Ecole Nationale de l'Aviation Civile

La référence aéronautique

TLS-SEC

Sûreté des systèmes industriels

Ladislas Hajnal

2020

www.enac.fr

The French Civil Aviation University

Ecole Nationale de l'Aviation Civile

La référence aéronautique

Objectifs

A la fin du cours l'étudiant saura:

- Comprendre ce qu'est un réseau industriel SCADA
- Enoncer les faiblesses de sécurité de ce type de réseau et être capable d'établir un lien avec les faiblesses de sécurité du réseau ATM aéronautique
- Mise en perspective des réseaux aéronautiques par rapport aux réseaux industriels SCADA
- Enumérer les solutions de sécurité utilisées par l'aviation civile française pour rendre le réseau ATM plus sûr

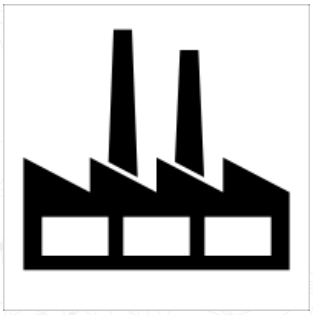
www.enac.fr

The French Civil Aviation University

Ecole Nationale de l'Aviation Civile

La référence aéronautique

Sûreté des Systèmes Industriels



C Quoi

Les enjeux

Vulnérabilités

Problèmes, Solutions et Standards

Contexte ATM

Conclusion

www.enac.fr

The French Civil Aviation University

Ecole Nationale de l'Aviation Civile

les systèmes industriels

C Quoi ?

Les systèmes industriels se composent le plus souvent des éléments suivants :

- *automates Programmables Industriels (API ou PLC)*
- *systèmes Numériques de Contrôle-Commande (SNCC) ;*
- *systèmes Instrumentés de Sécurité (SIS);*
- *capteurs et actionneurs (intelligents ou non);*
- *bus de terrain;*
- *logiciels de supervision et de contrôle : SCADA*;*
- *logiciels de gestion de production assistée par ordinateur (GPAO, MES);*
- *logiciels d'ingénierie et de maintenance*
- *systèmes embarqués.*

* **S**upervisory **C**ontrol **D**ata **A**cquisition (SCADA): Système de supervision industrielle Système permettant d'acquérir et de traiter un grand nombre de données (télémesures télésignalisations et télé-alarmes) et de contrôler des équipements industriels (automates, capteurs, actionneurs…) en leur envoyant des télécommandes et téléréglages.

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 ?

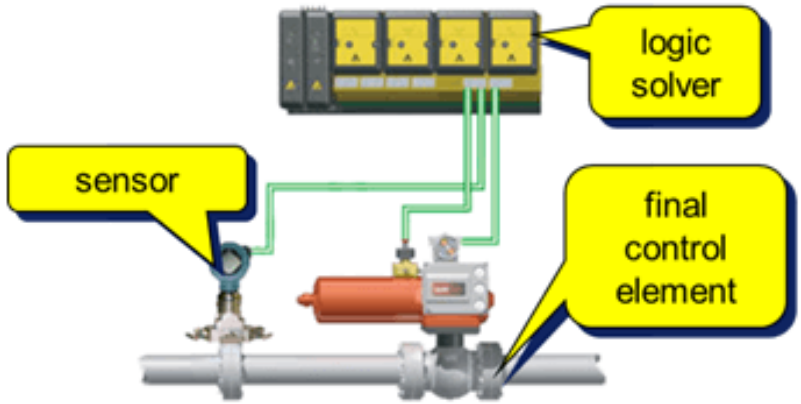
automates Programmables Industriels

www.enac.fr

The French Civil Aviation University

Ecole Nationale de l'Aviation Civile

OT, What is it ?

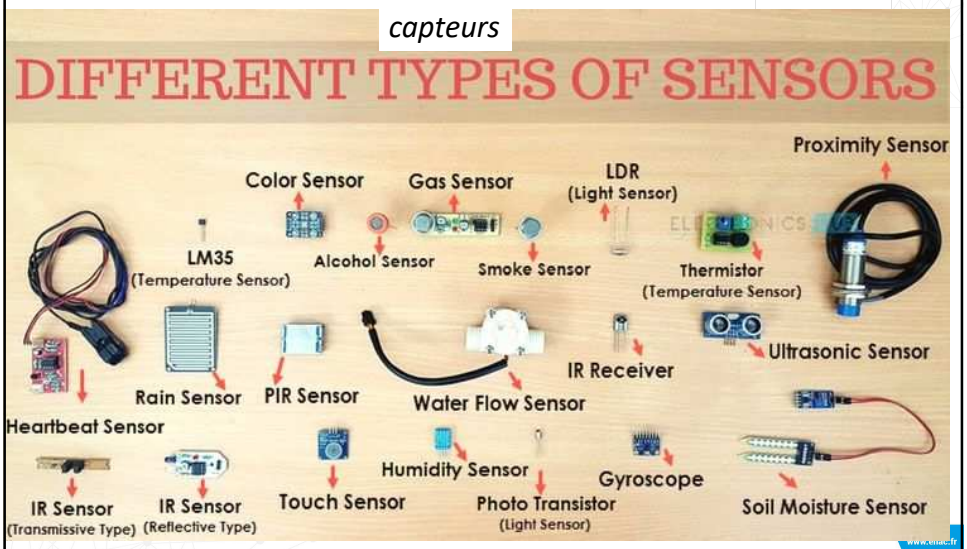


systèmes Instrumentés de Sécurité **(SIS)**

Ecole Nationale de l'Aviation Civile

OT, What is it ?

