Cyber-Argus: Modeling C2 Impacts of Cyber Attacks

Alexandre Barreto

Instituto de Controle do Espaço Aéreo

São José dos Campos, SP - Brazil

barretoabb@icea.gov.br

Paulo Costa, Michael Hieb

C4I Center - George Mason University

Fairfax, VA - USA

[pcosta, mhieb]@c4i.gmu.edu

Summary

- Cyber-ARGUS Framework
- Case Study: Campos Basin Scenario
- Simulation Testbed
- Preliminary Results

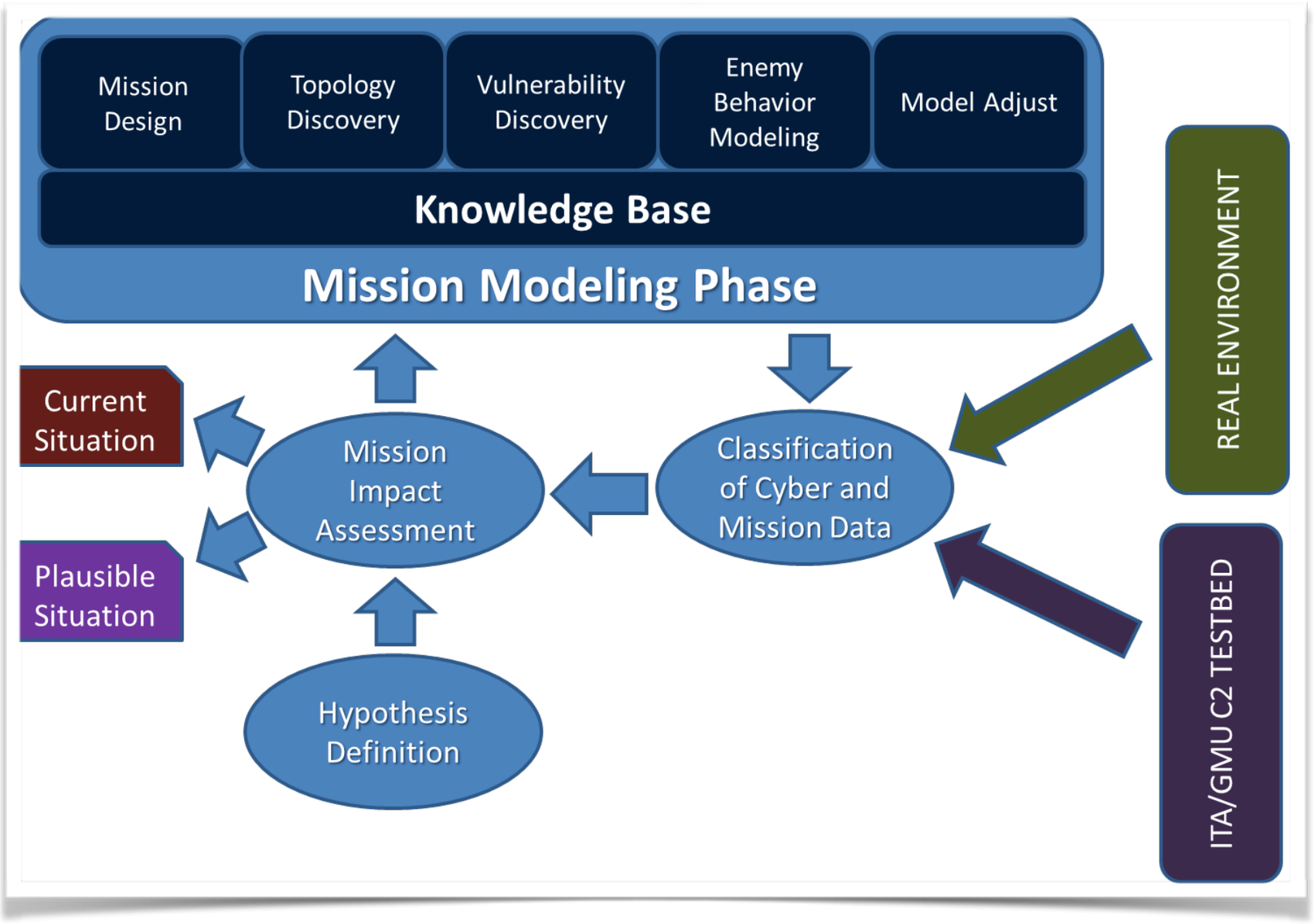
Premises

- Modern society is increasingly dependent on technology
- Cyberspace is a new way to conduct wars, similar to previous ground, air or sea combat
- Operations in cyberspace require:
  - Identifying the main events in space and time
  - Understanding how cyber threats would affect critical infrastructure
  - Responding with a suitable Course of Action
- Situational Awareness is key to succeed
  - Producing a view that integrates Mission and Cyber Tasks perspectives is a complex endeavor

Our Approach

- To achieve *situation awareness* by assessing how actions in the cyber domain affect events in the physical domain
  - The work presented here involves a methodology, a use case, and preliminary results that illustrate our Cyber-Argus framework
  - The framework is comprised of a suite of key technologies that together enable identifying and defeating cyber threats acting against an ongoing mission
- Our focus is on protecting the vital Information Technology (IT) assets during critical phases of the Mission, rather than protecting the entire IT infrastructure

Cyber-ARGUS Framework



Cyber-ARGUS links mission information to network information, as a means to assess impacts of cyber actions to critical infrastructure

Related Work

- Most used approach: to detect intrusions and system attack paths using a set of distributed sensors in the network
  - Relevant work include Denning (1987) and Bass (1999)
- To provide Situation Awareness (SA), it is not enough to identify attacks, but also requires a capability to understand the impact of an attack within the environment (Bass, 2000)
- Schneider (1999) uses an attack-tree approach to measure the impact

Related Work (cont.)

