INTEGRATED SAFETY AND SECURITY ANALYSIS USING STPA AND NIST SP800-30

DANIEL PEREIRA[1, 2], **CELSO HIRATA[2]**, RODRIGO PAGLIARES[2]

[1] EMBRAER, BRAZIL

[2] ITA, S. J. CAMPOS, SP, BRAZIL

DANIEL.PATRICK@EMBRAER.COM.BR HIRATA@ITA.BR PAGLIARES@GMAIL.COM

CONTEXT

- Part of the Project: Techniques of security and software engineering for development of aeronautics embedded systems
  - ITA, Brazil: Celso Hirata
  - Embraer, Brazil: Cláudio Castro
  - LiU, Sweden: Simin Nadjm-Tehrani
  - Saab, Sweden: Ingemar Söderquist
- Part of the PhD Work of Daniel Pereira

Hackers bombard aviation sector with over 1,000 attacks per month

Home | Justice & Home Affairs | News

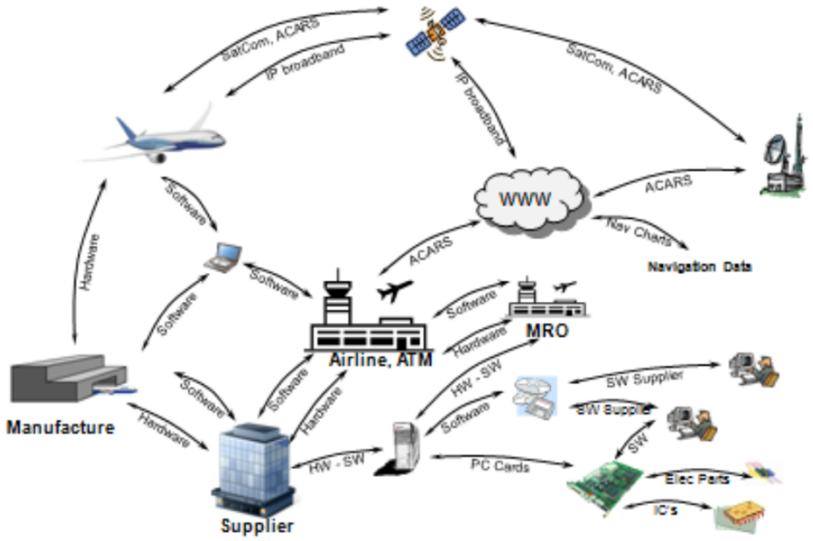
By Jorge Valero | EurActiv.com

11 de jul de 2016 (updated: 11 de jul de 2016)

According to experts, on-the-ground management systems offer more vulnerabilities than the plane systems.

[ROMAN BOED/Flickr]

Figure 1: The ICT Environment for Aviation



Cyber Security is a Shared Responsibility

AIAA

The World's Forum for Aerospace Leadership

SCIENTIFIC AMERICAN

SUBSCRIBE

THE CONVERSATION

AEROSPACE

Is Commercial Aviation as Safe and Secure as We're Told?

A criminologist who studies the issues weighs in on the latest risks

By Frederic Lemieux, George Washington University, The Conversation on May 20, 2016 Véalo en español

For instance, most planes use Automatic Dependent Surveillance–Broadcast, which sends unencrypted data on a plane's position. This data could be tampered with by an ill-intentioned person who could alter the real positioning of an aircraft.

In 2015, the hacker Chris Roberts claimed that he was able to access critical plane functions, including the engine, via the entertainment system of the plane.

The Government Accounting Office has also identified several vulnerabilities related to the information systems used by air traffic control.

GOAL

- Propose an approach to analyze safety and security in an integrated manner.
  - Our focus is aeronautical embedded systems
- We use **safety and security constraints** and identify their relationships obtained from STPA and NIST 800-30.

SAFETY AND SECURITY

- Safety measures prevent losses due to unintentional actions by benevolent actors
  - risks arising from the system and potentially impacting the environment.
- Security measures prevent losses due to intentional actions by malevolent actors
  - Risks originating from the environment and potentially affecting the system.