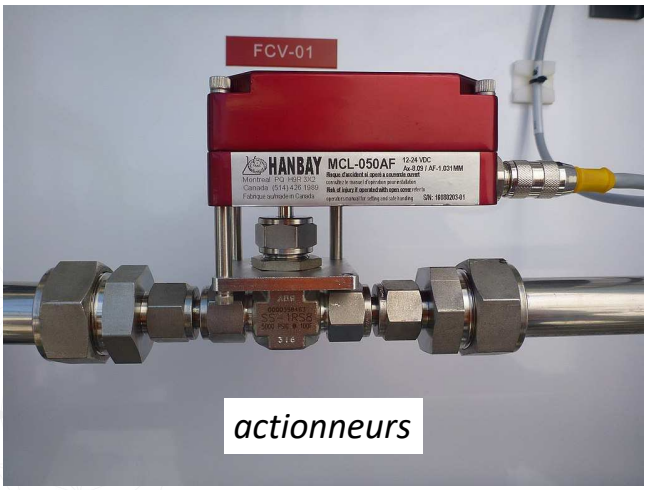
capteurs



www.enac.fr
The French Civil Aviation University

Ecole Nationale de l'Aviation Civile

OT, What is it ?



actionneurs

Electric valve actuator controlling a ½ needle valve

Ecole Nationale de l'Aviation Civile

OT, What is it ?

systèmes embarqués

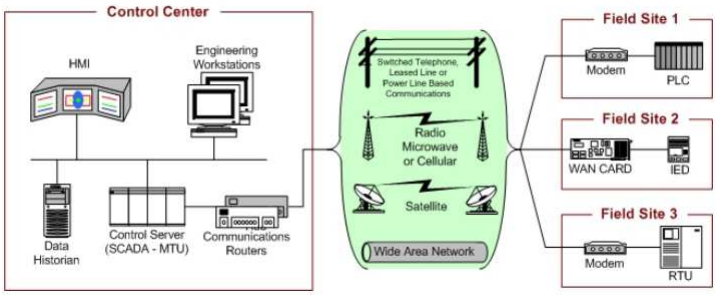
www.enac.fr
The French Civil Aviation University

Ecole Nationale de l'Aviation Civile

La référence aéronautique

OT, What is it ?

SCADA



Scada General Layout

Ecole Nationale de l'Aviation Civile

Les avantages de scada

- Interopérabilité
- coûts de développement réduits
- Flexibilité de l'Interaction Homme-Machine
- Rationalisation et centralisation des actions
- Logs et analyse;
- Centralisation des alarmes et corrélation des évènements

Ecole Nationale de l'Aviation Civile

La référence aéronautique

les systèmes industriels

C Quoi ?

Environnement:

- Fortes contraintes temps réels
- Exigences fortes en sûreté de fonctionnement
- Hétérogénéité:
  - Superpositions des vagues technologiques successives
- De plus en plus connectés
  - sinon à internet, au moins au réseau de gestion ou aux partenaires
- Protocoles de – en – propriétaires

✓Les systèmes industriels utilisent aujourd'hui abondamment les technologies de l'information alors qu'ils n'ont pas été conçus pour faire face aux menaces qu'elles introduisent.

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	

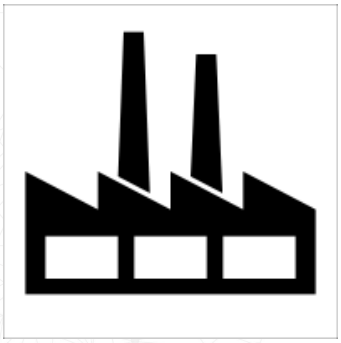
www.enac.fr

The French Civil Aviation University

Ecole Nationale de l'Aviation Civile

La référence aéronautique

Sûreté des Systèmes Industriels



C Quoi

Les enjeux

Vulnérabilités

Problèmes, Solutions et Standards

Contexte Aviation Civile

Conclusion

www.enac.fr

The French Civil Aviation University

Ecole Nationale de l'Aviation Civile

La référence aéronautique

Enjeux (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

Enjeux (2)

- 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.

Ecole Nationale de l'Aviation Civile
La référence aéronautique

Enjeux (3)

- 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

TELVENT

www.enac.fr
The French Civil Aviation University

Ecole Nationale de l'Aviation Civile

La référence aéronautique

SSI pour les systèmes industriels: Les enjeux (4)

- Dommages matériels / corporels
- Perte de chiffre d'affaires
- Impact sur l'environnement
- Vol de données
- Responsabilité civile / pénale -
- Image et notoriété

- Ces différents impacts génèrent des pertes financières liées à la perte d'activité ou au versement de compensations aux victimes potentielles (clients, particuliers, collectivités territoriales, associations, État voire Union Européenne) ainsi qu'une atteinte à l'image de l'entreprise.

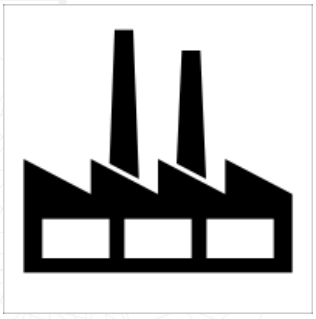
www.enac.fr

The French Civil Aviation University

Ecole Nationale de l'Aviation Civile

La référence aéronautique

Sûreté des Systèmes Industriels



C Quoi
Les enjeux
Vulnérabilités
Problèmes, Solutions et Standards
Contexte ATM
Conclusion

www.enac.fr

The French Civil Aviation University

Ecole Nationale de l'Aviation Civile

La référence aéronautique

Situation Courante

- Opérationnel 24/24 7/7 365/365
- Pas d'antivirus
  - « Ne pas entraver, ralentir le bon déroulement des opérations »
- Pas de veille en vulnérabilité
  - Sauf de la veille technologique pour les nouvelles fonctionnalités
- La Sécurité est principalement physique: pas d'accès au PLC
- Pas de sensibilisation aux risque de SSI