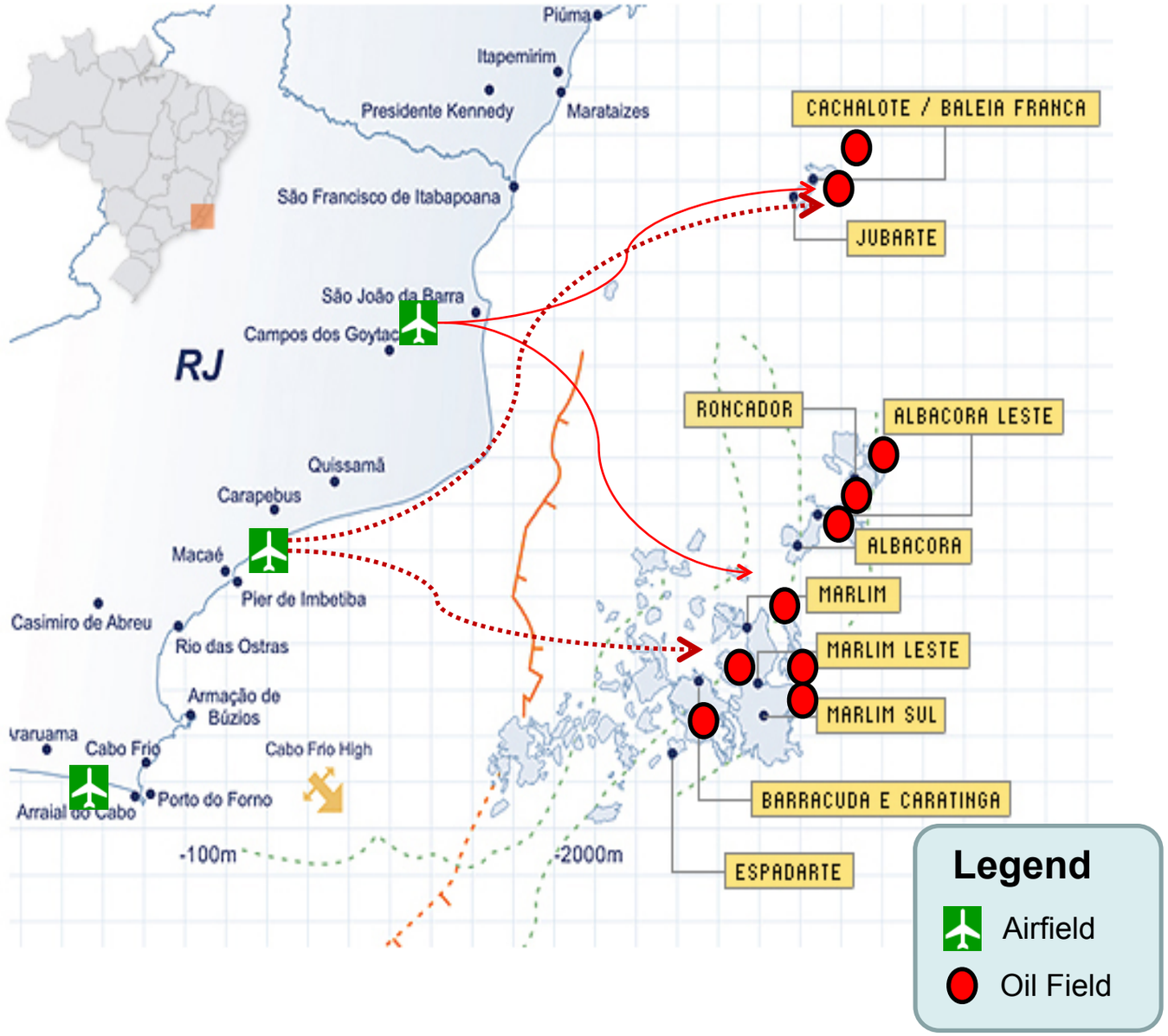
- Cauldron (Jajodia et al., 2010) transforms raw security data into attack graphs to provide a common operating picture and a concrete understanding of how individual and combined vulnerabilities impact overall network security
- Mission-Oriented Risk and Design Analysis (Evans et al., 2004) presents a methodology to develop risk assessment using information about mission, enemy and our forces
- Mission Impact Assessment (CMIA) (Musman et al., 2011a : Musman et al., 2011b) presents a general model to evaluate the cyber impact on a mission

This Research

- Started as a PhD Thesis (Barreto, 2013) that leveraged the GMU C4I Center's C2 Research Simulation Testbed, and continues to develop
- Main goals:
  - Simulate the effect of multiple cyber-attacks on a critical infrastructure
  - Understand the impact these attacks on the security and safety of the operations supported by that infrastructure
- Challenges (not a comprehensive list):
  - Develop a set of tools to adequately simulate real-time scenarios
  - Fuse physical and IT behavior in an integrated view