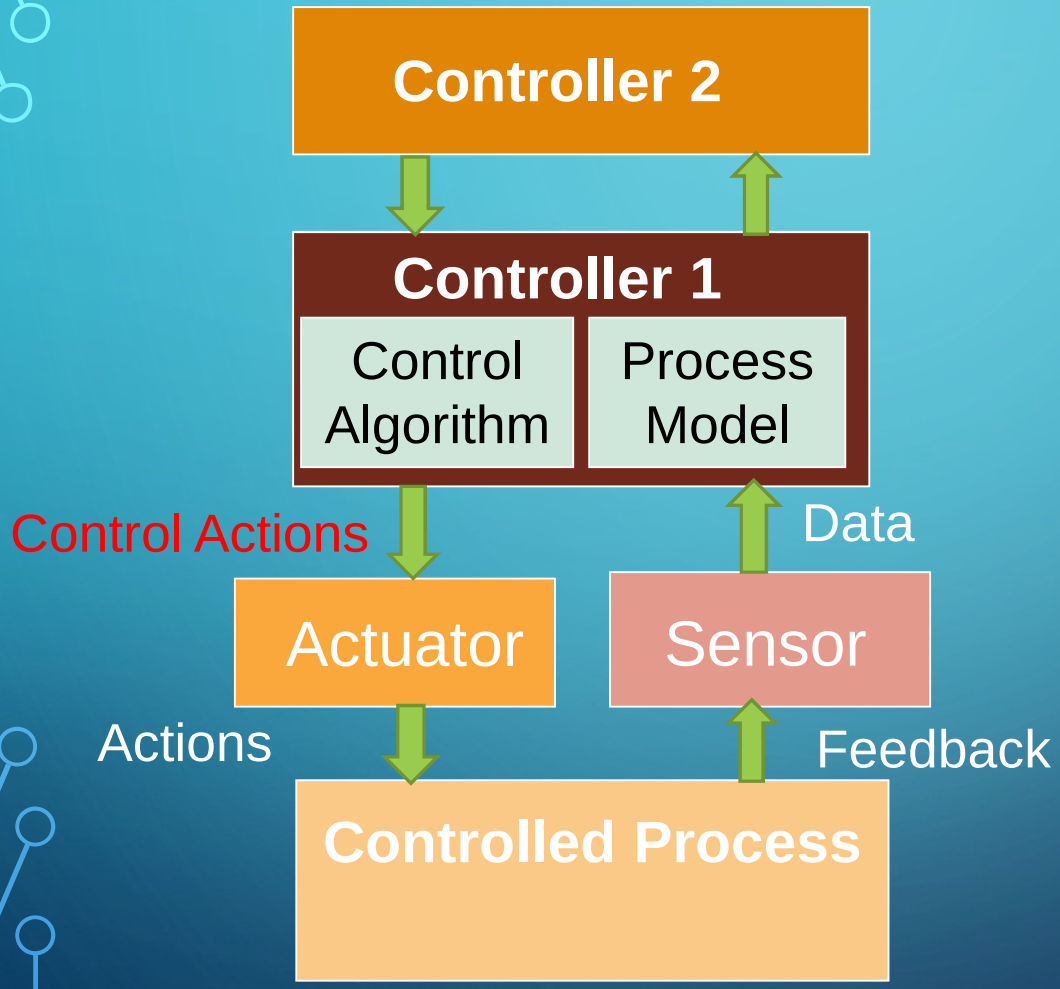
SAFETY AND SECURITY

- Both are emergent **system** properties and have loss prevention as the primary goal.
- Both are result of analysis and design decisions and operational decisions (controls).

STAMP

- Accident causality model that emphasizes the enforcing of safety constraints on system behavior.
- Safety is viewed as a control problem rather than a reliability problem.
- 3 basic constructs: safety constraints, hierarchical safety control structures and process models.

STAMP - HIERARCHICAL CONTROL STRUCTURE



- Controllers use a **process model** to determine control actions
- Accidents often occur when the process model is incorrect
- Hazardous control actions:
  - Control action is not given
  - Unsafe control action is given
  - Potentially safe control action
    - given too early or too late,
    - stops too soon or applies too long

STPA

- Identify the unsafe control actions that can lead to system unsafe behavior.
  - Types of unsafe control actions: *incorrect or unsafe control commands are provided; required control actions are not provided; potentially safe commands are provided too early or too late;* and *control action stopped too soon or applied too long.*
- Identifying the potential causes of scenarios that lead to unsafe control, which allows identify additional safety requirements.

NIST 800-30

- Provides guidance for carrying out tasks of a risk assessment process.
- Identifying specific risk factors and indicators that must be monitored on an ongoing basis.
- Identify threats event/source and vulnerabilities respectively.
- Determine the security controls, evaluating the adverse impact with risk as a combination of impact and likelihood.

