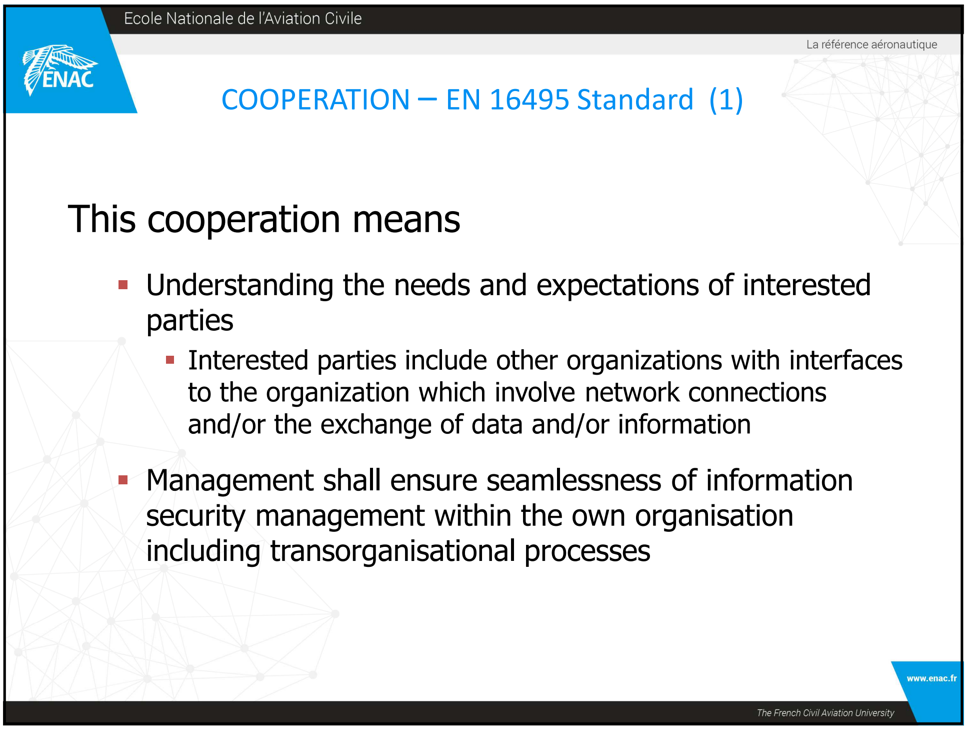
All requirements of this European Standard are based on trust and cooperation between the parties involved in air traffic management,

Service provision in aviation is essentially defined by the cooperation of individual participants.

Airports
Airlines
Owners and operators
MROs
Air Navigation Service Providers
Aircraft Manufacturers
Aircraft Suppliers
Aircraft Data Suppliers

www.enac.fr

The French Civil Aviation University



Ecole Nationale de l'Aviation Civile

La référence aéronautique

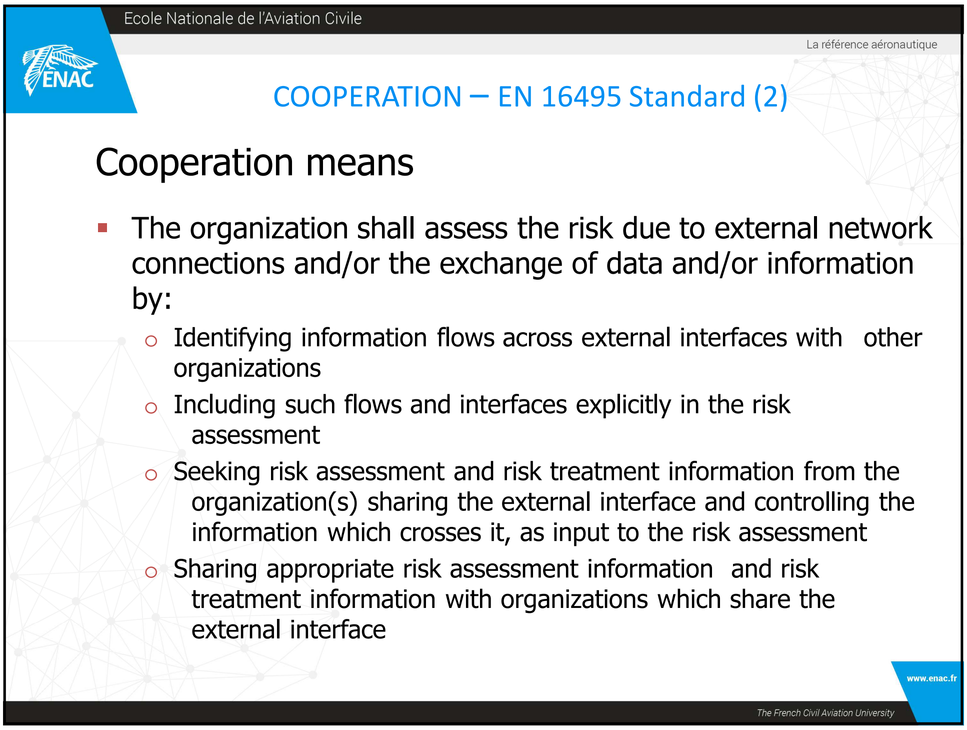
COOPERATION – EN 16495 Standard (1)

This cooperation means

- Understanding the needs and expectations of interested parties
  - Interested parties include other organizations with interfaces to the organization which involve network connections and/or the exchange of data and/or information
- Management shall ensure seamlessness of information security management within the own organisation including transorganisational processes