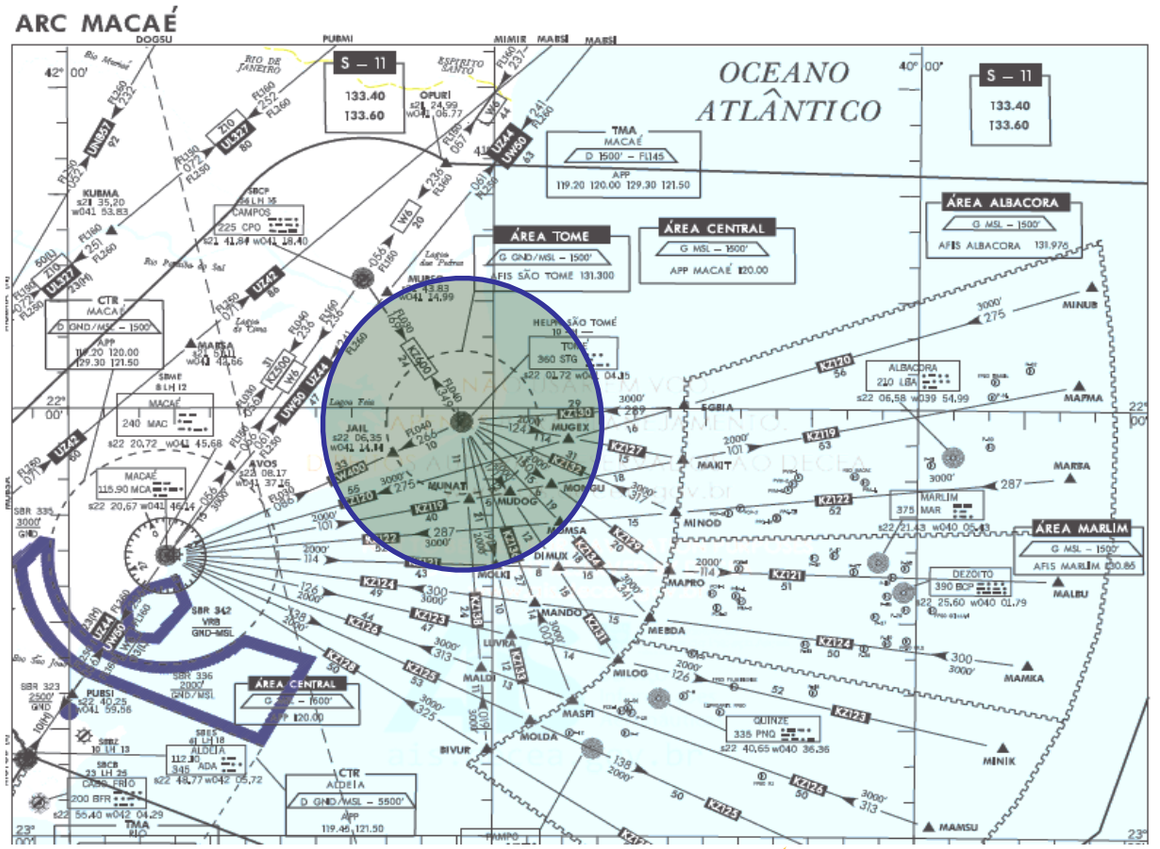
Campos Basin Scenario

- The scenario models Air Traffic Control operations in the Campos Basin.
- The Campos Basin is a petroleum rich area located in the Rio de Janeiro state, and is responsible for 80% of Brazil's petroleum production (1 million 265 thousand barrels).
- Oil development operations include heavy helicopter traffic between the continent and oceanic fields during daytime, with an average of 50 minutes per flight.



Campos Basin Scenario: Details

- The main airport in the Region (Macaé) has a Radar Station that supports the Air Traffic Service (ATS) within the Terminal Control Area (45 NM radius from the airport based at 9500 feet)
- Most oil platforms are located more than 60 Nautical Miles from Macaé and the helicopter flights are carried out at low altitude
- Therefore, the ATS provided on most of the oceanic area is based on non-radar procedures, which significantly reduces the efficiency of air operations



Campos Basin Scenario – ADS-B

GPS Track

GPS Track

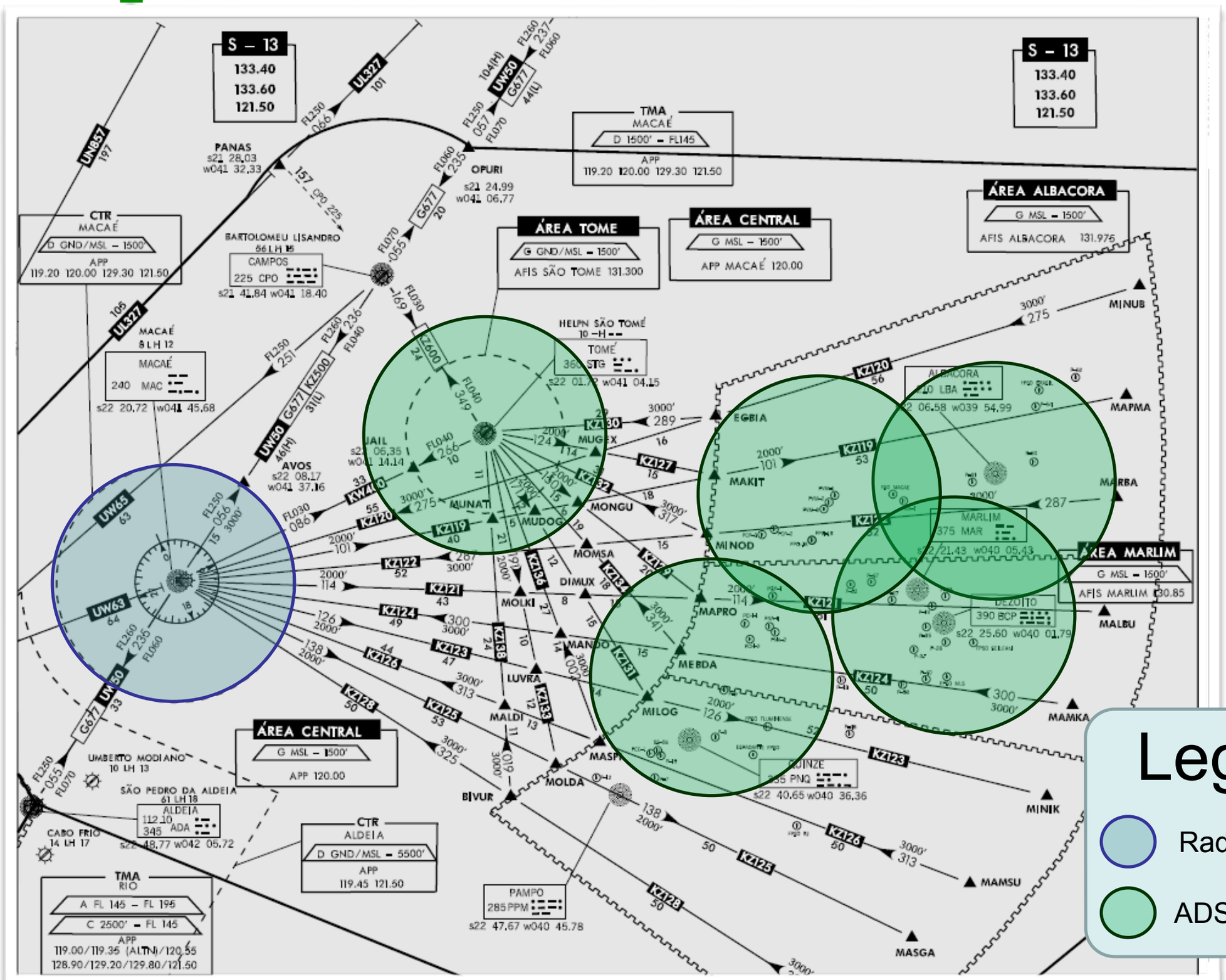
GPS Track

ADS-B
Radio Station Relay

Automatic Dependent Surveillance-Broadcast (ADS-B)