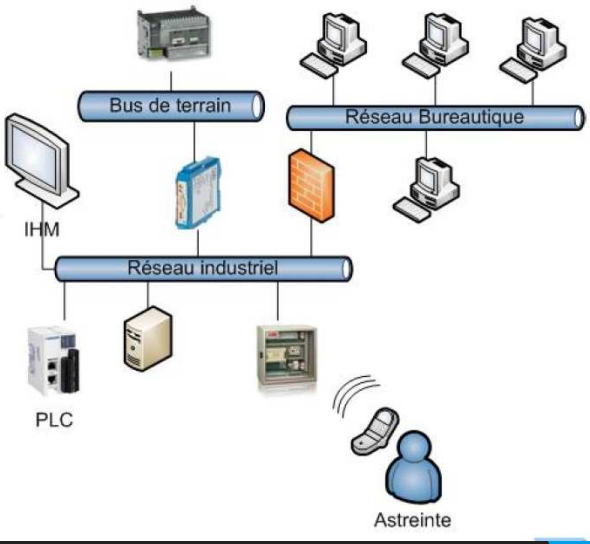
www.enac.fr

The French Civil Aviation University

Ecole Nationale de l'Aviation Civile

Situation courante

- Tout repose sur le filtrage entre les 2 mondes
  - Ne bloque pas toutes les attaques
    - Codes malfaisants
    - Individus
  - Problème des accès distants
    - Astreinte
    - Capteurs extérieurs
    - Équipements sur Internet



The French Civil Aviation University

Ecole Nationale de l'Aviation Civile

La référence aéronautique

OT systems
Résumé des Vulnérabilités

- Nombreux systèmes d'exploitation différents
- Présence de Systèmes hérités (legacy)
- Pas d'antivirus ou de politique de mise à jour
- Sous systèmes isolés (accès via ordi portables or supports amovible);
- Réseaux à plat (ni routeurs ni Firewalls);
- Maintenance fournisseurs par accès distant
- Accès aux systèmes operationnels authorisés à partir de l'environement bureautique.

www.enac.fr

The French Civil Aviation University

Ecole Nationale de l'Aviation Civile

La référence aéronautique

OT systems
Vulnerabilities summary

Aujourd'hui Les systèmes industriels utilisent beaucoup les technologies de l'information, même si elles n'ont pas été conçues pour faire face aux menaces qu'elles représentent.

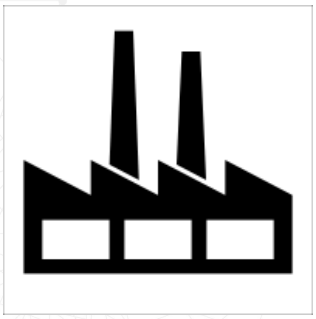
www.enac.fr

The French Civil Aviation University

Ecole Nationale de l'Aviation Civile

La référence aéronautique

Sûreté des Systèmes Industriels



C Quoi
Les enjeux
Vulnérabilités
Problèmes, Solutions et Standards
Contexte ATM
Conclusion

www.enac.fr

The French Civil Aviation University

Ecole Nationale de l'Aviation Civile

La référence aéronautique

Problèmes
Sécurité/Safety VS sûreté/Security

La relation avec la sécurité (SAFETY) augmente au fur et à mesure que vous atteignez les niveaux de contrôle et de processus

- La sûreté devra être réévaluée avec une échelle de temps différente
  - les attaques et les évolutions des menaces, les nouvelles vulnérabilités et les exploitations potentielles entraîneront le démarrage du cycle d'évaluation de la sûreté (security) à un taux supérieur à celui des incidents ou des défaillances qui relancent le cycle d'évaluation de la sécurité (safety).
- Les décisions prises en matière de sécurité ne doivent pas créer de nouvelles failles de sûreté
- De même, les décisions prises en matière de sûreté ne doivent pas compromettre la sécurité.

www.enac.fr

The French Civil Aviation University

Problems
Safety VS Security

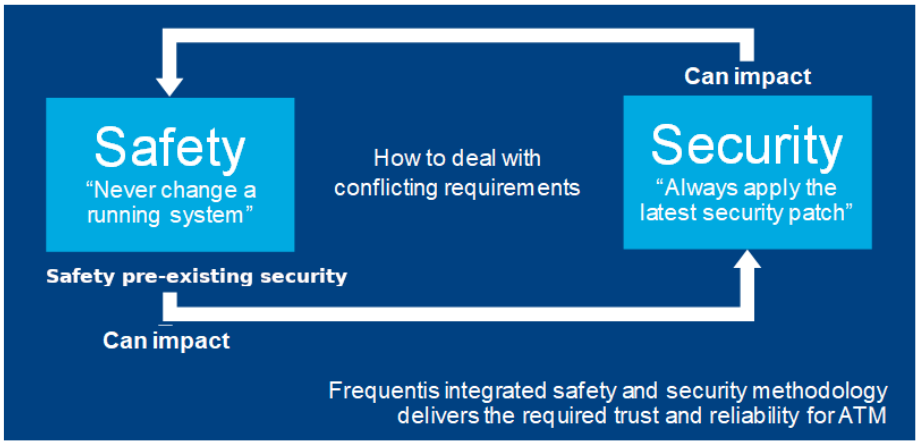
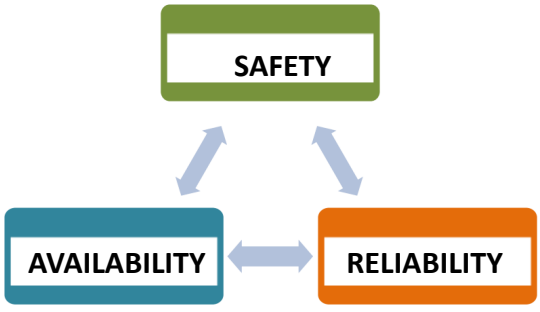


Figure 1 : Conflict of safety and security

Ecole Nationale de l'Aviation Civile
La référence aéronautique

Problems
Safety VS Security



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

Les Limites de l'approche conventionnelle (1)

- les règles informatiques (monde IT) ne s'appliquent pas facilement à l'environnement industriel (monde OT)

Les systèmes industriels sont complexes:

- Hétérogénéité
- Priorités Différentes
- Architectures Différentes
- Critères de performances différents
- Temps réel ….

www.enac.fr

The French Civil Aviation University

Ecole Nationale de l'Aviation Civile

La référence aéronautique

Les Limites de l'approche conventionnelle (2)