www.enac.fr

The French Civil Aviation University



Ecole Nationale de l'Aviation Civile

La référence aéronautique

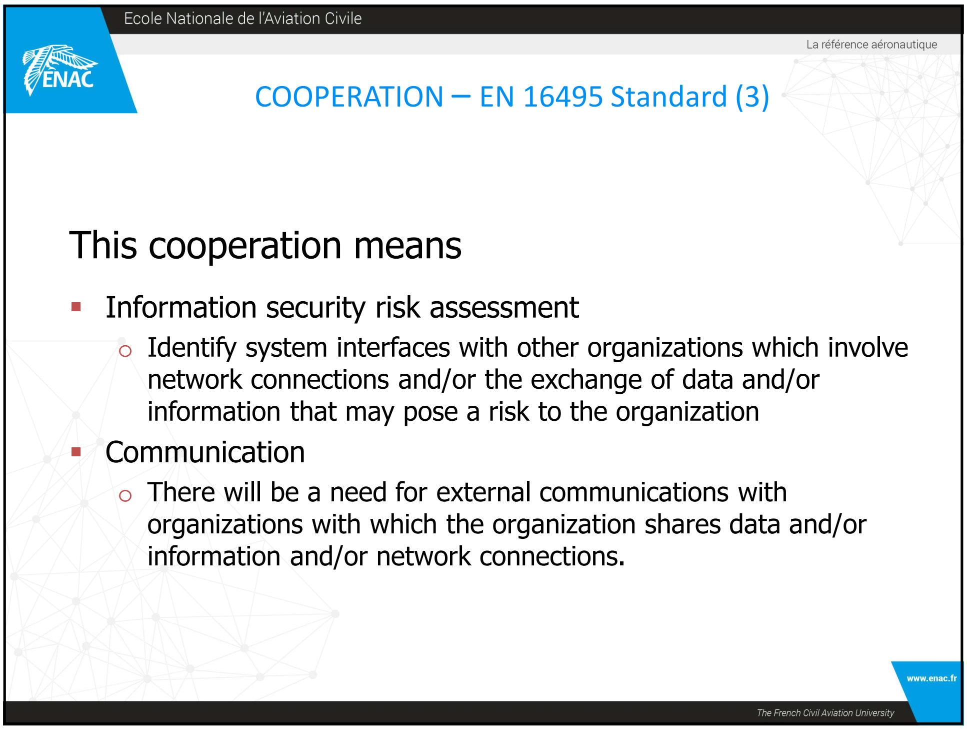
COOPERATION – EN 16495 Standard (2)

Cooperation means

- The organization shall assess the risk due to external network connections and/or the exchange of data and/or information by:
  - ○ Identifying information flows across external interfaces with other organizations
  - ○ Including such flows and interfaces explicitly in the risk assessment
  - ○ Seeking risk assessment and risk treatment information from the organization(s) sharing the external interface and controlling the information which crosses it, as input to the risk assessment
  - ○ Sharing appropriate risk assessment information and risk treatment information with organizations which share the external interface

www.enac.fr

The French Civil Aviation University



Ecole Nationale de l'Aviation Civile

La référence aéronautique

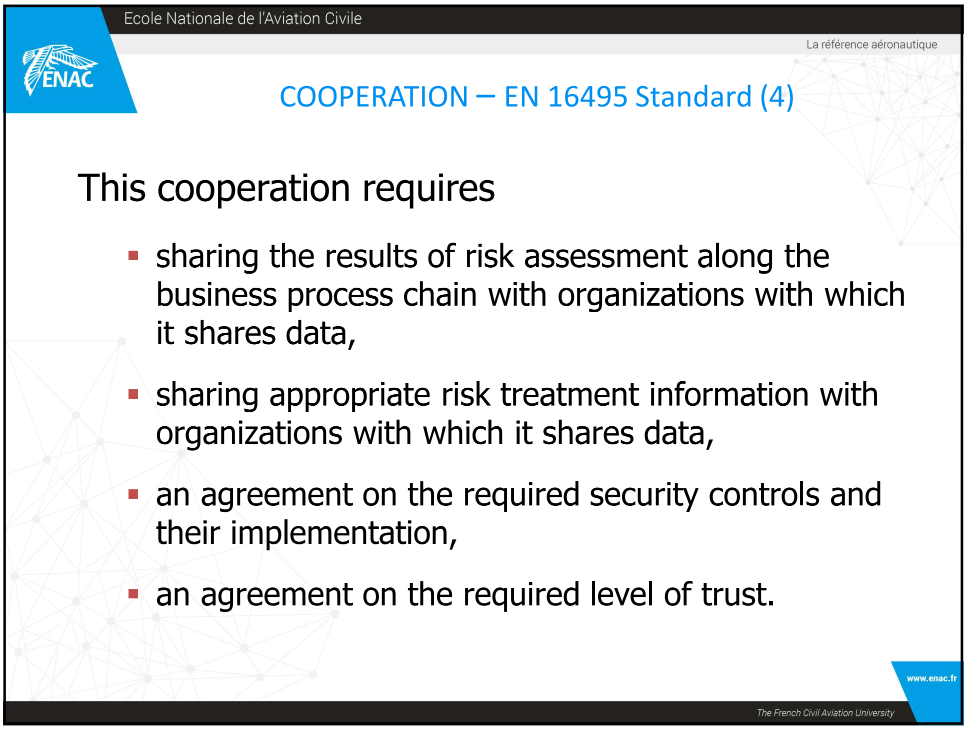
COOPERATION – EN 16495 Standard (3)

This cooperation means

- Information security risk assessment
  - Identify system interfaces with other organizations which involve network connections and/or the exchange of data and/or information that may pose a risk to the organization
- Communication
  - There will be a need for external communications with organizations with which the organization shares data and/or information and/or network connections.

www.enac.fr

The French Civil Aviation University



Ecole Nationale de l'Aviation Civile

La référence aéronautique

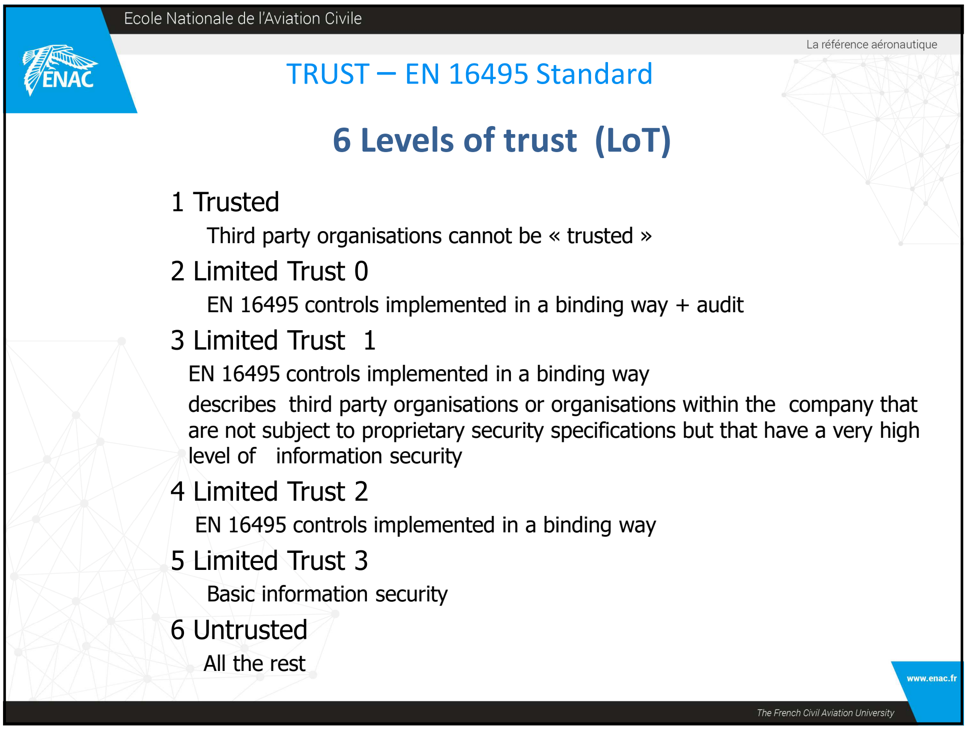
COOPERATION – EN 16495 Standard (4)