ATC Center

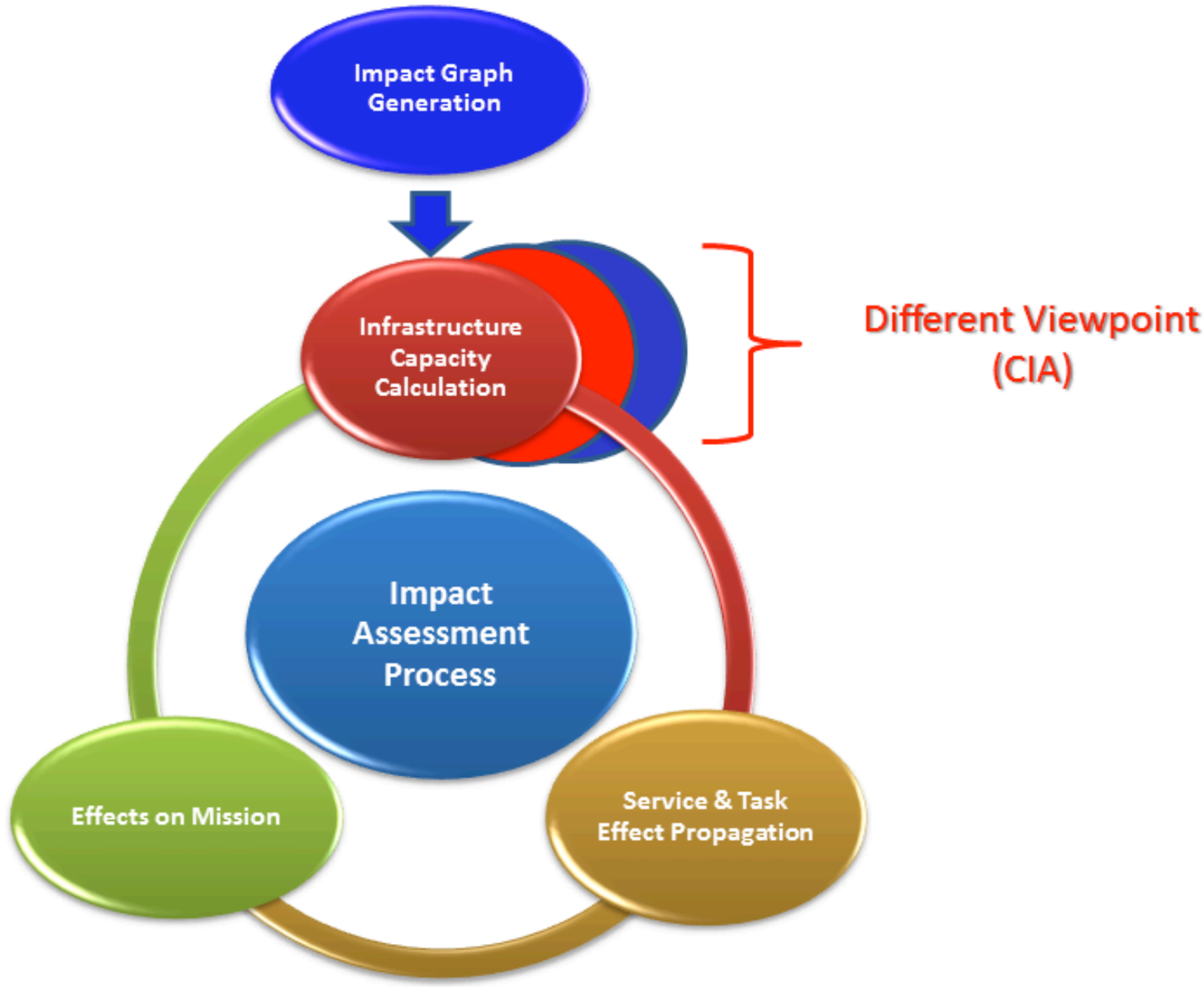
Campos Basin Scenario – ADS-B



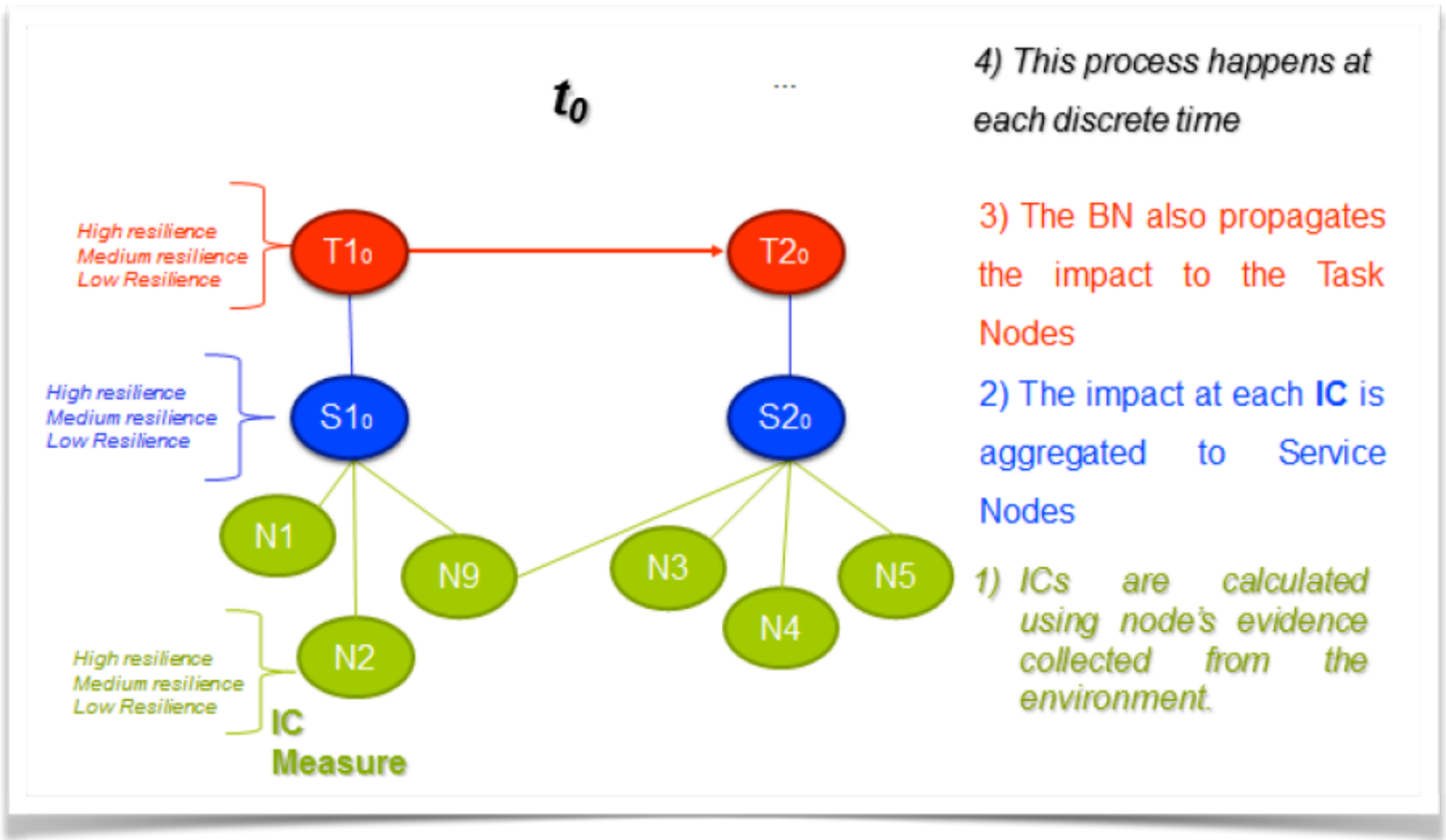
Legend

- Radar Coverage