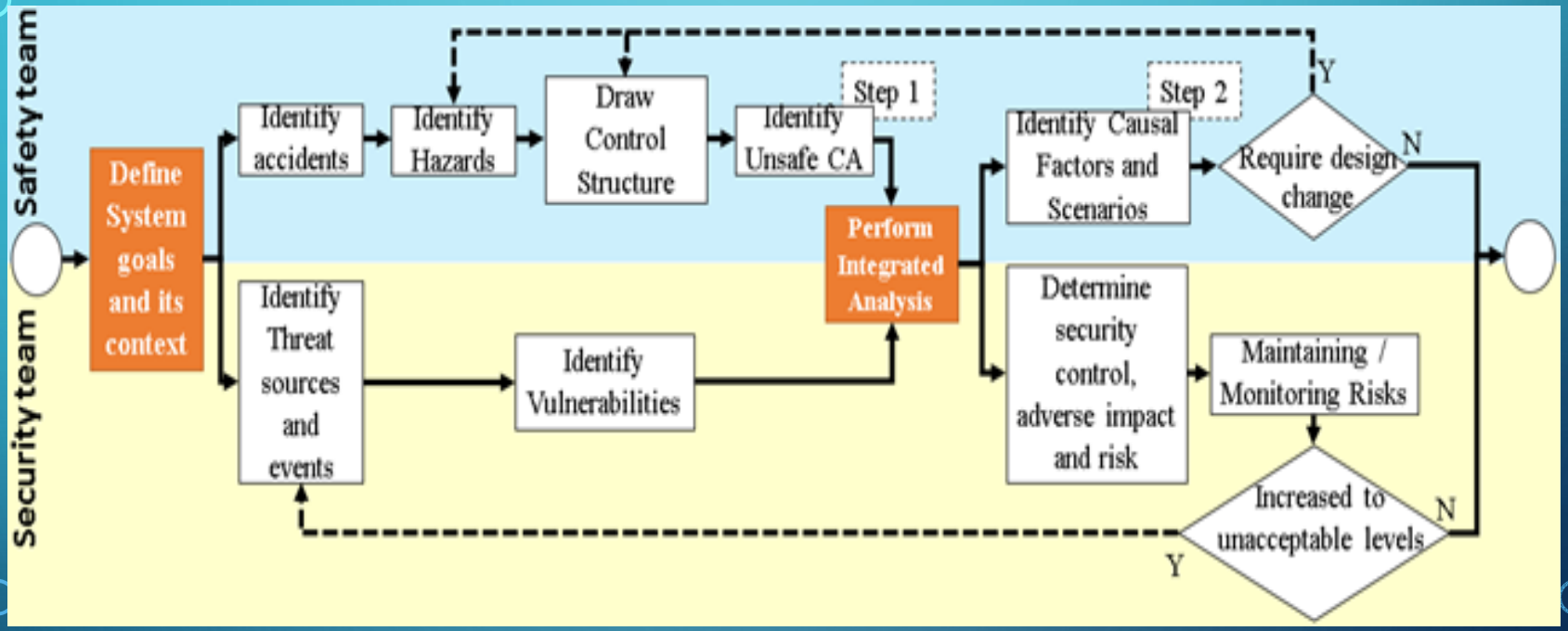
RELATED WORK

- STPA-Sec (Young and Leveson): based on systems theory and the STAMP causality model.
- STAMP applied to Safety reframes the problem as a control rather than a failure problem
- STAMP applied to security reframes security as a strategic problem rather than tactical problem.
- STPA-Sec is an extension to STPA and considers the intentional actions in the generation of the causal scenarios in the analysis process.
- The approach does not describe how safety and security teams share information with each other in order to detect conflicts among safety and security constraints.

