SECURING THE SKIES:

IN REQUIREMENTS WE TRUST

Bashar Nuseibeh | Charles B. Haley | Craig Foster

SEPTEMBER 2009

Presenter: *Or Shachar or12@cs*

***Computer* 42(9), pp. 64-72**

The Open University

Bashar Nuseibeh, PhD

***The Open University* (UK)**

- **Software Engineering chief scientist**

  The Irish Engineering Research Center
- **Head of software engineering lab**

  Imperial College London
- **Fellow:**

  Automated Software Engineering.

  British Computer Society

  Institution of Engineering and Technology

The Open University

Charles B Haley, PhD

***The Open University* (UK)**

- **Teacher**

  Many areas of CS
- **Researcher**

  Representation of Security Requirements

  Argumentation

  *Digital Forensics**

NATS

Craig Foster, Mr.

National Air Traffic Services (NATS)

- **Navigation & Surveillance Researcher**
- **Project Manager**

  Eurocontrol CASCADE program *

Complex system security

- **Security is much about understanding the context in which the system operates as it is about the systems themselves.**
- **A sociotechnical system compromises hardware, software and people.**
- **It is users and their assets that are harmed from an attack on the system.**

Complex system security

Organizations must look beyond the system to examine:

- **WHAT they are trying to protect?**
- **WHY they are trying to protect it?**
- **CONSEQUENCES of inadequate protection**

(Security) requirement engineering considers those questions and elicit the

SECURITY REQUIREMENTS

Security Requirements

Part of security requirement engineer challenges:

- **Identify stakeholders**
- **Wider problem scoping**
- **Representation of security requirement**
- **Requirement analysis**

Like other requirements, security req. should not be too general nor overly specific

Framework for finding the right SR

Quality / Business goals

ID System context & Functional Requirements

Infeasible

(REVISE)

Feasible

Infeasible

ID Security Goals

(REVISE)

(REVISE)

Feasible

ID Security Requirements

Infeasible

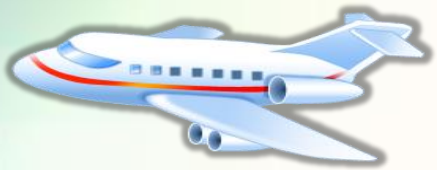
Feasible

Construct Satisfaction Argument

Feasible

Infeasible/
Secondary SG needed

CRYSTAL UK Project
[passive surveillance]

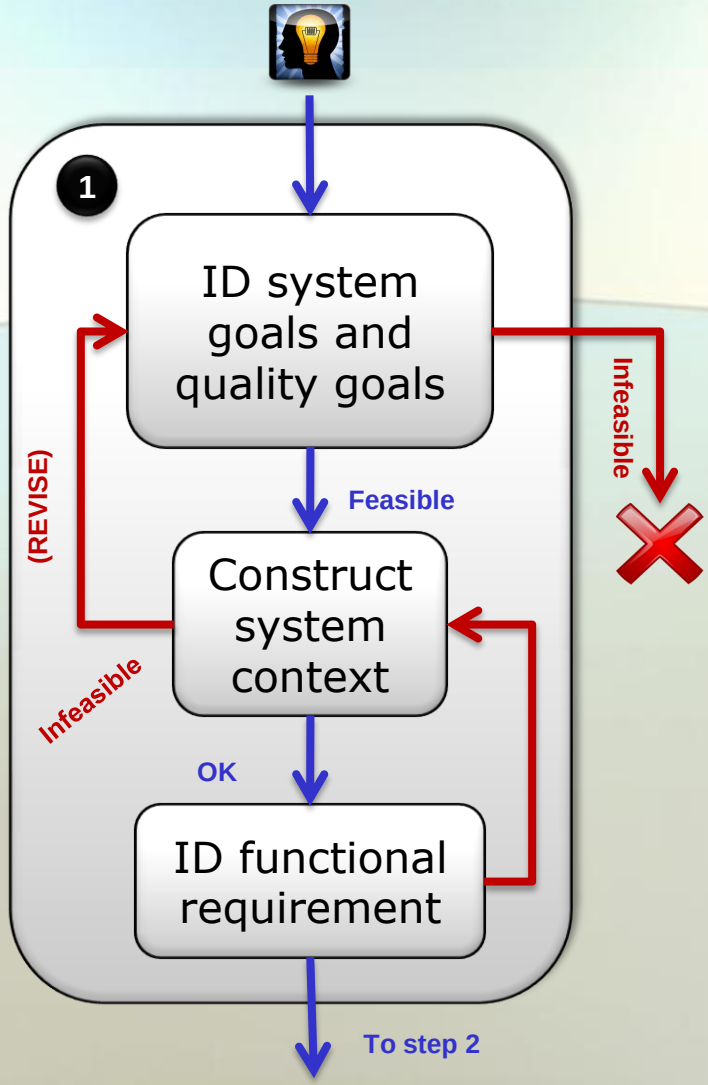


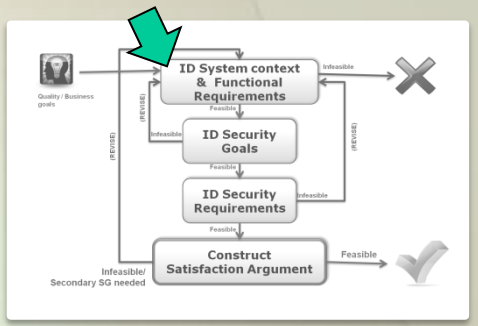
Air Traffic Control (ATC) – need of exact position and altitude of aircraft at any given moment.