- ADS-B Coverage

Mission Impact Assessment

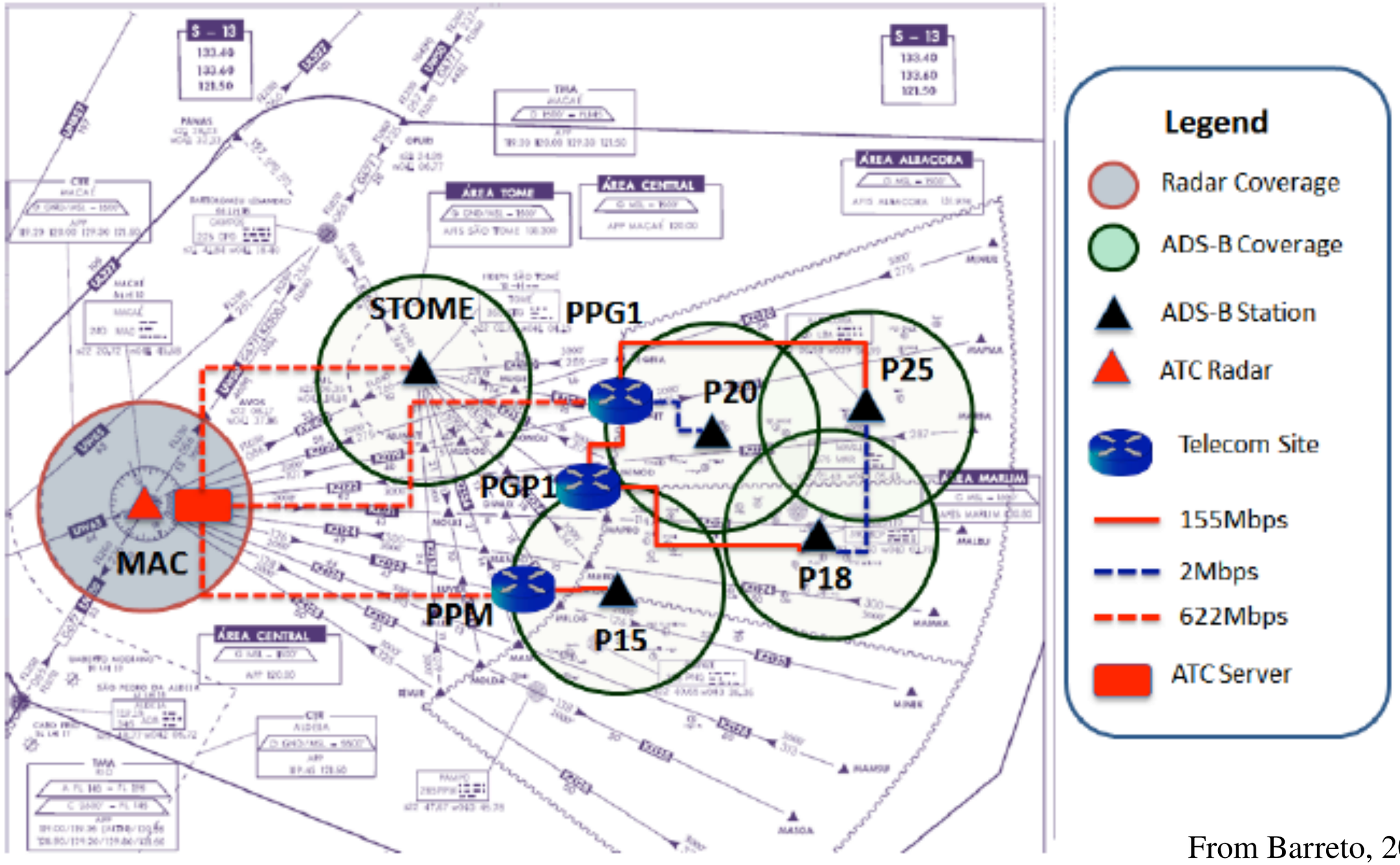


Impact Assessment with BNs



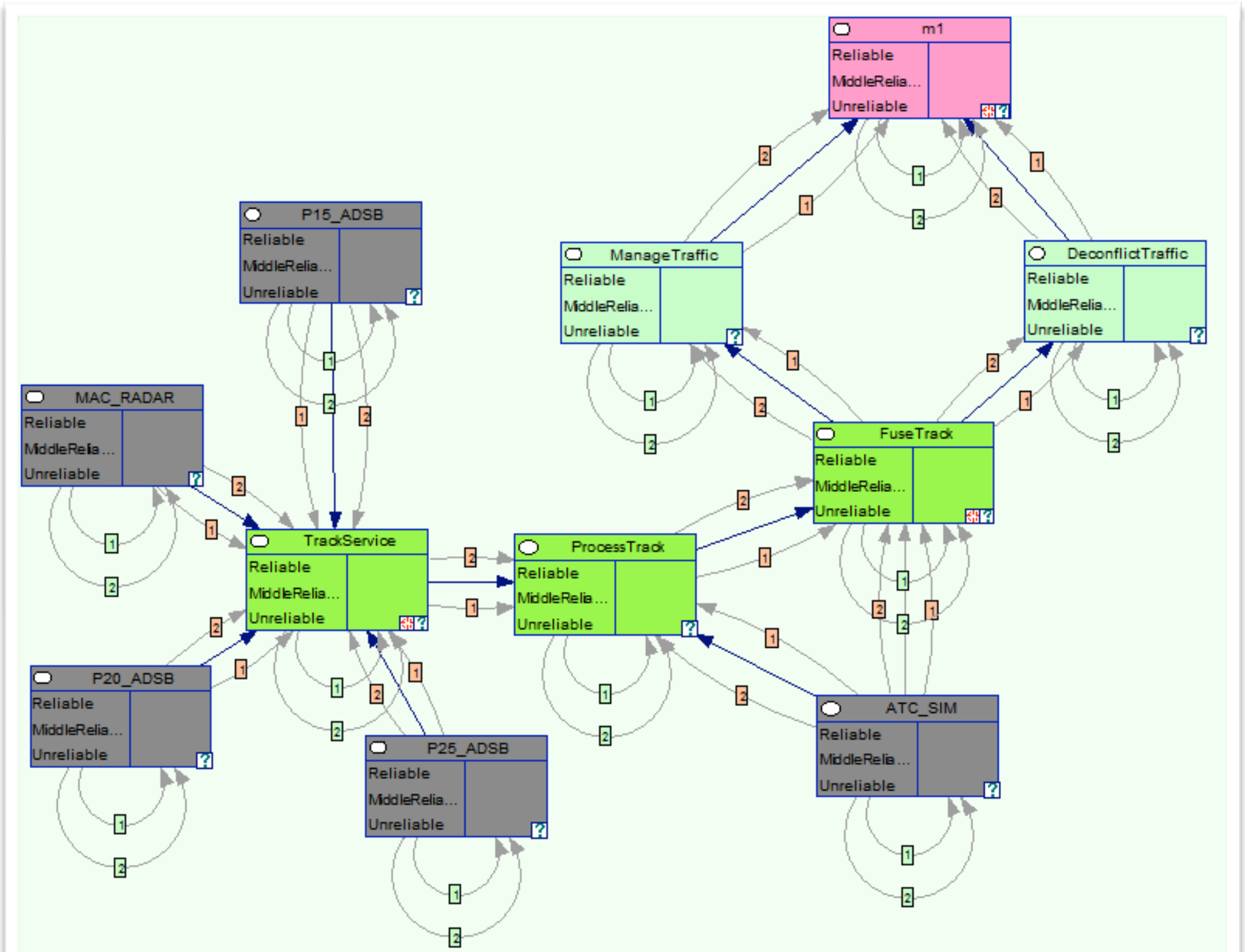
- Historic data of each node is used to infer the current belief
- Bayesian propagation ensures that each change in belief is properly computed