- **Hétérogéneité**

  des technologies, du matériel, du logiciel, des protocoles, des droits d'accès …

  - Les PLC ne sont pas facilement remplaçables
    - Le processus de certification est long et coûteux
    - Le matériel est coûteux
  - Les équipments ne sont pas adaptés et limités en ressources
    - Pas d' H-IDS
    - Pas d'authentification
    - Ni de chiffrement possible
  - La diversité des protocoles rend l'implementation de N-IDS difficile

www.enac.fr

The French Civil Aviation University

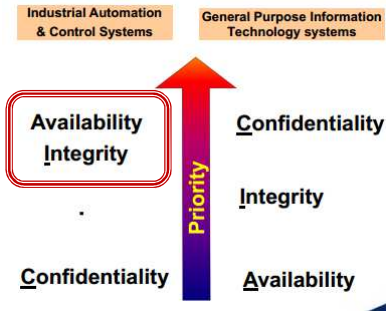
Ecole Nationale de l'Aviation Civile

La référence aéronautique

Les Limites de l'approche conventionnelle (2)

Le systèmes industriels sont complexes:

- **Priorités différentes**
  - Systèmes d'Information (IT)
    Confidentialite d'abord
    gros serveurs à protéger
  - Systèmes Industriels (OT)
    Disponibilité et Intégrité d'abord
    De nombreux points critiques à protéger



www.enac.fr

The French Civil Aviation University

Ecole Nationale de l'Aviation Civile

La référence aéronautique

Les Limites de l'approche conventionnelle (4)

- Architectures Différentes
  - Réseaux à plat
  - Systèmes distants
    - Physiquement accessibles
  - Systèmes isolés
    - Parfois situés dans l'espace public
  - De ce fait beaucoup de points critiques à protéger.

Ecole Nationale de l'Aviation Civile

La référence aéronautique

Solutions

- Réduction de la surface d'attaque
  - Défense en profondeur
  - Segmentation
- Augmenter l'indépendance des différents systèmes
  - Création de zones et de conduits (voir IEC 62443)
- Supervision
- Détection
- Réaction

Ecole Nationale de l'Aviation Civile

La référence aéronautique

La Défense en Profondeur ….

- … augmente la difficulté pour l'attaquant dans le but de rendre l'attaque plus longue
  - Le niveau de sécurité d'un coffre fort se quantifie en temps
- … augmente les chances de détecter l'attaque suffisamment tôt
  - Temps de détection / temps de réaction

Ecole Nationale de l'Aviation Civile

La référence aéronautique

Segmentation (1)

- Limiter les points d'accès
- Création de couches indépendantes
- Chaque couche contient une catégorie d'éléments
  - Cette catégorisation s'appuie sur la fonctionalité, l'inter connectivité, la nature des opérations et l'approche intégrée.

www.enac.fr
The French Civil Aviation University

Segmentation (2)

- Interdire l'accès au réseau opérationnel
  - Mise en place d'une ou plusieurs DMZ interne
    - DMZ par fonction afin de réduire la surface d'attaque
  - Filtrage réseau
    - En entrée comme en sortie
  - Contrôles physiques

Deux 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

Ecole Nationale de l'Aviation Civile

La référence aéronautique

ISA/IEC-62443 Standard

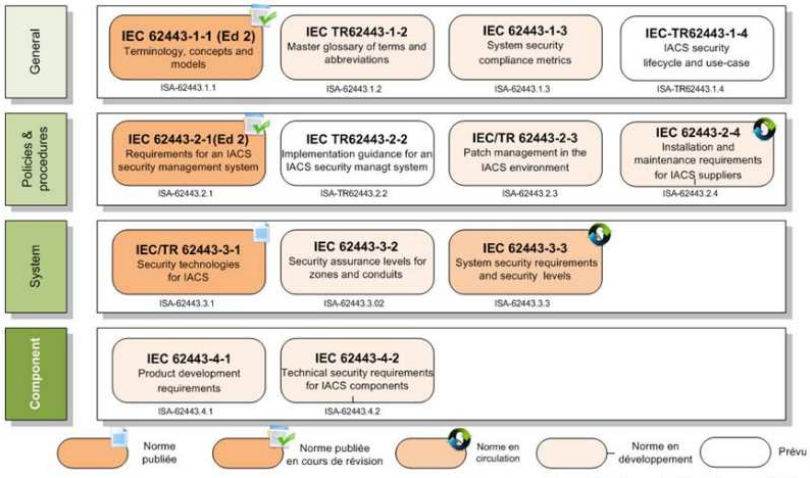
- ISA/IEC-62443: série de normes, rapports techniques et informations définissant des procédures pour la mise en place de systèmes électroniques d'automatisation et de contrôle (IACS).

- Ces directives s'appliquent aux utilisateurs, aux intégrateurs de systèmes, aux praticiens de la sécurité et aux fabricants de systèmes de contrôle responsables de la fabrication, de la conception, de la mise en œuvre ou de la gestion des systèmes d'automatisation et de contrôle industriels.

