Objectives of a robust and resilient CNS infrastructure

Working paper

07th March 2022

Control

Approved by	**Name** Role SDM Planning Manager	**Date** date 22/03/2022	**Signature** Signed
Reviewed by	**Cristian Pradera** SDM Planning Manager	**Date** 22/03/2022	**Signature** Signed
Prepared by	**Jan Stibor** SDM **Costas Christoforou** IFATSEA	**Date** 22/03/2022	**Signature** Signed

Table of contents

Introduction

This Working Paper presents the objectives of a Robust and Resilient CNS infrastructure. It was elaborated in early 2022 by SDM and IFATSEA in support of the activities under the scope of the CNS Advisory Group.

Objectives of a robust and resilient CNS infrastructure

- Implement an overall thoughtful and well considered architecture in the system design of CNS infrastructure to cover all scenarios of service disruptions as well as possible cascade failures, especially for distributed architecture cases. Enabling highest levels of CNS/ATM systems and service availability.

- Define Required Levels of performance (matrix) by CNS systems for specific services provision, per airspace type etc. For distributed architectures or cross border service provision, define the required Quality criteria and requirements at the various interfaces between service chain elements.

- Implement a proactive and continuous threat management mechanism which considers the broadest possible spectrum of threat origin categories: physical, technical, socio-economic, political. Nb: particular attention to be paid to centralized/cross-border/global service provision where political development in foreign state can interfere with the service provided (nationally or regionally).

- Define and implement determined degradation modes for any threat. Degraded modes meet defined requirements on performance levels and recovery duration.

- Design, Configure and Implement graceful degradation, with special consideration given to modes of degradation common between C, N, S and Surveillance Data processing systems.

- Provide concise, timely, reliable and accurate service status/level information to users and operators.

- Implement an appropriate level of autonomous recovery capability while maintaining the Human (ATSEP) in the loop.

- Consider the cumulative impact of multiple/frequent disruptions throughout the service delivery chain, from Sensor data production, distribution, processing to the ultimate application layer e.g. ATCO, PILOT or machine (FMS).

- Identify, elaborate and produce a practical Contingency framework for the Human in the loop that is shared by all actors in the service chain to enhance the Resilience of CNS and ATM systems and service delivery, irrespective of the type of actor/user/operator (ATCO, PILOT, ADSP ATSEP,..).

- In general, while elaborating on all aspects, always consider the Human factor (ATSEP) as an integral part and an enabler for system robustness and resilience. Build a matrix on their qualification, training and competence(s) required to deliver at maximum level (buy-in from other safety critical industries e.g airlines, nuclear stations, railways) for mid- and long-term technological roadmaps. Include in any study the Human in the loop, as their intervention is the last resort with a transversal impact even for non-associated systems.

- Based on the various concept and technology roadmaps, starting from the ATMMP, the AAS and with a horizon to 2035 elaborate all possible scenarios of hybrid (space and ground combined) system and services delivery models and their mitigation.

- Identify the types and the functionality of the tools that will have to be developed for the ATSEP Working Position utilizing the most appropriate types of Automation including AI, while maintaining the Human in the loop as need in the response, recovery and restoration phases. Proactive Health monitoring both for Technical and Cyber related failures.

- Develop guidance material /common requirements specification for the design of an intuitive, effective and reasonably standardized user / operator working position and HMI (ATSEP WP, ATCO WP and Pilot flight deck).

Additional considerations

Definitions:

Robustness: the ability of a system to resist a disruptive event without impact on its functions.
Resilience: the ability of a system to respond to and recover from a disruption.