THE OLD METHOD **Ground RADAR** (Active surveillance)	THE SUGGESTED METHOD **Aircrafts' GPS** (Passive surveillance)
▪Aircraft equipment independent ▪Expensive	▪Aircraft equipment dependant ▪Advanced, cost saving

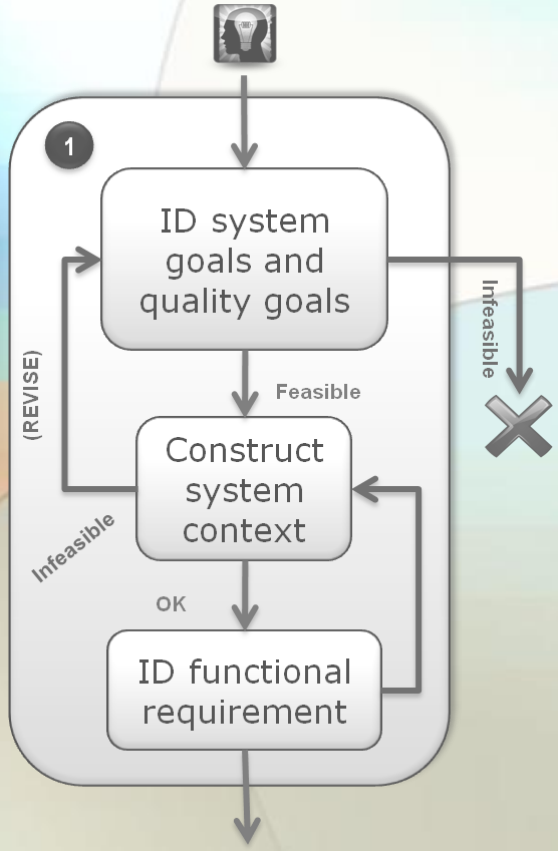
What are the suggested method security requirement?

Step1: Produce Functional Requirement





Step1: In action



System goal was already given:

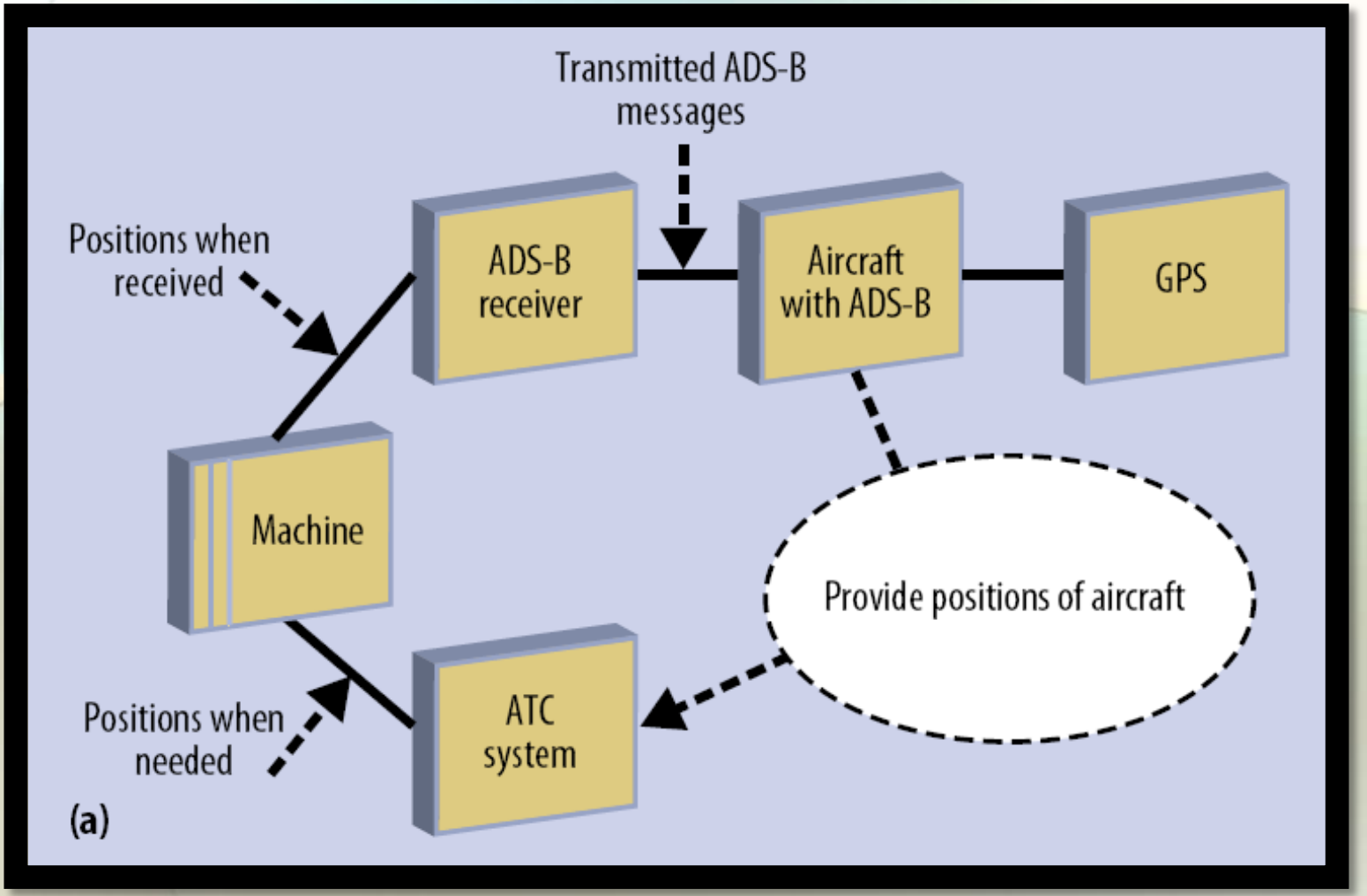
"Provide safe and efficient air traffic management."