Ecole Nationale de l'Aviation Civile

La référence aéronautique

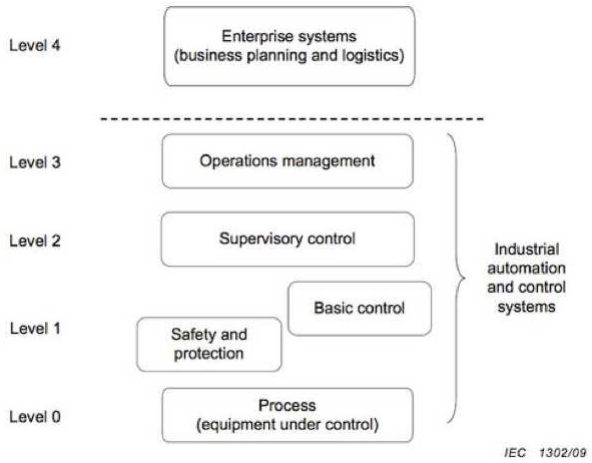
IEC 62443 – Structure des Documents



www.enac.fr
The French Civil Aviation University

IEC 62443 Industrial Control System Reference model

GESTION par SEGREGATION en COUCHES



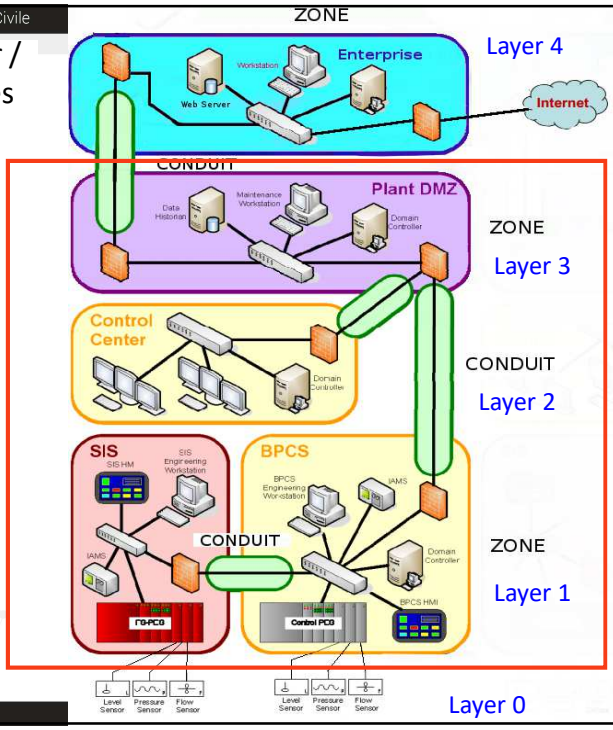
- Chaque couche possède des entités système spécifiques.
  - La plupart d'entre eux seront intégrés par l'environnement en réseau, mais certains d'entre eux peuvent être encore autonome.

Défense en profondeur / Ségrégation en couches

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

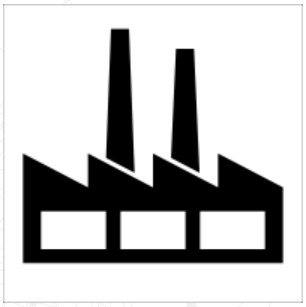
ICS ENVIRONMENT



Ecole Nationale de l'Aviation Civile

La référence aéronautique

Sûreté des Systèmes Industriels



C Quoi
Les enjeux
Vulnérabilités
Problèmes, Solutions et Standards
Contexte ATM
Conclusion

www.enac.fr

The French Civil Aviation University

Ecole Nationale de l'Aviation Civile

La référence aéronautique

Les Fonctions

Communication

Air/ Ground com

Ground com

Surveillance

Navigation

Plan de vol

www.enac.fr

The French Civil Aviation University

Ecole Nationale de l'Aviation Civile

La référence aéronautique

Le contexte ATM, c'est de l'OT

- Fortes contraintes temps réel
  - Disponibilité et intégrité du Contrôle du trafic aérien
- Fortes exigences de fiabilité
  - Les systemes doivent fonctionner correctement
- Hétérogénéité:
  - Superpositions de vagues technologiques successives
- Les composants peuvent être isolés et/ou distants
  - Stations sol de Radio navigation, balisage d'approche ….
- De plus en plus connectés
  - ATC, Compagnies, aéroports, constructeurs, maintenance avion, service météo…
- Protocoles de - en - propriétaires
  - Ethernet, Internet protocol ...

www.enac.fr

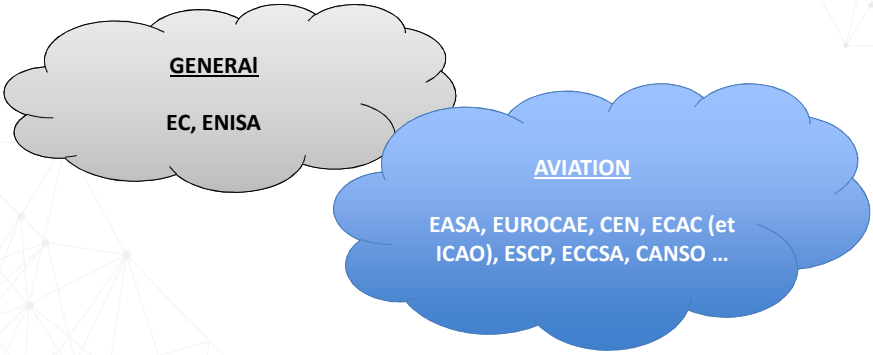
The French Civil Aviation University

Ecole Nationale de l'Aviation Civile

Référentiel → légal

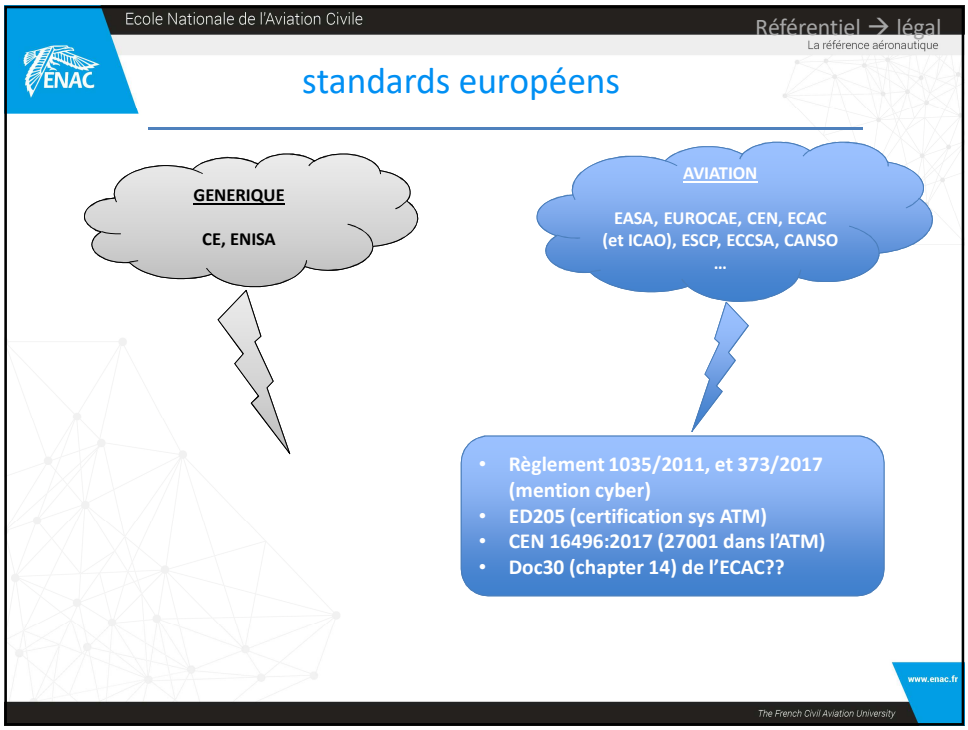
La référence aéronautique

Règlementation



www.enac.fr

The French Civil Aviation University


Ecole Nationale de l'Aviation Civile
Référentiel → légal
La référence aéronautique
standards européens
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
Réglementation France
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