This cooperation requires

- sharing the results of risk assessment along the business process chain with organizations with which it shares data,
- sharing appropriate risk treatment information with organizations with which it shares data,
- an agreement on the required security controls and their implementation,
- an agreement on the required level of trust.

www.enac.fr

The French Civil Aviation University



Ecole Nationale de l'Aviation Civile

La référence aéronautique

TRUST – EN 16495 Standard

6 Levels of trust (LoT)

1 Trusted

Third party organisations cannot be « trusted »

2 Limited Trust 0

EN 16495 controls implemented in a binding way + audit

3 Limited Trust 1

EN 16495 controls implemented in a binding way

describes third party organisations or organisations within the company that are not subject to proprietary security specifications but that have a very high level of information security

4 Limited Trust 2

EN 16495 controls implemented in a binding way

5 Limited Trust 3

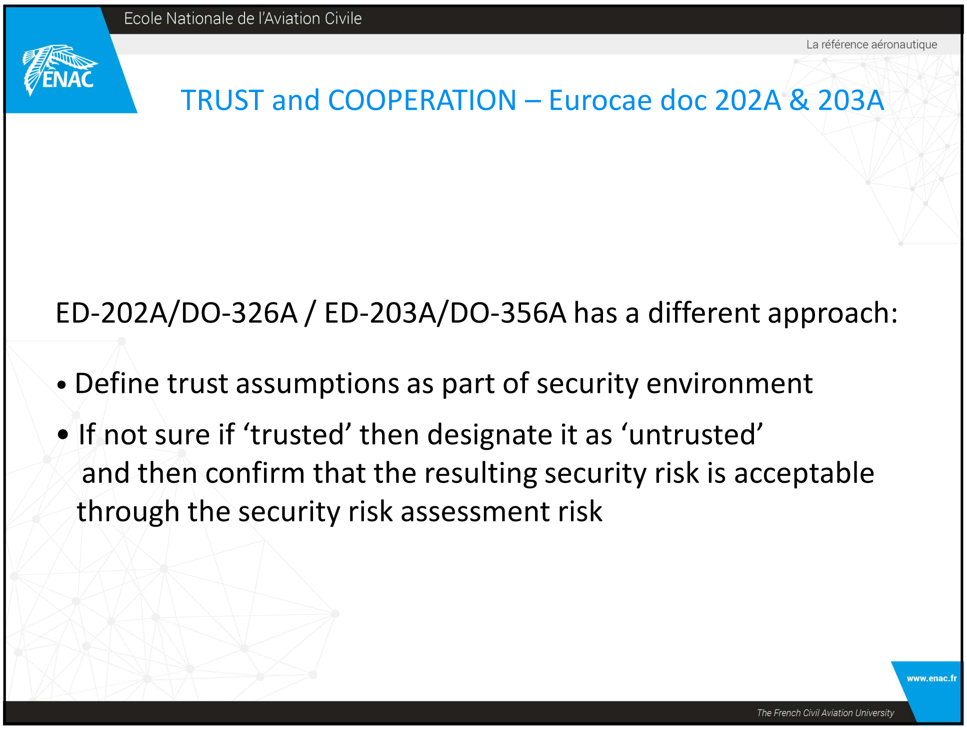
Basic information security

6 Untrusted

All the rest

www.enac.fr

The French Civil Aviation University



Ecole Nationale de l'Aviation Civile

La référence aéronautique

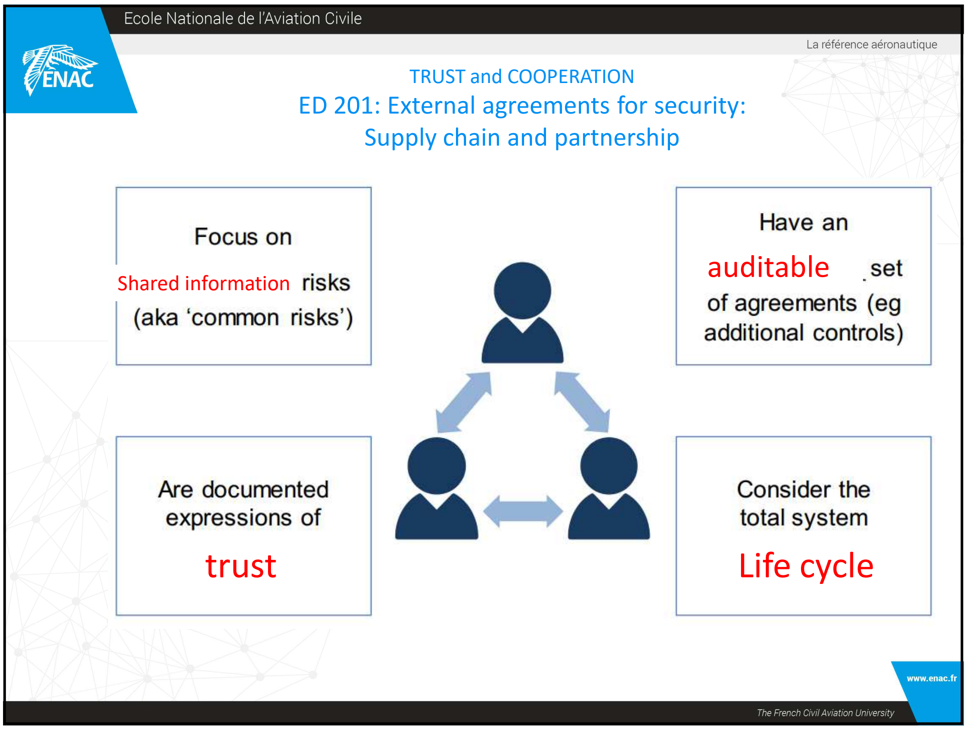
TRUST and COOPERATION – Eurocae doc 202A & 203A

ED-202A/DO-326A / ED-203A/DO-356A has a different approach:

- Define trust assumptions as part of security environment
- If not sure if 'trusted' then designate it as 'untrusted' and then confirm that the resulting security risk is acceptable through the security risk assessment risk

www.enac.fr

The French Civil Aviation University



Ecole Nationale de l'Aviation Civile

La référence aéronautique

TRUST and COOPERATION

ED 201: External agreements for security: Supply chain and partnership

Focus on Shared information risks (aka 'common risks')

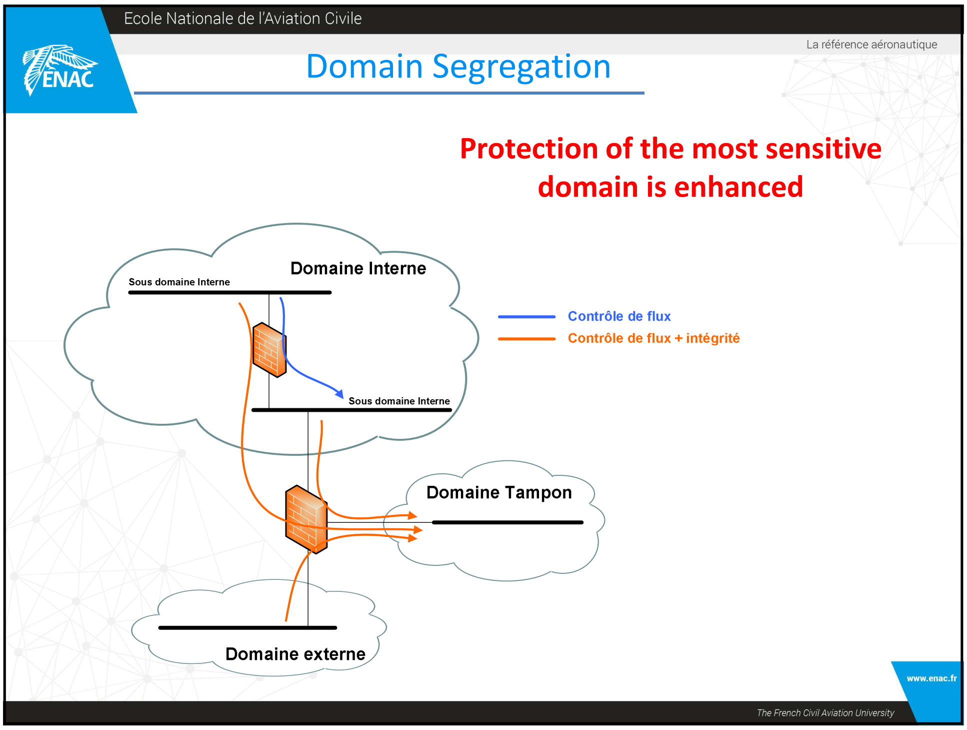
Have an auditable set of agreements (eg additional controls)