Experimental Design



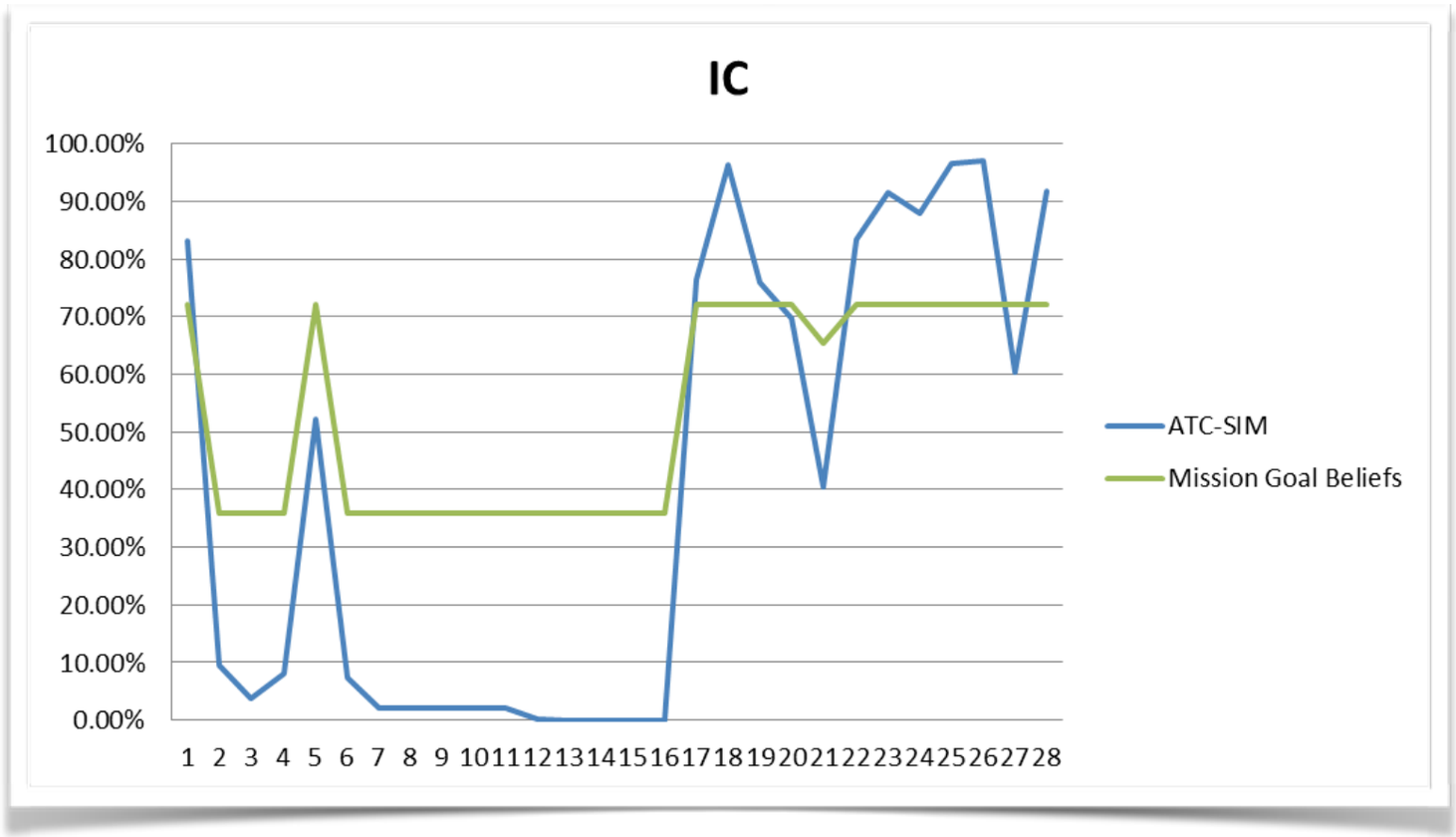
From Barreto, 2013

Impact Graph



Initial Results

- The figure below shows that ATC-SIM' infrastructure capacity decreases during UDP attacks against MAC-RADAR
  - During the slot-time when the attacks happened, aircraft were returning to continental air fields (when only the MAC-RADAR provides track coverage)
  - Thus, an attack against this sensor directly impacts the IC of the ATCSIM, since most of the information needed to perform its work is absent

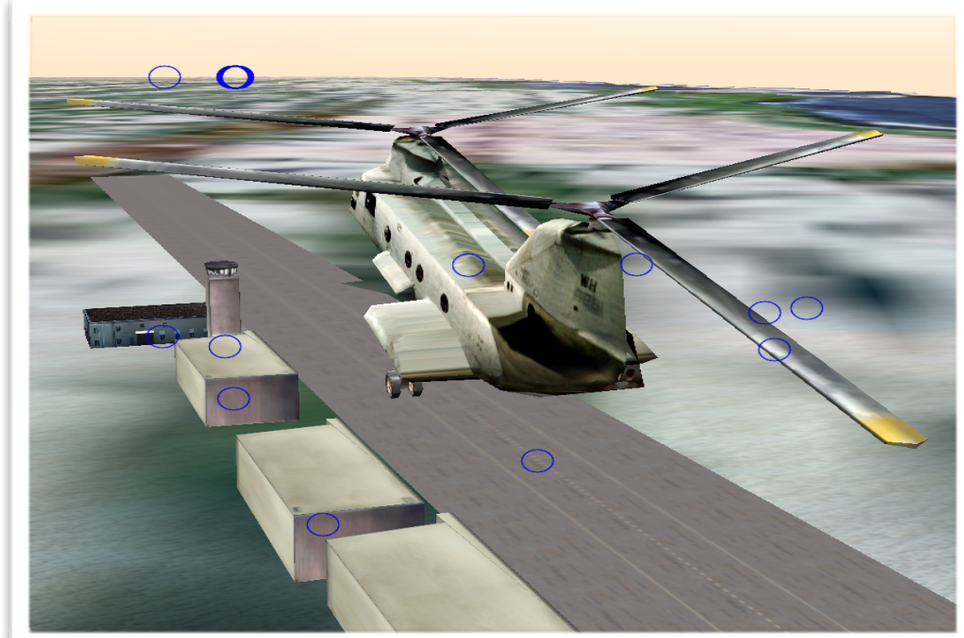


- Analyzing this graph, it is possible to see that mission goal belief follows the ATC-SIM' IC trend