Défense en profondeur ATM couches ED-205*

4 couches :

- Défense périmétrique
- Systèmes d'exploitation et protection serveurs
- Protection du terminal (end-point)
- Protection de l'information

* ED-205 : eurocae documentation 205

www.enac.fr

The French Civil Aviation University

Ecole Nationale de l'Aviation Civile

La référence aéronautique

Défense en profondeur ATM couches ED-205*

Couche sûreté -1:

Systèmes de sécurité pour la défense périmétrique

Réduction et maîtrise des points d'interconnexion entre l'intérieur et l'extérieur

Maîtrise du filtrage des flux sur toutes les couches de la pile réseau, y compris les données d'application (concept de proxy d'application)

* ED-205 : eurocae document 205

www.enac.fr

The French Civil Aviation University

Ecole Nationale de l'Aviation Civile

La référence aéronautique

Défense en profondeur ATM couches ED-205

Couche sûreté -2 :

Systèmes de sécurité des OS et des serveurs d'applications

Cette couche contient la protection des systèmes d'exploitation, des serveurs d'applications, des serveurs Web et des serveurs de messagerie.

Un abus de privilège du système d'exploitation peut potentiellement compromettre la sécurité du réseau.

Le renforcement de cette couche protégera le réseau contre un certain nombre de menaces internes.

Ecole Nationale de l'Aviation Civile

La référence aéronautique

Défense en profondeur ATM couches ED-205

Couche sûreté -3 :

Protection des terminaux

Maintenant que la défense périmétrique est renforcée et que le système d'exploitation est ajusté, les postes de travail internes connectés au réseau constituent une autre menace.

La sécurité des postes de travail (terminaux) est nécessaire pour deux raisons:

- protéger contre toute personne qui tente d'attaquer depuis le réseau
- pour protéger les données stockées sur les postes de travail d'une personne entrant par le pare-feu

www.enac.fr
The French Civil Aviation University

Ecole Nationale de l'Aviation Civile

La référence aéronautique

Défense en profondeur ATM couches ED-205

Couche sûreté -4 :

Protection de l'information (1)

La protection des données est à la mesure des besoins en confidentialité intégrité disponibilité

Lorsque les données sont collectées en dehors de l'organisation, par exemple un ordinateur portable utilisé en dehors du périmètre de sécurité, d'autres contrôles peuvent s'avérer nécessaires, comme par exemple le chiffrement.

La Contextualisation et l'adaptation des contrôles de sécurité dans le domaine le plus sensible

- dépend des besoins du système en disponibilité
- Ne pas oublier que le chiffrement peut avoir une incidence sur la disponibilité en raison du temps nécessaire pour chiffrer et déchiffrer.

www.enac.fr

The French Civil Aviation University

Ecole Nationale de l'Aviation Civile

La référence aéronautique

Défense en profondeur ATM couches ED-205*

Couche sûreté -4 :

Protection de l'information (2)

Les bonnes pratiques de défense en profondeur :

- Considérez toutes les interfaces par lesquelles les données entrent dans un réseau ou un hôte comme un vecteur de menace possible et protégez ces interfaces.
- Les contrôles de sécurité doivent être indépendants, divers et isolés les uns des autres.
- Les protections physiques sont généralement prises en compte dans les hypothèses d'environnement de sécurité concernant les zones et les accès sécurisés.

www.enac.fr

The French Civil Aviation University

Ecole Nationale de l'Aviation Civile

La référence aéronautique

ATM défense en profondeur

ATM OPERATIONAL SYSTEMS are PHYSICALY ISOLATED

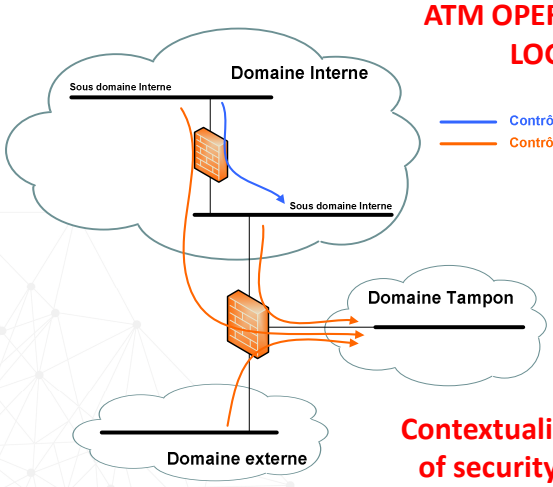
badge access control system for staff,

Ecole Nationale de l'Aviation Civile

La référence aéronautique

ATM défense en profondeur

ATM OPERATIONAL SYSTEMS are LOGICALY ISOLATED

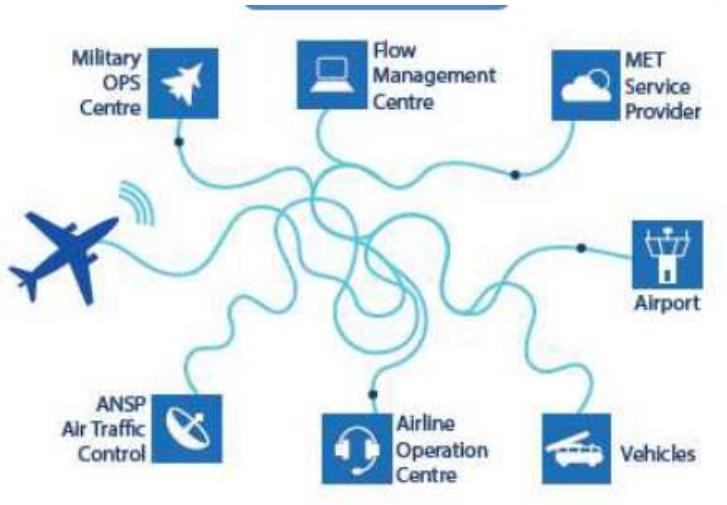


Contextualisation and Adaptation of security controls in the most sensitive domain