Are documented expressions of trust

Consider the total system Life cycle

www.enac.fr

The French Civil Aviation University



Ecole Nationale de l'Aviation Civile

La référence aéronautique

Domain Segregation

Protection of the most sensitive domain is enhanced

Domaine Interne

Sous domaine Interne

Sous domaine Interne

Domaine Tampon

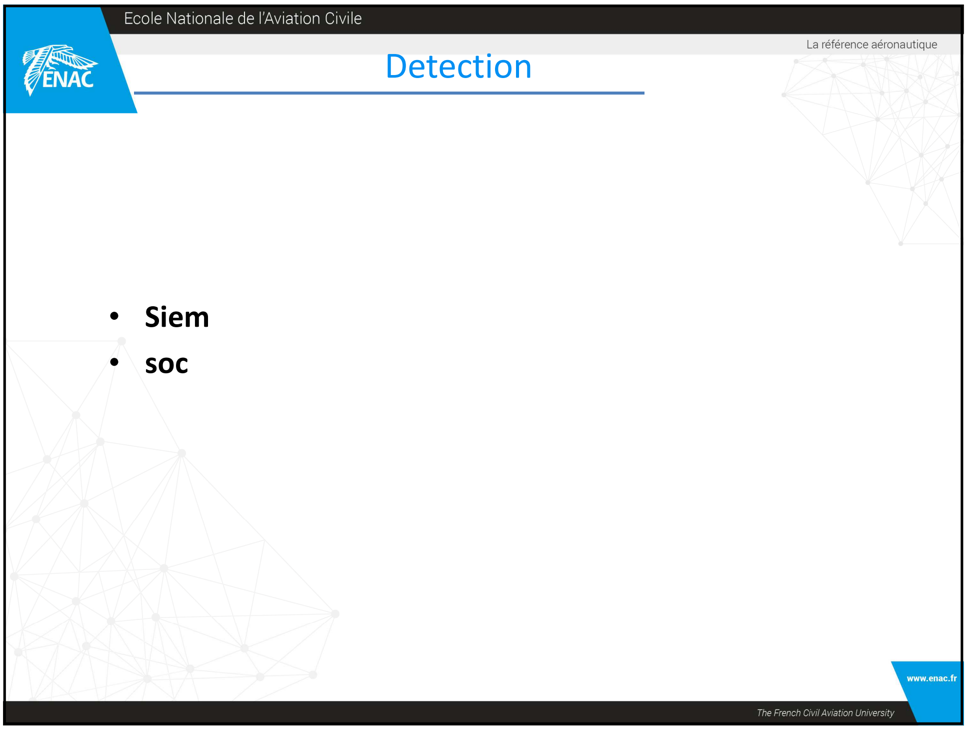
Domaine externe

Contrôle de flux

Contrôle de flux + intégrité

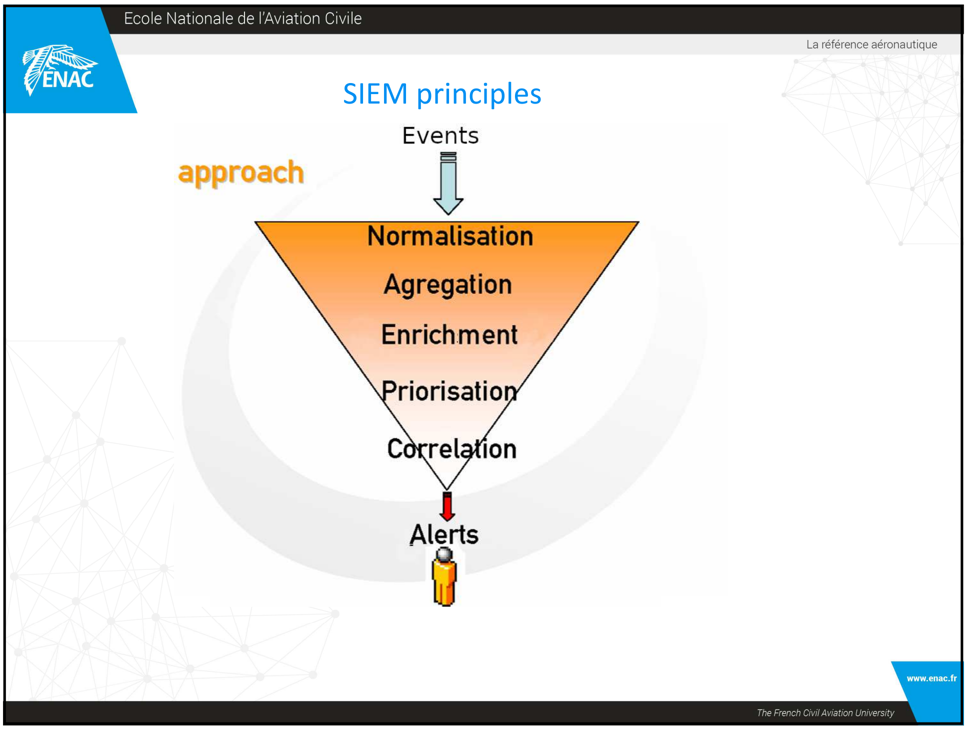
www.enac.fr

The French Civil Aviation University

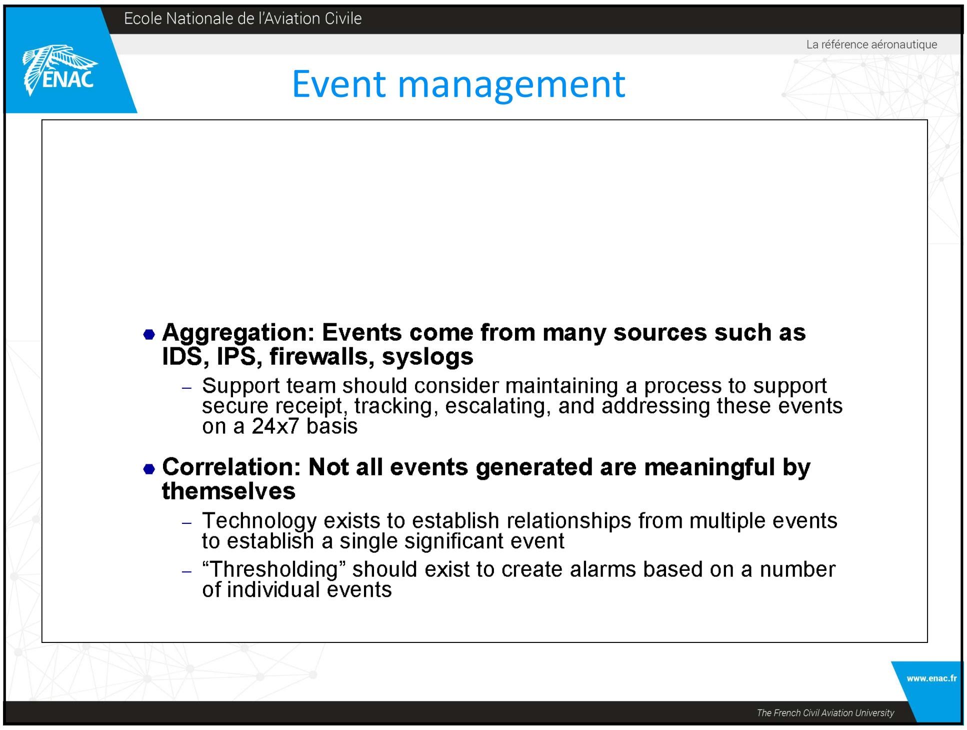


Detection

- **Siem**
- **soc**



SIEM principles



Ecole Nationale de l'Aviation Civile

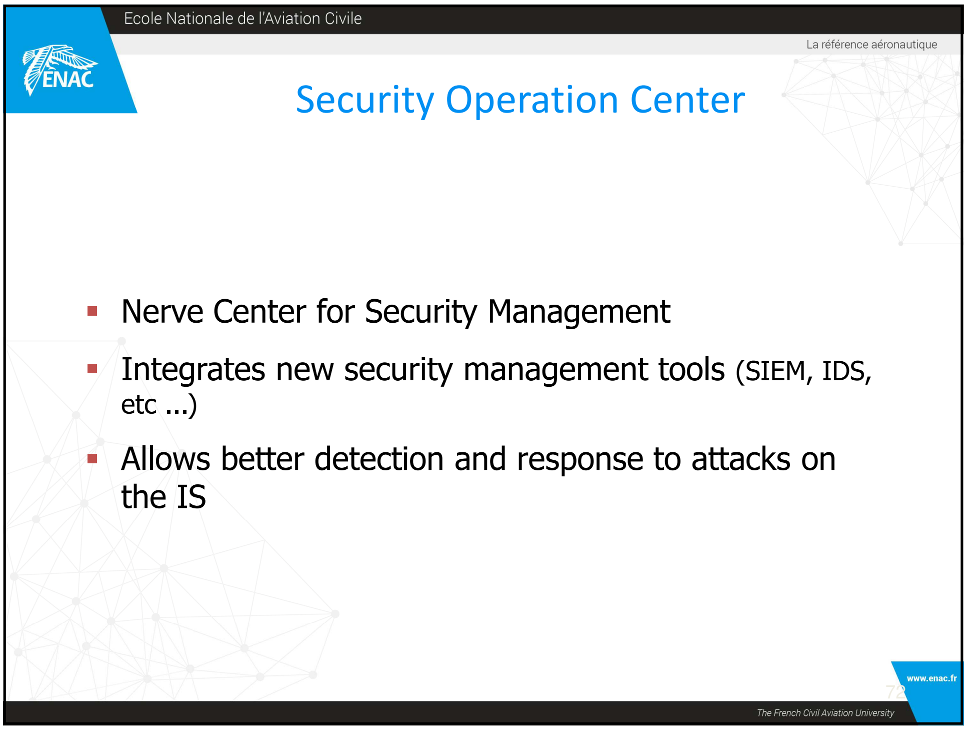
La référence aéronautique

Event management

- **Aggregation: Events come from many sources such as IDS, IPS, firewalls, syslogs**
  - Support team should consider maintaining a process to support secure receipt, tracking, escalating, and addressing these events on a 24x7 basis
- **Correlation: Not all events generated are meaningful by themselves**
  - Technology exists to establish relationships from multiple events to establish a single significant event
  - "Thresholding" should exist to create alarms based on a number of individual events