PROPOSED WORKFLOW

- Identify the safety and security constraints using STPA and NIST
- Verify whether the satisfaction of a safety constraint affects a security constraint, and vice-versa.
- When conflicts arise, change or redesign the system components.
- If constraints do not conflict, then a design that satisfies both sets is safe and secure

PROPOSED WORKFLOW

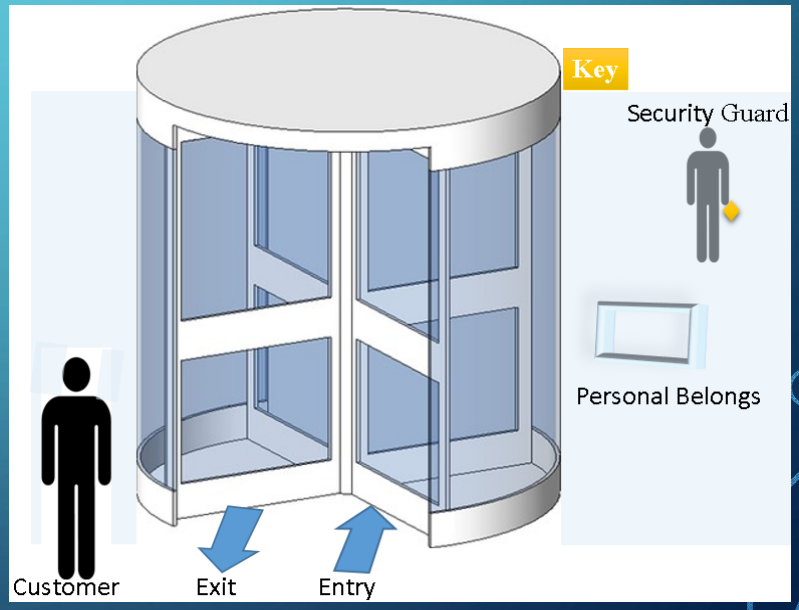


DEFINE SYSTEM GOALS AND ITS CONTEXT

- Activity that establishes a context for the safety and security assessment.
- Context includes identifying the purpose and scope of the assessment and identifying assumptions and constraints associated with the assessment, system boundaries.

REVOLVING DOOR SYSTEM (RDS)

- Provide secure access safely
- Three components: Revolving Door, Repository and Guard



STPA

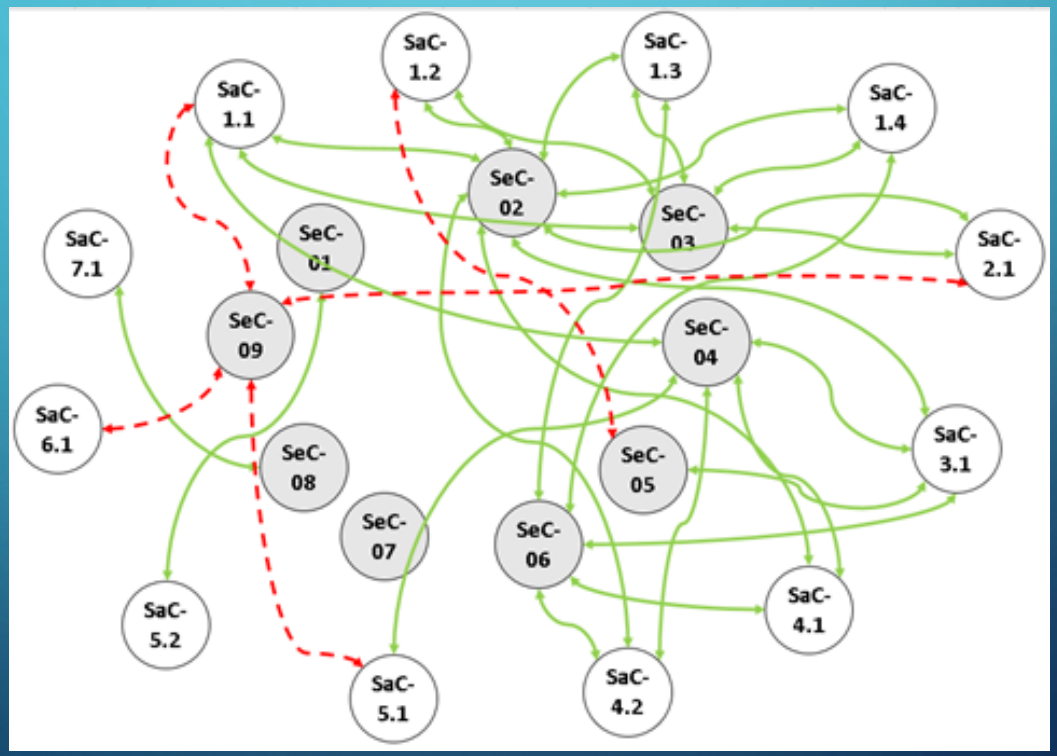
- Identify accidents
  - People burnt
- Identify hazards
  - People held in the building during a fire
- Elaborate safety control structure
- Identify unsafe control actions: 12 safety constraints
  - SG must remotely provide unlock door command when there is an emergency -> Procedure
- Identify causal factors and scenarios
  - Failure of the actuator to unlock door -> Reliability
  - Failure of the emergency siren -> Reliability