Ecole Nationale de l'Aviation Civile

La référence aéronautique

ATM: un système de systèmes



www.enac.fr

The French Civil Aviation University

Ecole Nationale de l'Aviation Civile

La référence aéronautique

Coopération et confiance

Le transport aérien étant un système de systèmes, la coopération est essentielle

- Les membres internes du personnel sont dignes de confiance
  - Formations initiales et continues
  - Campagnes de sensibilisation
- Réseau de confiance
  - Niveaux de confiance - cf. Norme EN 16495
  - Eurocae Doc 201: Accords externes pour la sécurité

www.enac.fr

The French Civil Aviation University

Ecole Nationale de l'Aviation Civile

La référence aéronautique

CONFIANCE et COOPERATION – EN 16495 Standard

Toutes les exigences de la présente Norme européenne sont basées sur la confiance et la coopération entre les parties impliquées dans la gestion du trafic aérien

La fourniture de services dans l'aviation est essentiellement définie par la coopération entre participants individuels.

Aéroports
Compagnies Aériennes
opérateurs
Maintenance (MRO Maintenance Repair and operations)
ANSP (Air Navigation Service Providers)
Constructeurs Aéro
Fournisseurs Avions
Fournisseurs de données Aéro

Ecole Nationale de l'Aviation Civile

La référence aéronautique

COOPERATION – EN 16495 Standard (1)

Cette coopération signifie

- Comprendre les besoins et attentes des parties concernées
  - Les parties intéressées sont les organisations communiquant par échange de données et/ou d'information et/ou via des connexions réseau
- La direction doit assurer la transparence de la gestion de la sécurité de l'information au sein de sa propre organisation, y compris des processus transorganisationnels.

www.enac.fr
The French Civil Aviation University

Ecole Nationale de l'Aviation Civile

La référence aéronautique

COOPERATION – EN 16495 Standard (2)

Coopération signifie

- L'organisation doit évaluer le risque lié aux connexions réseau externes et/ou à l'échange de données et/ou d'informations en:
  - Identifiant les flux d'informations via des interfaces externes avec d'autres organisations
  - Prenant en compte explicitement ces flux et interfaces dans l'évaluation des risques
  - Obtenant les informations sur l'évaluation et le traitement des risques auprès des organisations avec lesquelles on partage une interface externe et qui contrôlent les informations qui la traversent et ce, dans le but de contribuer à sa propre évaluation de risques,
  - Partageant les informations appropriées pour l'évaluation et le traitement des risques avec les organisations avec lesquelles on communique.

www.enac.fr

The French Civil Aviation University

Ecole Nationale de l'Aviation Civile

La référence aéronautique

COOPERATION – EN 16495 Standard (4)

La cooperation requiert

- Le partage des résultats de l'évaluation du risque tout au long du processus avec les entités partenaires
- Le partage des informations appropriées sur le traitement des risques avec les organisations tierces
- un accord sur les contrôles de sécurité requis et leur mise en œuvre,
- un accord sur le niveau de confiance requis

www.enac.fr

The French Civil Aviation University

Ecole Nationale de l'Aviation Civile

La référence aéronautique

TRUST – EN 16495 Standard

6 Niveaux de confiance (LoT)

1 De confiance

Les organismes tiers ne sont pas « de confiance »

2 Confiance Limitée 0

EN 16495 Toutes les mesures sont implémentées de manière contraignante + audit

3 Confiance Limitée 1

EN 16495 Toutes les mesures sont implémentées de manière contraignante décrit des organismes tiers ou des organismes au sein de l'entreprise qui ne sont pas soumis aux spécifications de sécurité propriétaires mais qui ont un niveau très élevé de sécurité de l'information

4 Confiance Limitée 2

EN 16495 les mesures sont implémentées de manière contraignante

5 Confiance Limitée 3

Basic information security

6 Non Fiable

Tout le reste

www.enac.fr

The French Civil Aviation University

Ecole Nationale de l'Aviation Civile

La référence aéronautique

Confiance et Coopération – Eurocae doc 202A & 203A

ED-202A/DO-326A / ED-203A/DO-356A propose une approche différente:

• Définir les hypothèses de confiance dans l'environnement de sécurité

• Si la confiance n'est pas assurée, le tiers doit être désigné comme non fiable et la confirmation que le risque de sécurité résultant est acceptable se fera au moment du processus d'évaluation des risques de sécurité.