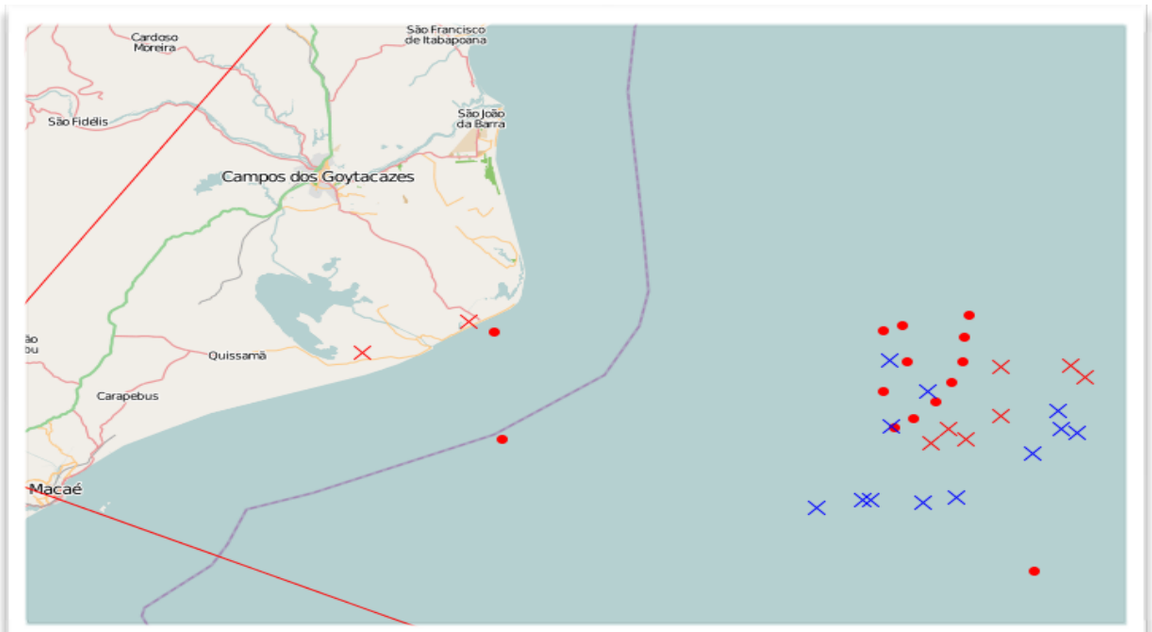
Visualizations

Tactical Visualization

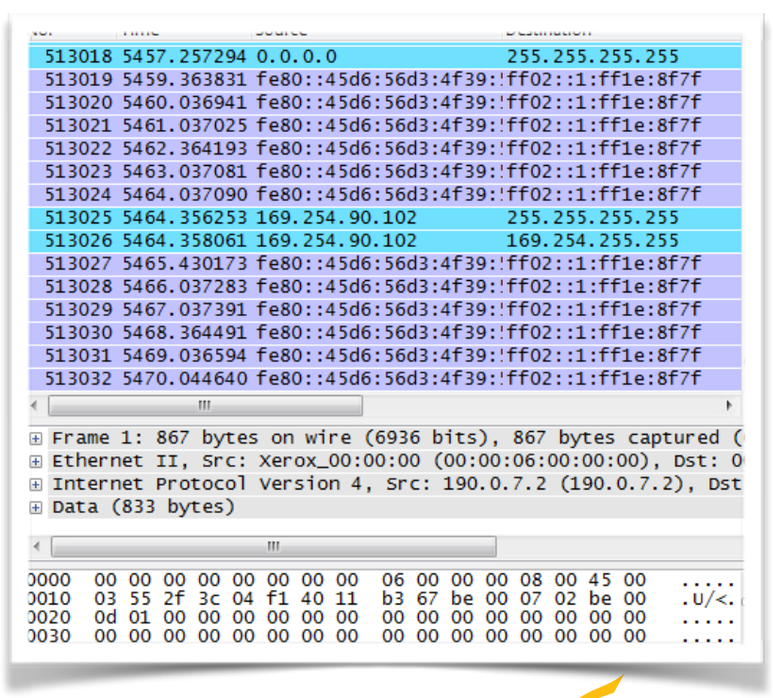
3D Visualization



ATC Visualization



Network Visualization



```
513018 5457.257294 0.0.0.0                255.255.255.255
513019 5459.363831 fe80::45d6:56d3:4f39:!ff02::1:ff1e:8f7f
513020 5460.036941 fe80::45d6:56d3:4f39:!ff02::1:ff1e:8f7f
513021 5461.037025 fe80::45d6:56d3:4f39:!ff02::1:ff1e:8f7f
513022 5462.364193 fe80::45d6:56d3:4f39:!ff02::1:ff1e:8f7f
513023 5463.037081 fe80::45d6:56d3:4f39:!ff02::1:ff1e:8f7f
513024 5464.037090 fe80::45d6:56d3:4f39:!ff02::1:ff1e:8f7f
513025 5464.356253 169.254.90.102         255.255.255.255
513026 5464.358061 169.254.90.102         169.254.255.255
513027 5465.430173 fe80::45d6:56d3:4f39:!ff02::1:ff1e:8f7f
513028 5466.037283 fe80::45d6:56d3:4f39:!ff02::1:ff1e:8f7f
513029 5467.037391 fe80::45d6:56d3:4f39:!ff02::1:ff1e:8f7f
513030 5468.364491 fe80::45d6:56d3:4f39:!ff02::1:ff1e:8f7f
513031 5469.036594 fe80::45d6:56d3:4f39:!ff02::1:ff1e:8f7f
513032 5470.044640 fe80::45d6:56d3:4f39:!ff02::1:ff1e:8f7f

⊞ Frame 1: 867 bytes on wire (6936 bits), 867 bytes captured (
⊞ Ethernet II, Src: Xerox_00:00:00 (00:00:06:00:00:00), Dst: 0
⊞ Internet Protocol Version 4, Src: 190.0.7.2 (190.0.7.2), Dst
⊞ Data (833 bytes)

0000  00 00 00 00 00 00 00 00  06 00 00 00 08 00 45 00   ......
0010  03 55 2f 3c 04 f1 40 11  b3 67 be 00 07 02 be 00   .U/<..
0020  0d 01 00 00 00 00 00 00  00 00 00 00 00 00 00 00   ......
0030  00 00 00 00 00 00 00 00  00 00 00 00 00 00 00 00   ......
```

Conclusions and Future Work

- Cyber-ARGUS enables cyber impact assessment for an ongoing mission to be achieved using overall effects
  - knowledge of enemy plans no longer required
  - It addresses the complexity and level of subjectivity involved in continuous impact assessment

- Future work involves improvement of the simulation testbed and new forms of propagation. Examples include:
  - Emulating cyber attacks with software-defined radios
  - Using Multi-Entity Bayesian Networks (MEBNs) to calculate and propagate the impact in dynamic infrastructures