NIST

- Identify threat sources and events
  - Armed robber inside the building
- Identify vulnerabilities: 9 security constraints
  - Communication lines must be protected for confidentiality and integrity
  - RDS must have procedures to monitor portable objects
  - RDS must never release revolving door during emergency
- Determine security control, adverse impact and risk
- Maintain and monitor risks

PERFORM INTEGRATED ANALYSIS

- Analyze the relationship of constraints: reinforcement and conflict: 12 SaCs and 9 SeCs



PERFORM INTEGRATED ANALYSIS

- Analyze the relationship of constraints: reinforcement and conflict

SaC-1.1: SG must remotely provide unlock door command when there is an emergency.	
SeC-01: RDS must be set up with the correct parameters.	No relation
SeC-02: Employee must be satisfied with his job.	SeC reinforces SaC
SeC-03: Communication lines must be protected for confidentiality and integrity.	SeC reinforces SaC
SeC-04: SG must never be absent of workplace.	SeC reinforces SaC
SeC-05: RDS must have policies to release armed authorized persons to get in the bank branch.	No relation
SeC-06: RDS must have procedures to monitor portable objects.	No relation
SeC-07: RDS must have redundancy for critical activities.	No relation
SeC-08: Electrical system must never be interrupted when the system is ON.	No relation
SeC-09: RDS must never release revolving door during emergency.	SeC conflicts with SaC

SOLVE CONFLICT

- Conflict occurs when the entities have opposing interests.
- Try to refine constraints for the entities to avoid conflict:
  - In a safety emergency, exit must be allowed whereas entry should be controlled (to allow the entrance of firefighters).
  - In a security emergency, exit should be controlled whereas entry should be prohibited.
  - For security and/or safety emergency, exit should be controlled (more restrictive) whereas entry should be prohibited (more restrictive).

SOLVE CONFLICT

- Refinement of constraints:
  - SaC-1.1 "*SG must remotely provide unlock door command during an emergency for customer/employee in the exit lane*";
  - SeC-09: "*RDS must never release revolving door during an emergency for customer/employee in the entry lane*".
- Constraints do not conflict with each other if we assume that there are two separate lanes.

DEFINE COUNTERMEASURES

SaC-1.1 (re-written): SG must remotely provide unlock door command when there is an emergency for customer/employee in the exit lane.			
SeC-02: Employee must be satisfied with his/her job	SeC reinforces SaC	CM01: Employee should periodically perform psychological examinations.	P
SeC-03: Communication lines must be protected for confidentiality and integrity.	SeC reinforces SaC	CM02: Data transmitted through the communication lines between revolving door and remote control should be encrypted; CM03: Before start communication, the revolving door should authenticate the remote control.	C
SeC-04: SG must never be absent of his/her workplace.	SeC reinforces SaC	CM04: Company should have at least two SGs during a period in order to allow the replacement of the SG in the workplace.	P
SeC-09 (re-written): RDS must never release revolving door during emergency for customer/employee in the entry lane.	No relation	CM05: Company should provide guidance to reinforce that the SG should provide command when there is an emergency for customer/employee in the exit lane and there is nobody in the entry lane.	C

SAFETY AND SECURITY DOSSIER

- Documents the safety and security constraints and the resulting countermeasures/recommendations.
- Must also be updated after the safety team has performed the analysis of the causal factors and scenarios (Step 2 of STPA) and the security team has determined the adverse impact and risks.

DISCUSSION & CONCLUSIONS

- Current approaches do not address conflicts and reinforcements in an integrated manner combining current safety and security processes.
- In our approach, the processes are integrated with little modification and conflicts are identified and solved.
- Currently we working on a case study: Flight Management System
- Elaborating a technique to automate detection of conflicts
  - Require formalism to model the system.
- We are building a tool to make safety and security analysis using STPA and STPA /Sec.
  - Rules to specify hazardous states
  - Perform Step 2 of STPA.
  - Language to specify constraints
  - Analyzer of conflicts.

THANK YOU!

Questions?

Celso Hirata

hirata@ita.br