www.enac.fr

The French Civil Aviation University



Ecole Nationale de l'Aviation Civile

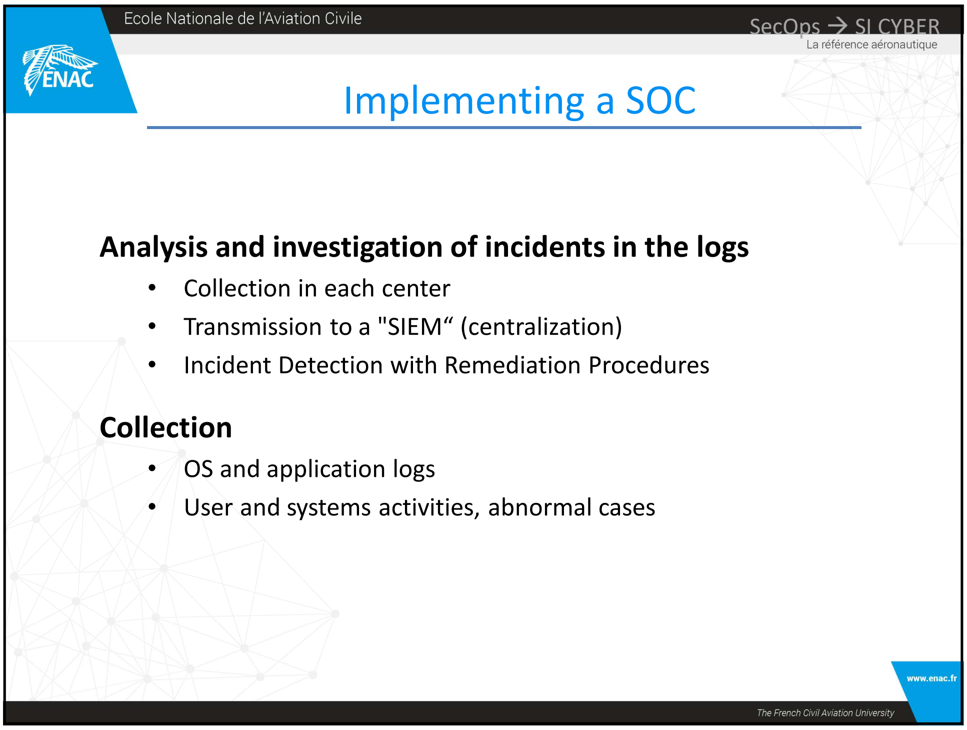
La référence aéronautique

Security Operation Center

- Nerve Center for Security Management
- Integrates new security management tools (SIEM, IDS, etc ...)
- Allows better detection and response to attacks on the IS

www.enac.fr

The French Civil Aviation University



Ecole Nationale de l'Aviation Civile

SecOps → SI CYBER

La référence aéronautique

Implementing a SOC

Analysis and investigation of incidents in the logs

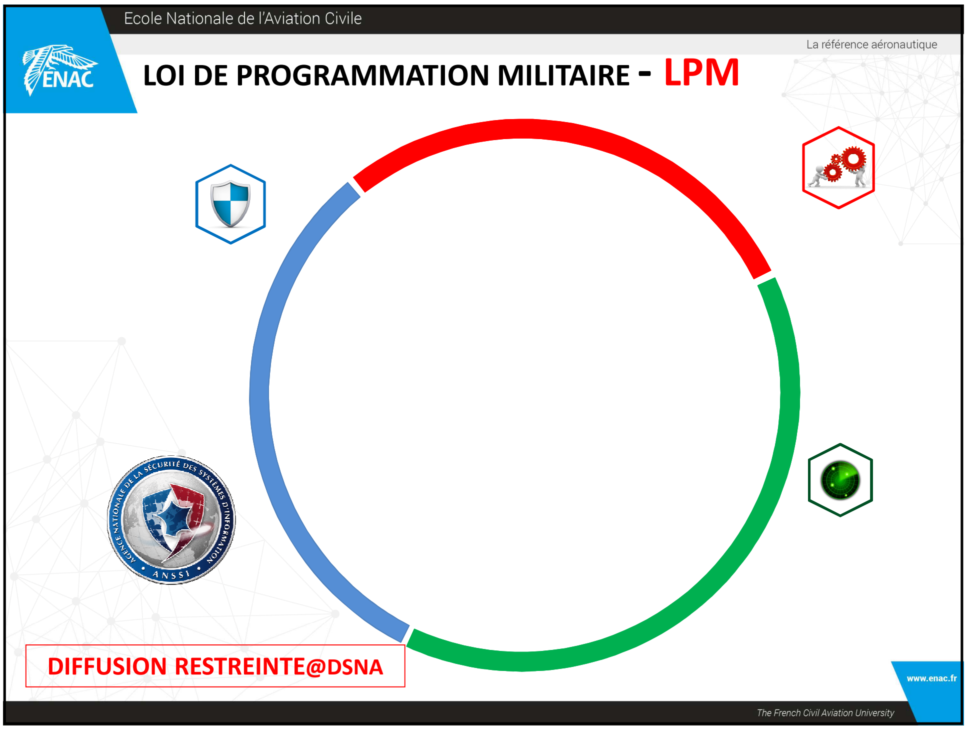
- Collection in each center
- Transmission to a "SIEM“ (centralization)
- Incident Detection with Remediation Procedures