www.enac.fr

The French Civil Aviation University

Ecole Nationale de l'Aviation Civile

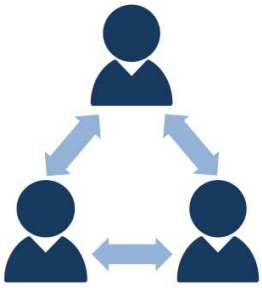
La référence aéronautique

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

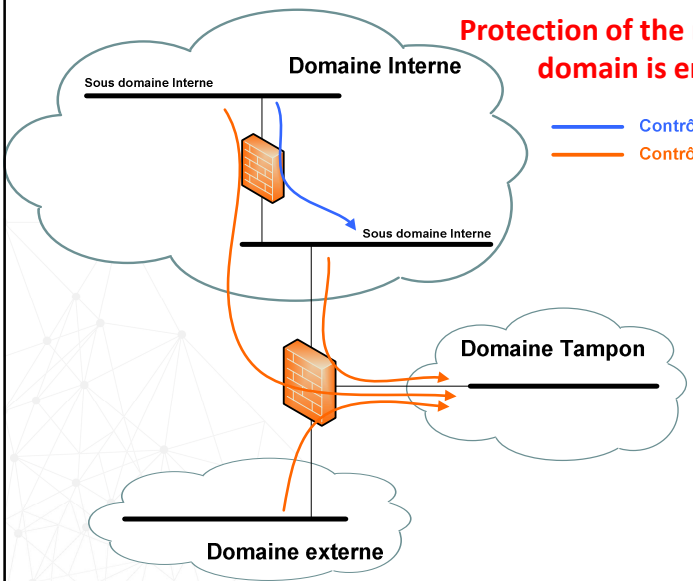
La référence aéronautique

Ségrégation de domaine

Protection of the most sensitive domain is enhanced

Contrôle de flux

Contrôle de flux + intégrité



www.enac.fr

The French Civil Aviation University

Ecole Nationale de l'Aviation Civile

La référence aéronautique

Detection

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

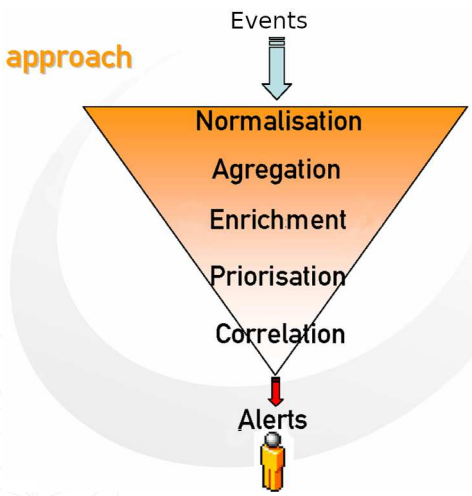
www.enac.fr

The French Civil Aviation University

Ecole Nationale de l'Aviation Civile

La référence aéronautique

SIEM principles



www.enac.fr

The French Civil Aviation University

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

Ecole Nationale de l'Aviation Civile

La référence aéronautique

Security Operation Center

- Centre nerveux pour la gestion de la sûreté
- Implémente de nouveaux outils de gestion de la sûreté (SIEM, IDS, etc ...)
- Assure meilleure détection et réponse aux attaques sur le système d'information
- une

www.enac.fr
The French Civil Aviation University

Mise en place d'un SOC

Analyse et investigation des incidents dans les logs

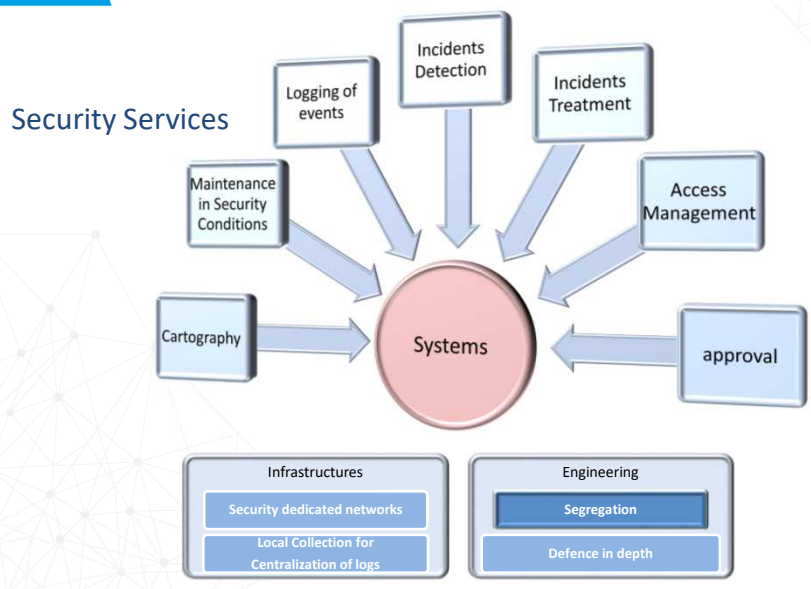
- Collecte dans chaque centre
- Transmission vers 1 "SIEM" (centralisation)
- Detection d'Incidents avec procédures de Remédiation

Collecte

- Journaux (logs) des OS et des application
- Activités utilisateurs et systémes, situations anormales

Ecole Nationale de l'Aviation Civile
SecOps → SI CYBER
La référence aéronautique

Attack surface reduction + Supervision + Detection



www.enac.fr
The French Civil Aviation University

Ecole Nationale de l'Aviation Civile

La référence aéronautique

Réaction

- **Plan de reprise**
- **procédures**
- **Supervision H24**

www.enac.fr

The French Civil Aviation University

Ecole Nationale de l'Aviation Civile

La référence aéronautique

Réaction: Plan d'intervention

- acquérir et inventorier les outils nécessaires à la détection des intrusions, y compris les sauvegardes, les logiciels d'identification et les outils de récupération des systèmes de fichiers
- Former les personnels à la réaction en cas d'incident de SSI
- Mettre en place un équipe d'intervention
- créer un kit hors ligne d'utilitaires système standard
- Documenter avec soin les incidents:
  - Qui à relevé l'incident
  - Systèmes ciblés
  - But de l'attaque
  - Personnes et autorités informeés

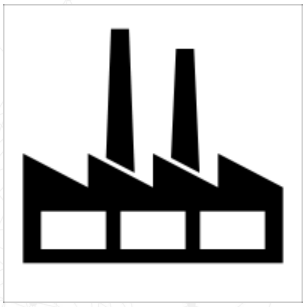
www.enac.fr

The French Civil Aviation University

Ecole Nationale de l'Aviation Civile

La référence aéronautique

Sécurité des systèmes industriels



C quoi?
Enjeux
Vulnérabilités
Problèmes, Solutions et Standards
Le contexte ATM
Conclusion

www.enac.fr

The French Civil Aviation University

Ecole Nationale de l'Aviation Civile

La référence aéronautique

Conclusion

- Le contexte ATM est celui d'un système industriel
- La SSI passe par un ensemble de méthodes, règles et mécanismes qui affectent toutes les entités du système d'information (machines, réseau, ressources humaines).
- La définition d'une PSSI est la première étape pour sécuriser un système.
- Nécessité de plus en plus d'interconnexions "en temps réel" plutôt que de transferts de fichiers asynchrones.
- Nécessité de limiter les points d'accès pour faciliter le contrôle

www.enac.fr

The French Civil Aviation University