Existing equipment:

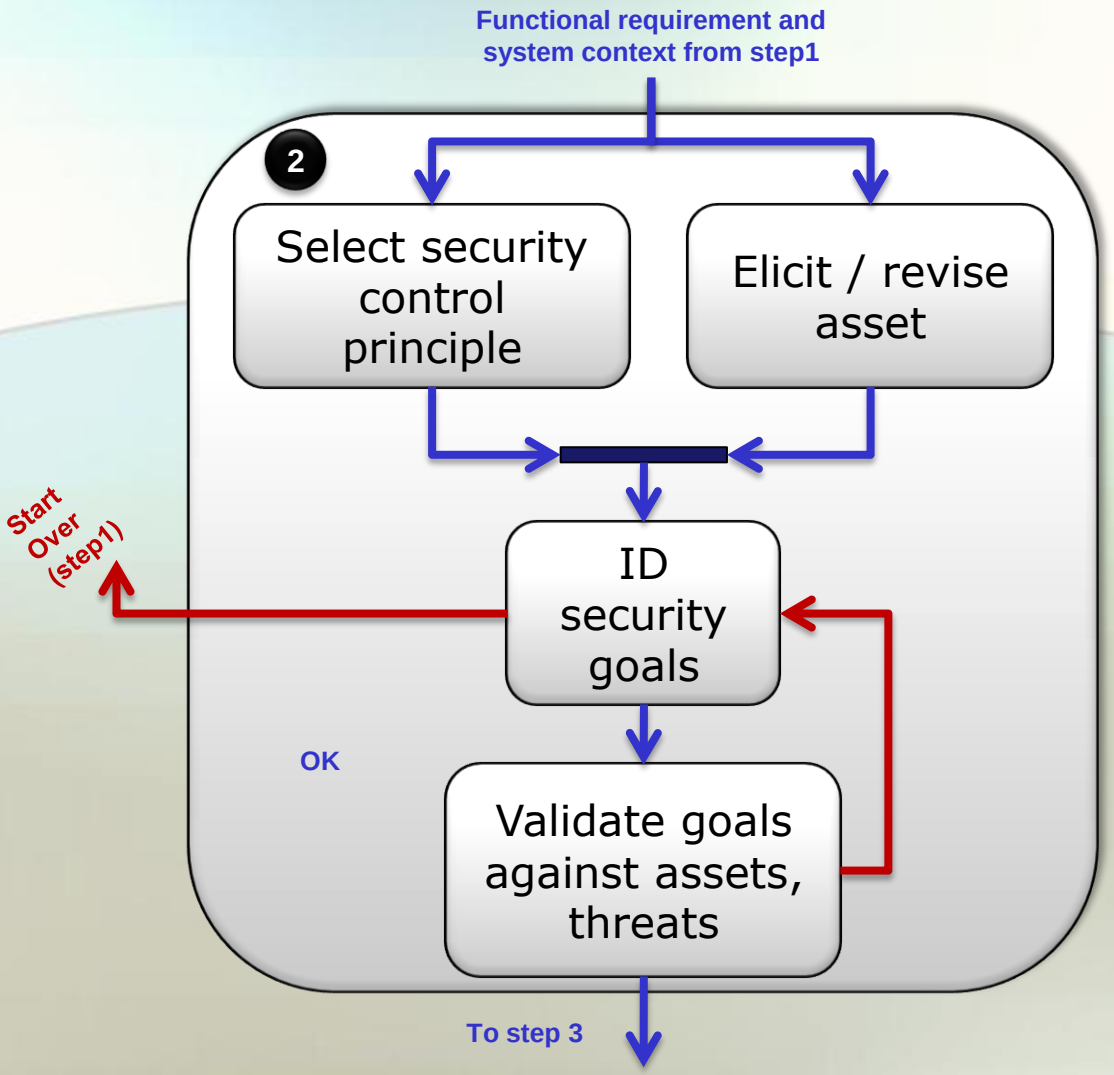
ADS-B equipment

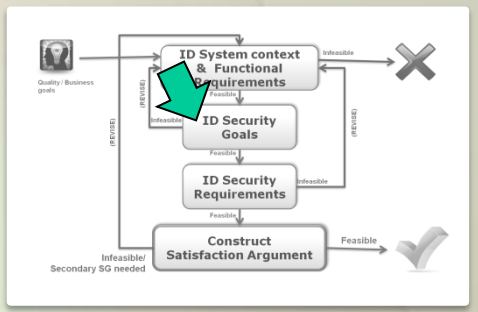
➔FR: **provide position of aircraft**

Step1: Example of system context

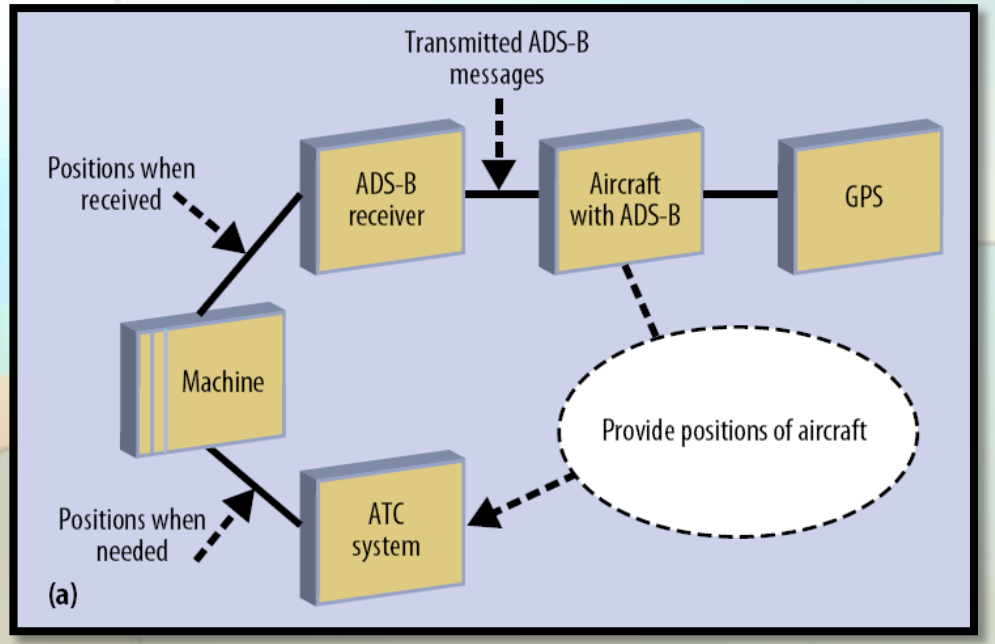


Step2: Produce Security Goals





Step2: Example Assets Mapping



Passengers

Signals

Aircraft

Airport

Ground receiver

Items around ATC systems

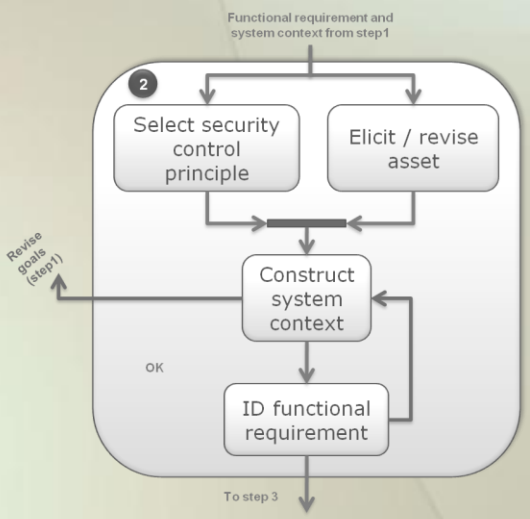
Step2: In action

Security principles:

Confidentiality | Integrity |Availability

➔Formal Threads representation

i.e: T3:{~correct, airplanes' position, lost revenue due to increased separation}

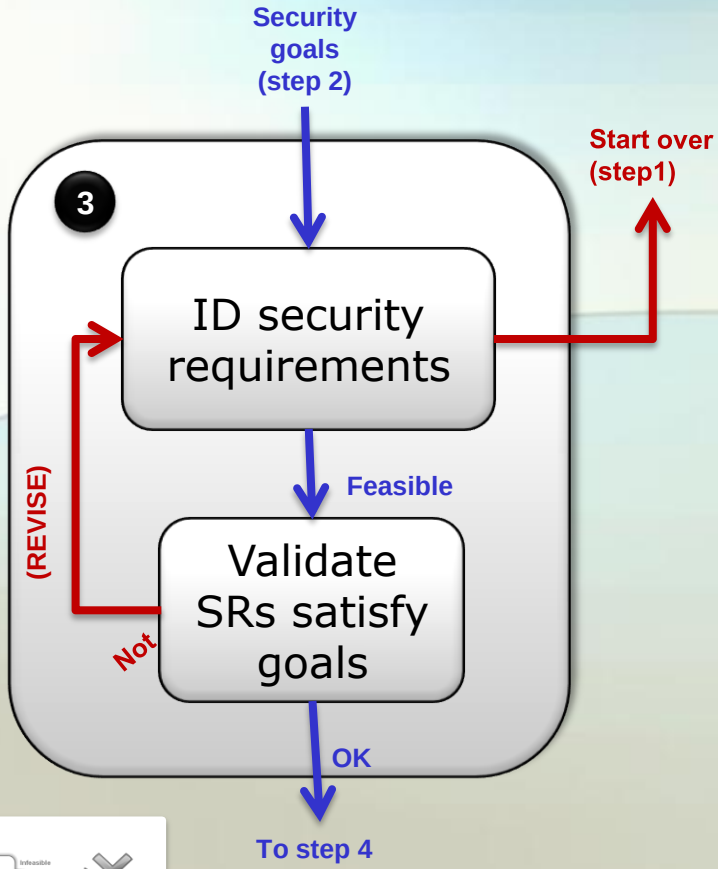


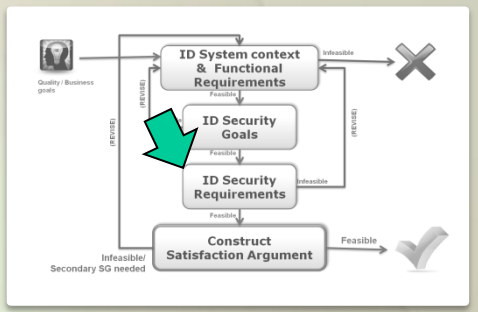
Security goals:

-Have correct positions

-Report positions as often as needed

Step3: Produce Security Requirements





Think of constraints to place on functional req. to that will satisfy the goals.
[Very immediate]

Step3: in action

Security goals:

-SG1: Have correct positions

-SG2: Report positions as often as needed

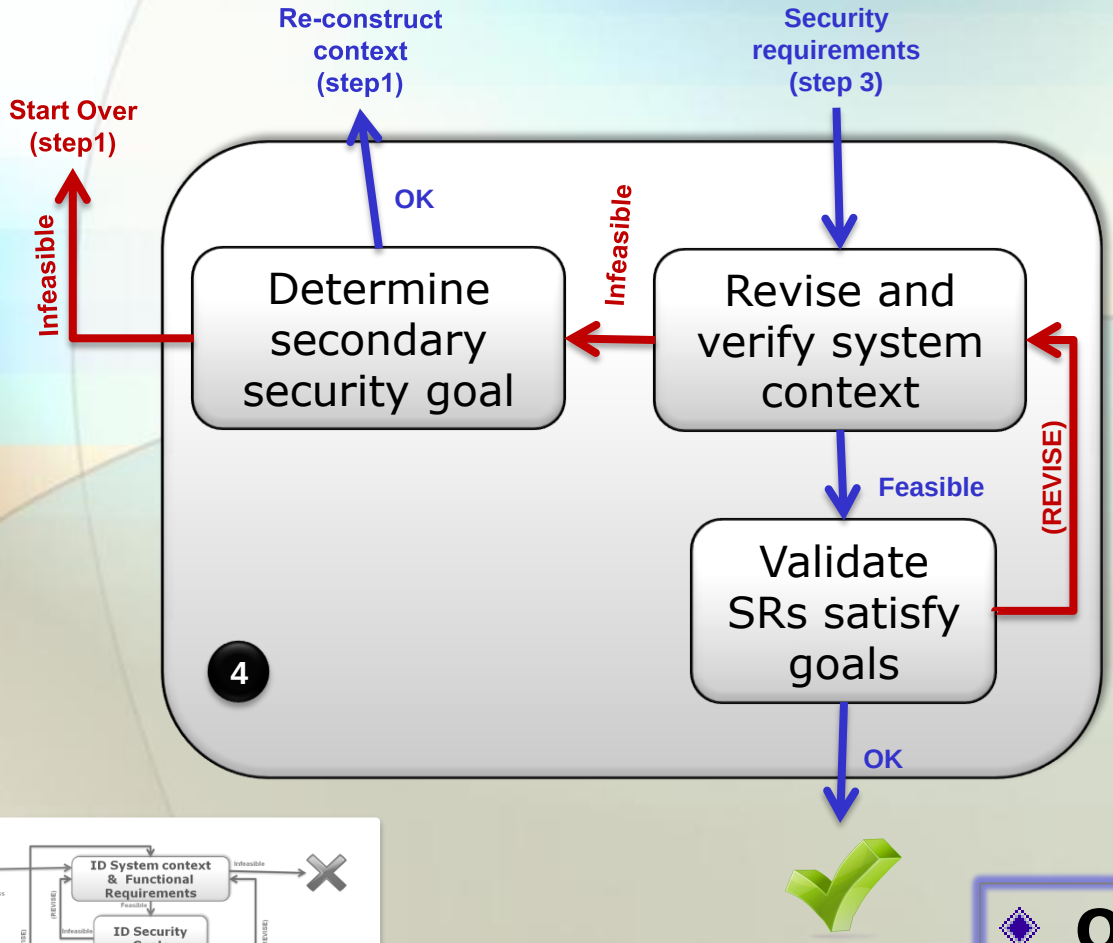
Security requirements:

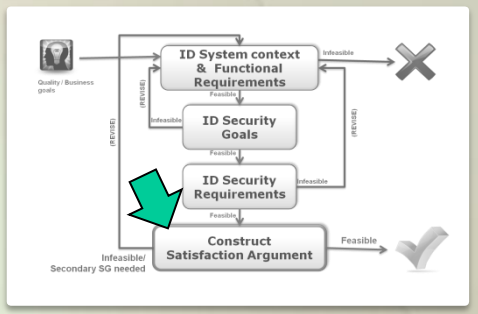
[On FR1: Provide position of aircraft]