Collection

- OS and application logs
- User and systems activities, abnormal cases

www.enac.fr

The French Civil Aviation University



Ecole Nationale de l'Aviation Civile

La référence aéronautique

LOI DE PROGRAMMATION MILITAIRE - LPM

DIFFUSION RESTREINTE@DSNA

www.enac.fr

The French Civil Aviation University

Ecole Nationale de l'Aviation Civile

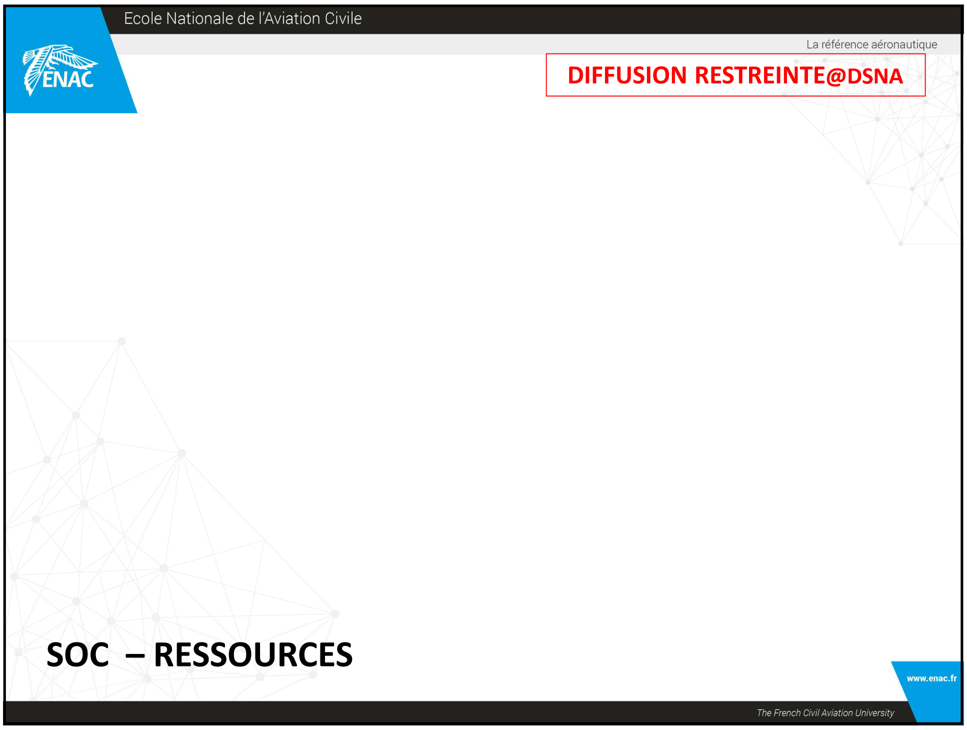
La référence aéronautique

DIFFUSION RESTREINTE@DSNA

SOC – ORGANISATION

www.enac.fr

The French Civil Aviation University



Ecole Nationale de l'Aviation Civile

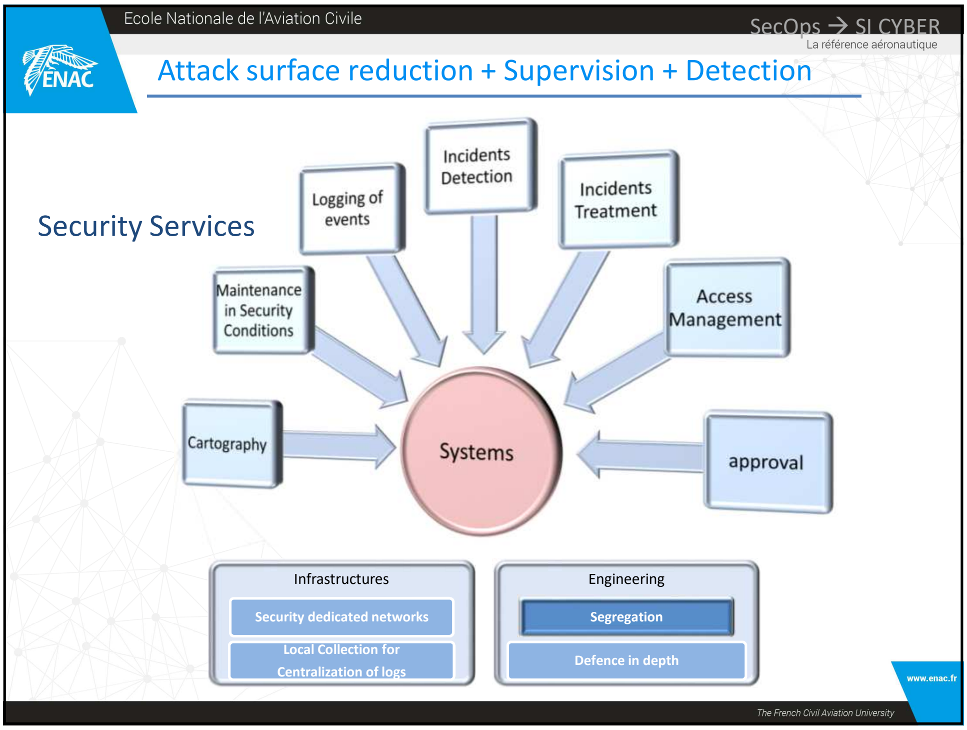
La référence aéronautique

DIFFUSION RESTREINTE@DSNA

SOC – RESSOURCES

www.enac.fr

The French Civil Aviation University



Ecole Nationale de l'Aviation Civile

SecOps → SI CYBER

La référence aéronautique

Attack surface reduction + Supervision + Detection

Security Services

Incidents Detection

Logging of events

Incidents Treatment

Maintenance in Security Conditions

Access Management

Cartography

Systems

approval

Infrastructures

Security dedicated networks

Local Collection for Centralization of logs

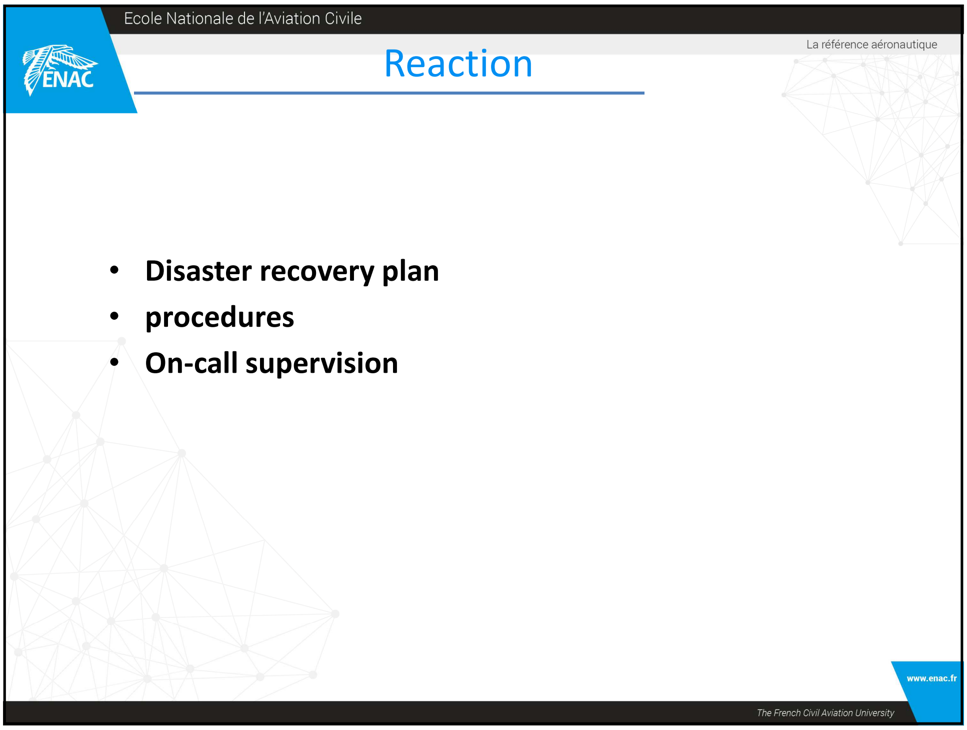
Engineering

Segregation

Defence in depth

www.enac.fr

The French Civil Aviation University



Ecole Nationale de l'Aviation Civile

La référence aéronautique