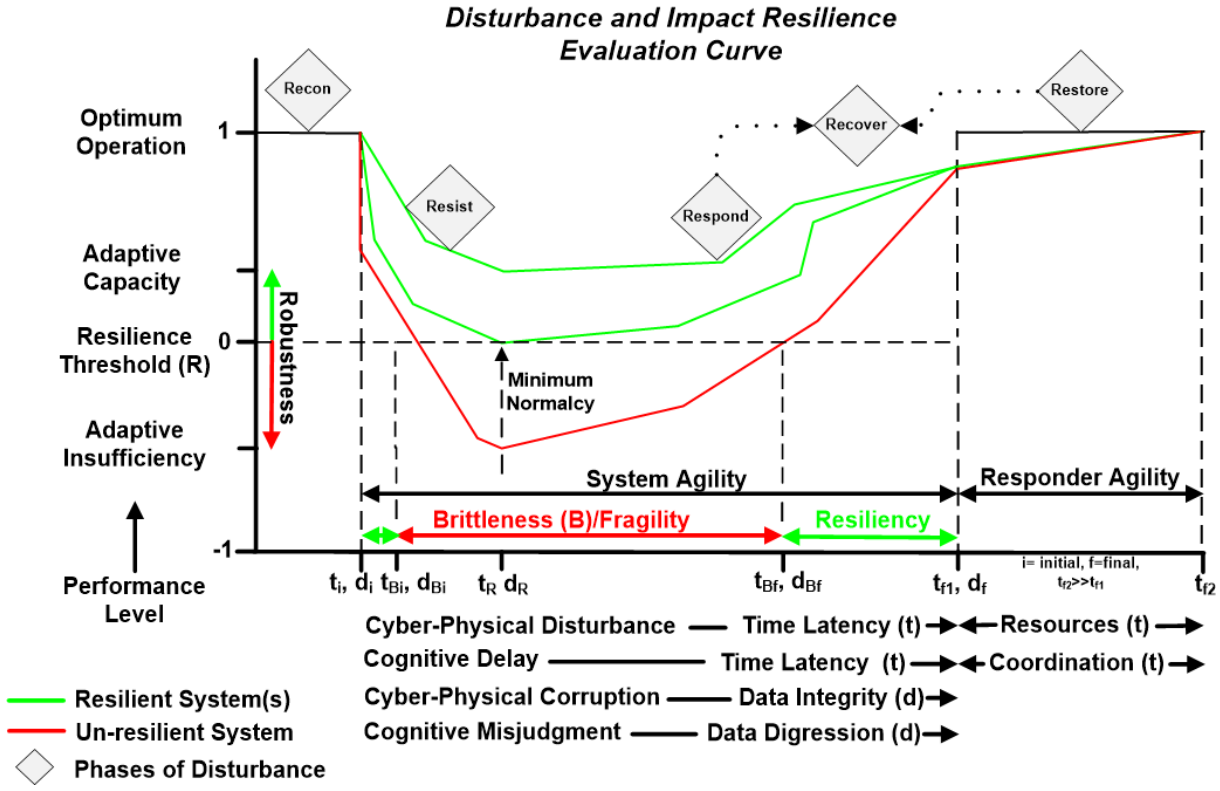

Figure 1 From Wikipedia article on resilient control systems

In generic terms, to be robust the CNS infrastructure must be able to withstand some amount of disruption to its operating environment without degrading its performance, in the full range of normal operating conditions (~ assume worst case scenario). To be resilient, the infrastructure must be able to gracefully degrade to an acceptable lower performance level/levels – which consequently need to be defined and designed for, and to recover to the nominal performance level at full range of operating conditions within an acceptable (determined and defined) timeframe.

As the CNS and ATM infrastructure is not running on its own and the Recovery phase involves the intervention of the Human (ATSEP) their competence, tools, coordination capabilities administrative (Inc. Funding) resources, logistics, staff availability, provided that many CNS stations are at remote locations subject to weather phenomena or other like RF spectrum interference, all these impact Responder Agility and Recovery time as a result.

Applied to the contemporary European CNS infrastructure, the above principle translates to the following considerations:

- What amount of disruption can C, N, and S, separately, suffer before they degrade (with and without Human intervention)?
- Where are the threats coming from?
    - Physical disasters (catastrophes) and extreme phenomena.
    - Technical
        - Internal - equipment failure, improper handling, operator error, unanticipated user behaviour
        - External – disruption of the operating environment
            - Inadvertent: Weather, disturbances in RF spectrum, terrain changes in vicinity
            - Deliberate: breach in physical and cyber security
    - Socio-economic and political – more diffuse, harder to categorize. Some examples:
        - Military crisis
            - Disruptors
                - Foreign power
                - Own national defence
        - Political crisis – in cases of cross-border or global provision, what if the state/national entity controlling some of the components in the chain, turns hostile and denies or subverts service (consider GPS), or becomes unable to deliver the service.
        - Pandemic effects leading to loss of maintenance due personnel unavailability including periodic inspections (partial to full).
        - Economic crisis – loss of operational funding or access to energy sources (electric, fossil)
- What levels can C, N and S separately degrade to?
    - What is the effect of these degradations on the ATC service provided?
    - Are there common points in the degradation? Example: loss of GPS timing affects C, N, S. Loss of GPS position affects N, S. What is the compound effect of such degradation?
    - How is the disruption discovered? (identify and research the new toolsets required for the ATSEP WP including distributed architectures e.g. AAS)
    - How is degradation level reported to operators and users? (identify and research the new toolsets required for the ATSEP WP including distributed architectures (e.g Remote towers, AAS). Include Human factors in their design and development as one of the issues in the above diagram, is Cognitive Misjudgement) . (Note: most tools for CNS for ATSEP are still in text/character mode!)
- Is the degradation graceful? What proportion of the user spectrum will retain what levels of service?
- How do C, N, and S recover, legacy and modern systems?
    - What level of human intervention is needed to recover?
        - None/remote/local
    - How competently can systems self-diagnose to discover the presence/absence of abnormal behaviour, can they isolate it? Identify and elaborate on new build in system capabilities that will enable Systems Monitoring and Control through the ATSEP WP tools and functionalities (for local and remote installations)

- What is the delay between the removal of the disruption and the recovery to nominal performance?
- Will infrastructure recover after repeated onsets of disturbances in the absence of full restoration?
- Recovery from disruptors of socio-economic and political nature