-SR1: Positions shall be accurate

-SR2: Positions shall be timely

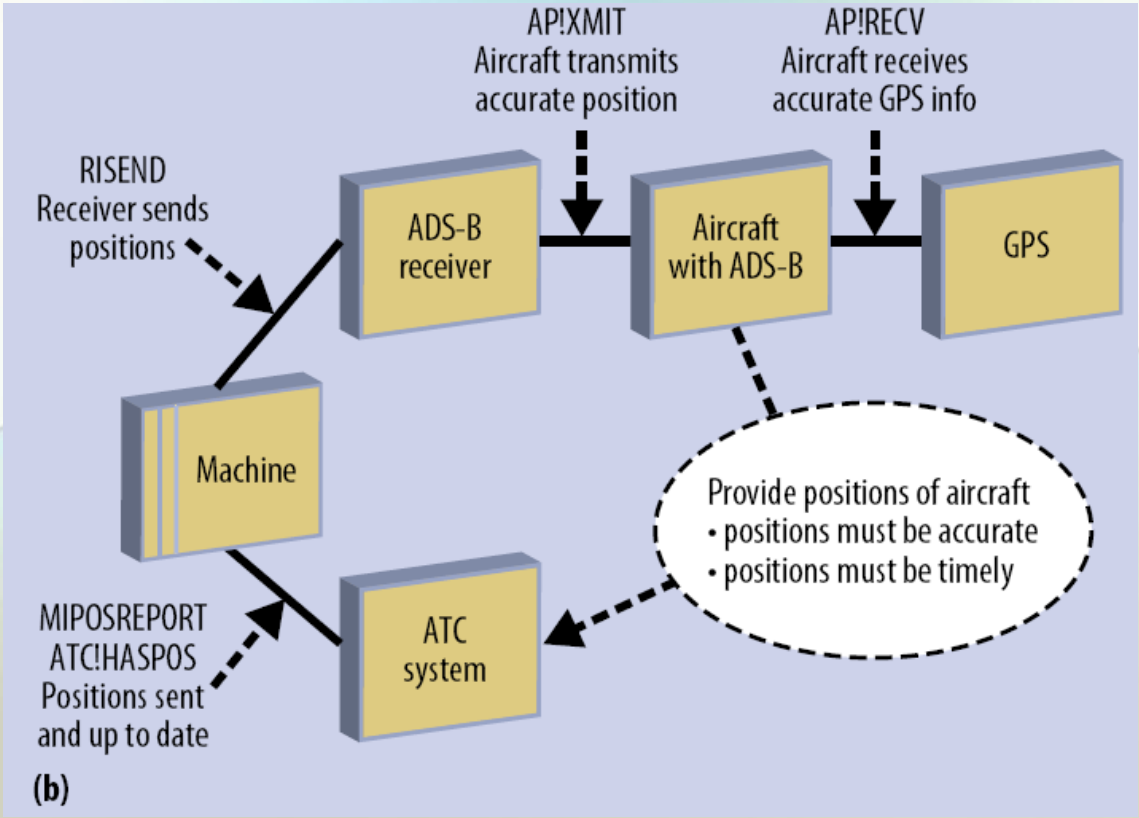
Step4: Validate Satisfaction Ability





- **Outer argument**
- **Inner arguments**

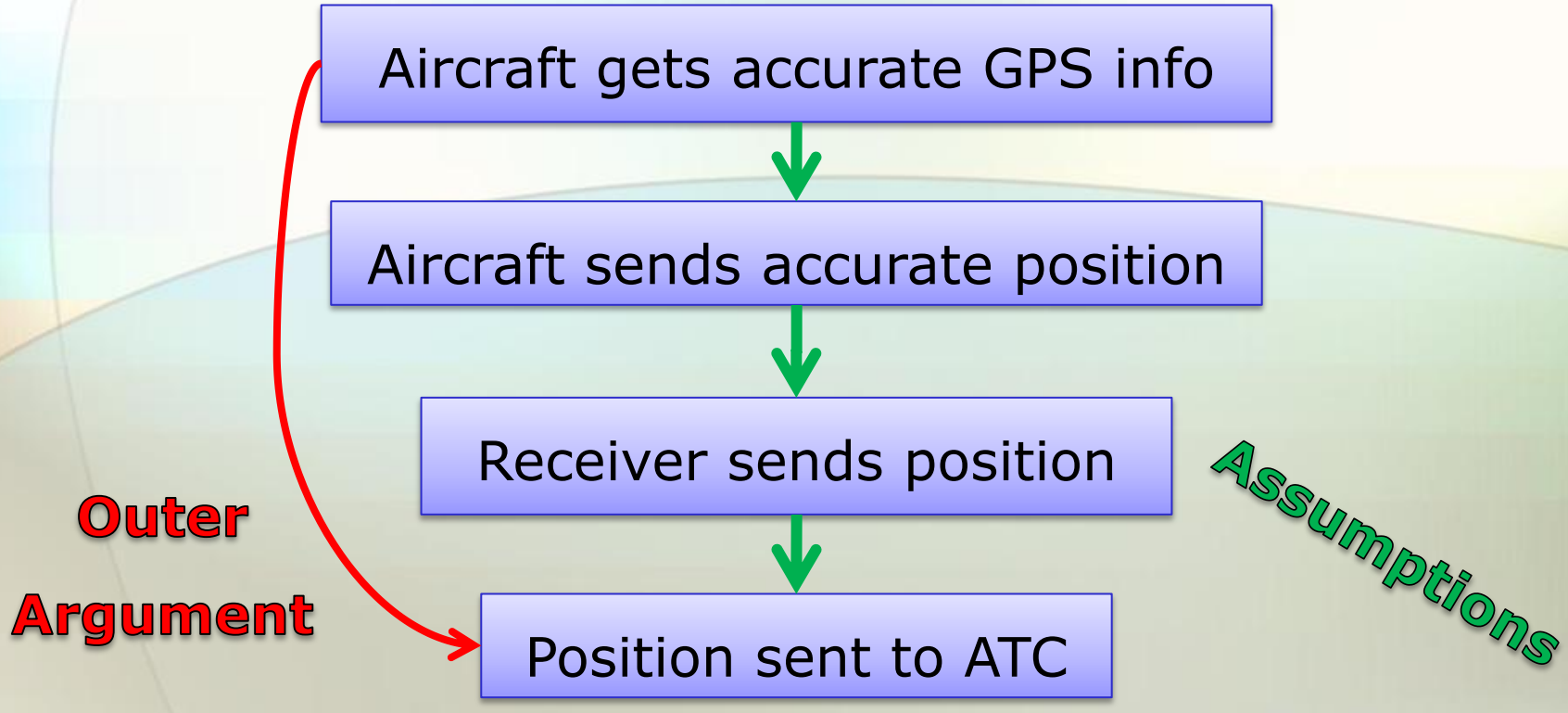
Step4: In action



Outer argument:

Aircraft gets accurate GPS info → Position sent to ATC

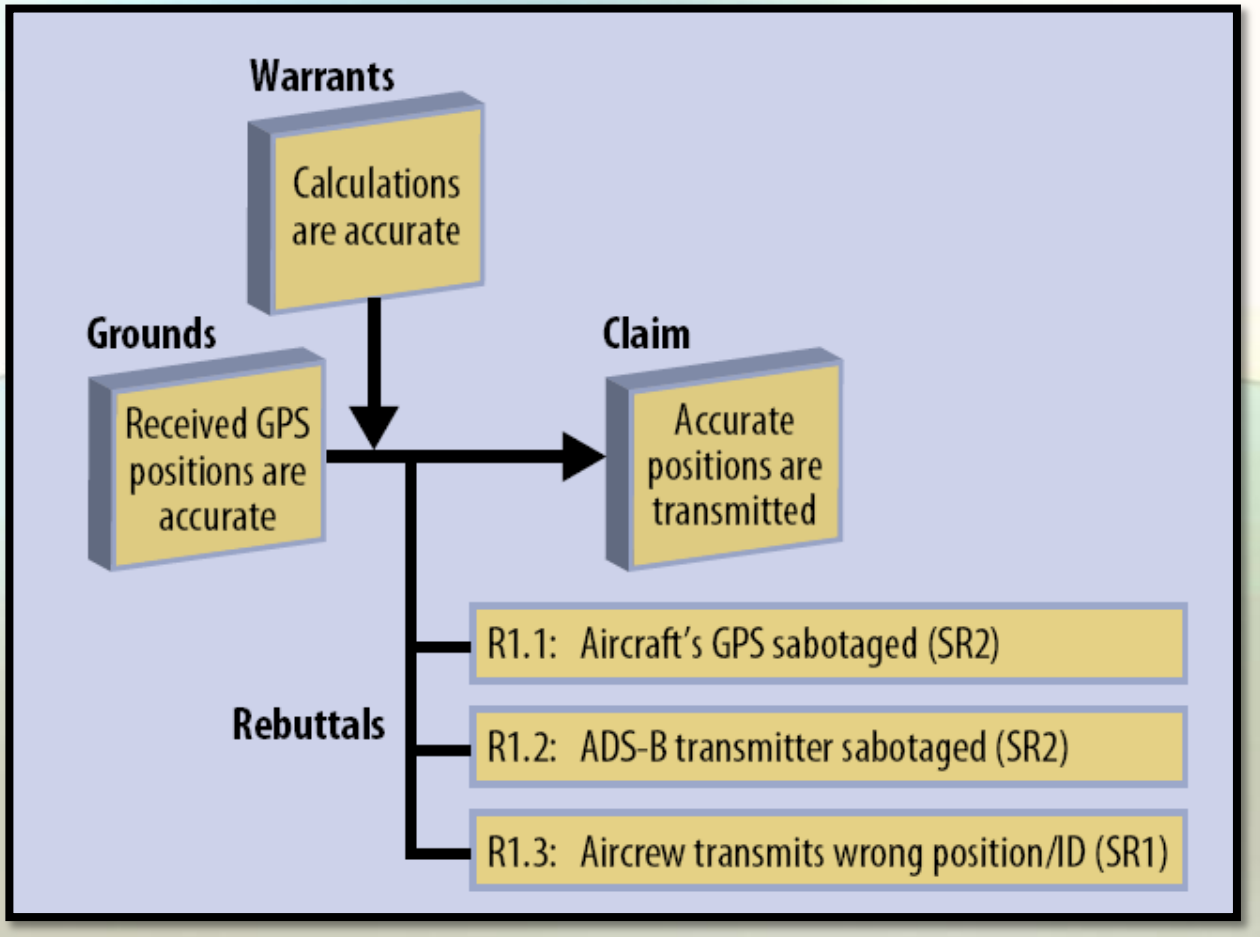
Step4: List of terms for outer argument



Step4: Assumption test example

Aircraft gets accurate GPS info

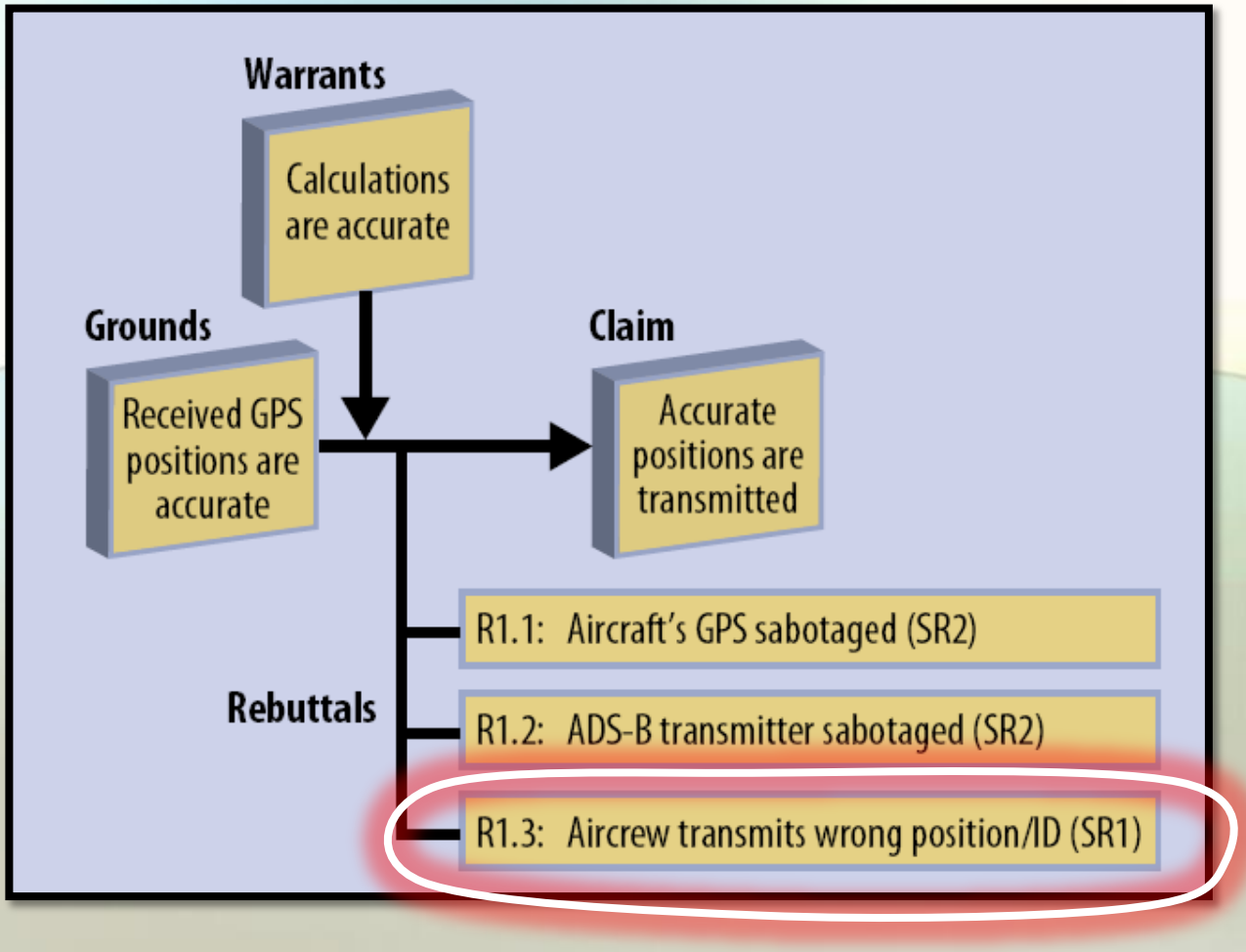
Aircraft sends accurate position



Step4: Assumption test example

Aircraft gets accurate GPS info

Aircraft sends accurate position

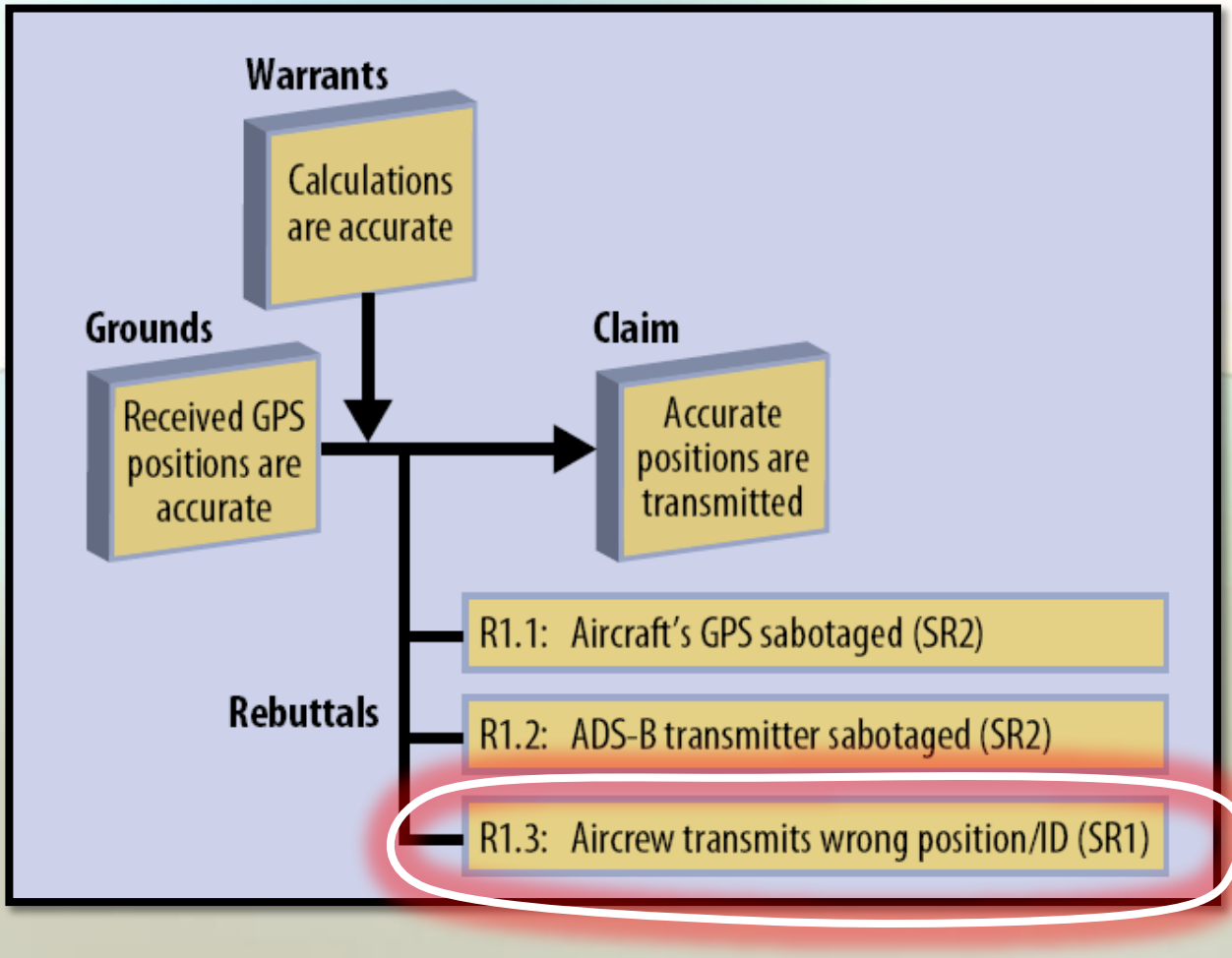


Possible terrorist attack – must be addressed!

Step4: Assumption test example

Aircraft gets accurate GPS info

Aircraft sends accurate position



Possible solution: Multilateration

Lesson Learned

- **Use domain experts**
- **Use domain non-experts** (Remember D. Berry)
- **Scope the problem** (WIDER than you might think)
- **Iterate to mitigate**
- **Formalize but argue informally too.**

security is much about being persuaded "beyond reasonable doubt" that a system is secure than it is about a proof of security, whatever that means

Summary and Discussion

Better Req. → Better system

Better security Req. → Better secured system

- **Powerful tool** – Intelligent requirement

  Proof of security

- **Security is more and more important**
- **"Secure" – against lost of assets**

  against possible attacks (Thompson)

- **Learn more: Security principles, "legally secured"**

Questions?