Reaction

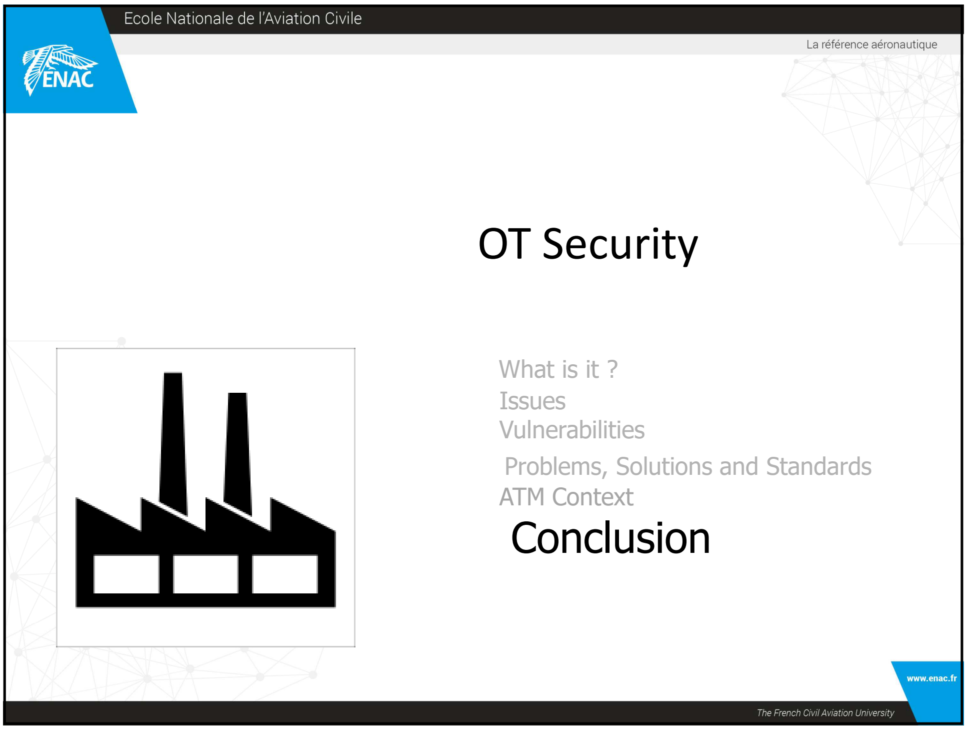
- **Disaster recovery plan**
- **procedures**
- **On-call supervision**

www.enac.fr

The French Civil Aviation University

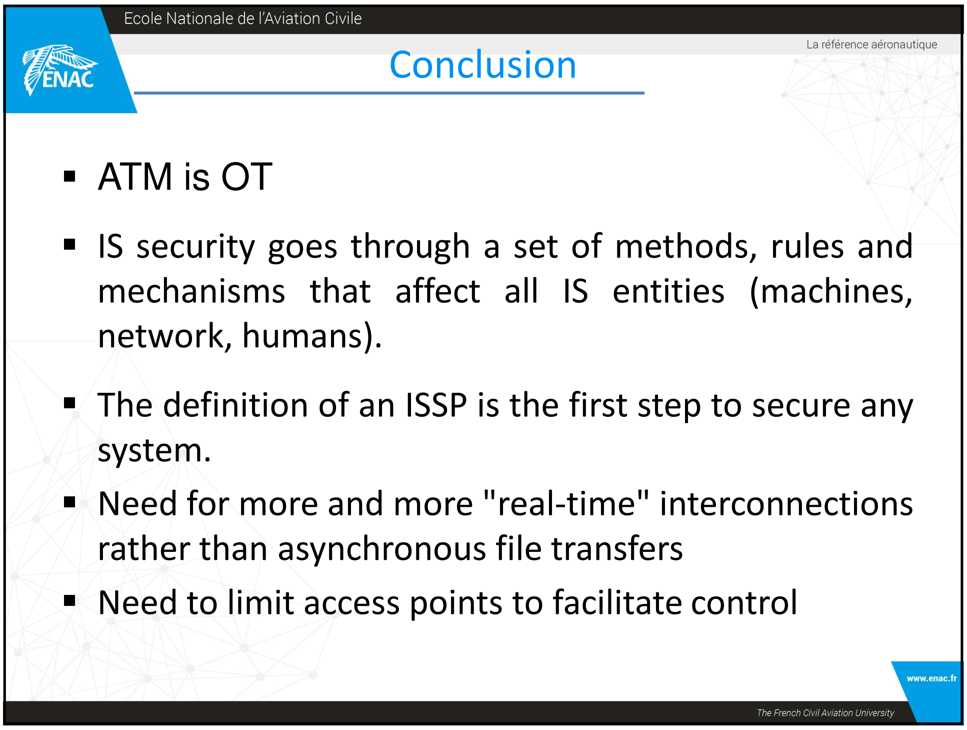
Reaction: Response Plan

- Acquire and inventory the tools needed for intrusion detection, including ID software, backups and file system recovery tools
- Train staff on how to deal with intrusions. This can be through SANS courses, CERT training, vendor courses
- Form a response team
- Build an offline kit of standard system utilities
- Document all incidents carefully; incident reporting should include:
  - person discovering,
  - target systems,
  - purpose of attack
  - Parties notified



OT Security

What is it ?
Issues
Vulnerabilities
Problems, Solutions and Standards
ATM Context
Conclusion



Ecole Nationale de l'Aviation Civile

La référence aéronautique

Conclusion

- ATM is OT
- IS security goes through a set of methods, rules and mechanisms that affect all IS entities (machines, network, humans).
- The definition of an ISSP is the first step to secure any system.
- Need for more and more "real-time" interconnections rather than asynchronous file transfers
- Need to limit access points to facilitate control

www.enac.fr

The French Civil Aviation University