Institut pour la Maîtrise des Risques
Sûreté de Fonctionnement - Management - Cindyniques

Evaluation of STPA Safety methodology on satellite servicing missions with MBSE tool

GENET Emilien
Thales Alenia Space
Cannes
emilien.genet@thalesaleniaspace.com

BONNE Thomas
Thales Alenia Space
Cannes
thomas.bonne@thalesaleniaspace.com

***Résumé* —** Traditionnellement, les analyses de risques sont dominées par les défaillances matérielles, et elles s'appuient sur des données de fiabilité accessibles, et utilisées en arbre de défaillance . Le STPA (Systems-Theoretic Process Analysis) est une méthode d'analyse de risque qui se focalise sur l'investigation de causes plus larges que les seules défaillances matérielles. L'approche STPA [1] [2][3] se concentre sur un problème de contrôle, en accordant une importance aux échanges de données et au temps. Les actions de contrôle indésirables sont analysées sur une structure de contrôle via une méthodologie rigoureuse qui prend notoirement en compte des omissions et des dysfonctionnements des logiciels et des données.

Cet article se concentre sur la méthodologie STPA appliquée à une mission de service en orbite à l'aide d'un outil MBSE (Model Based System Engineering). Thales TRT a développé un *viewpoint* STPA [4] dans Capella [5], une suite logicielle open source MBSE basée sur la méthodologie Arcadia [6]. L'analyse est effectuée sur des phases spécifiques de rendez-vous en orbite. Les avantages de l'utilisation de ce MBSE pour effectuer une STPA et les résultats supplémentaires de la STPA sont évalués. Le but est d' améliorer la compréhension des causes sur une mission complexe. Les missions de service en orbite [7] comprennent un client, un véhicule de service , un segment sol et des tiers à proximité de l'orbite. En aboutissant à des contre-mesures contre les scénarios identifiés, les étapes finales de la STPA augmentent le nombre de contrôles de risques, via des spécifications, ce qui permet ensuite une poursuite avec un processus de sécurité traditionnel.

En effectuant une STPA tôt pendant le processus de conception, elle peut fournir des informations précieuses à une équipe RAMS et d'ingénierie, tant pour les contrôles de sécurité que pour les besoins de la mission. La construction d'un processus complet de système de sécurité avec MBSE, les diagrammes associés permettent de traiter la STPA plus facilement et plus précisément qu'une étude STPA faite sur Excel, comme montré dans un chapitre dédié. Ce travail aborde l'utilité de la STPA pour la spécification en pré-conception et la spécification d'unités et de sous-systèmes avancés spécifiques. Le visuel de l'approche, la traçabilité entre les scénarios de perte et les contre-mesures, la connexion à une structure de contrôle évolutive, la compatibilité multi-utilisateurs et l'amélioration de la spécification des logiciels en matière de sécurité opérationnelle sont les résultats positifs discutés dans cette démonstration de concept.

Mots-clefs — STPA, MBSE, Satellite, Service en orbite, Sécurité spatiale

***Abstract* —** Traditional cause and controls analysis used for hazard analysis are dominated by hardware failures, because they have a reliability data connection easier to obtain when using FTA (fault tree analysis). STPA (Systems-Theoretic Process Analysis) is a holistic risk analysis method that investigates more causes than hardware failures. The STPA approach [1] [2][3] focuses on a control problem with importance given to data exchanges and time. Unwanted control actions on safety-related control loops are analyzed against the timeline of operations via a rigorous methodology that considers also software and data failures, omissions and faults.

This paper focuses on the STPA methodology applied to an in-orbit servicing mission with a MBSE (Model Based System Engineering) tool. Thales TRT developed a STPA viewpoint [4] in Capella [5], an open source MBSE software suite compliant with the Arcadia methodology [6]. The analysis is performed on specific rendezvous phases. Both the benefits of using this MBSE for performing STPA and the STPA additional findings are evaluated. This evaluation is done to focus on a new complex mission: in-orbit servicing missions [7] consist of a client, a servicer, a ground segment, and third parties near the orbit. By building countermeasures against the identified loss scenarios, STPA final steps increase the number of hazard controls, tracked down on specifications at various levels; then the transition to traditional Safety method (control, verification) can happen.

By performing STPA during the design process, earlier than the traditional analysis, it can provide valuable insights to a RAMS and Engineering team for both safety controls and mission purposes. The build of a complete safety system process with MBSE, the associated diagrams allow the STPA to be processed more easily and more precisely than a based on Excel STPA In particular, specifications and discussions on technical controls are being raised in a more efficient and exhaustive way. This work discusses the usefulness of STPA for predesign specification (early stage) and specific advanced subsystem and units' specification (consolidated design stage). Great visuals (loss scenario and countermeasures tracking, connection to an evolving control structure, multi-users compatibility, increasing software specification to operation safety purpose are the positive outcomes discussed in this proof-of-concept for using MBSE STPA on in-orbit servicing mission.

Keywords — STPA, MBSE, Satellite, In-orbit servicing, Safety

I. INTRODUCTION

STPA (Systems-Theoretic Process Analysis) is a holistic risk analysis method [1] that investigates more causes than hardware failures. The STPA approach focuses on a control problem with importance given to data exchanges and time. Unwanted control actions on safety-related control loops are analyzed against the timeline of operations via a rigorous methodology that considers also software and data failures, omissions and faults.

In this article, the STPA method is applied to the in-orbit servicing which consists in a servicer providing maintainance, disposal, via docking berthing and eventual ORU (Orbital Replacing Units) replacements and client satellites that are receiving the services [7][8][9]. These servicing missions typically features a satellite servicer with a robotic arm that can grab and berth to a specific satellite in orbit [7]. After berthing, there is a docking possibility to enhance the servicer capabilities onto the client mission. The mission has several phases:

- Launch and Commissioning
- Far rendez-vous
- Inspection
- **Close rendez vous**
- **Capture (**Berthing/ Docking/…)
- Composite activities (ORU transfer, robotic arm / servicing operations)
- Unberthing

The time to react to a mishap (failure, fault, anomaly) is shorter for the close rendez-vous and capture phases. Therefore these critical phases are the focus of the STPA assessment for the in-orbit servicing mission. The exhaustiveness effort required by STPA is hence judged more relevant for these phases because there is only partial heritage and new phenomenon to assess.

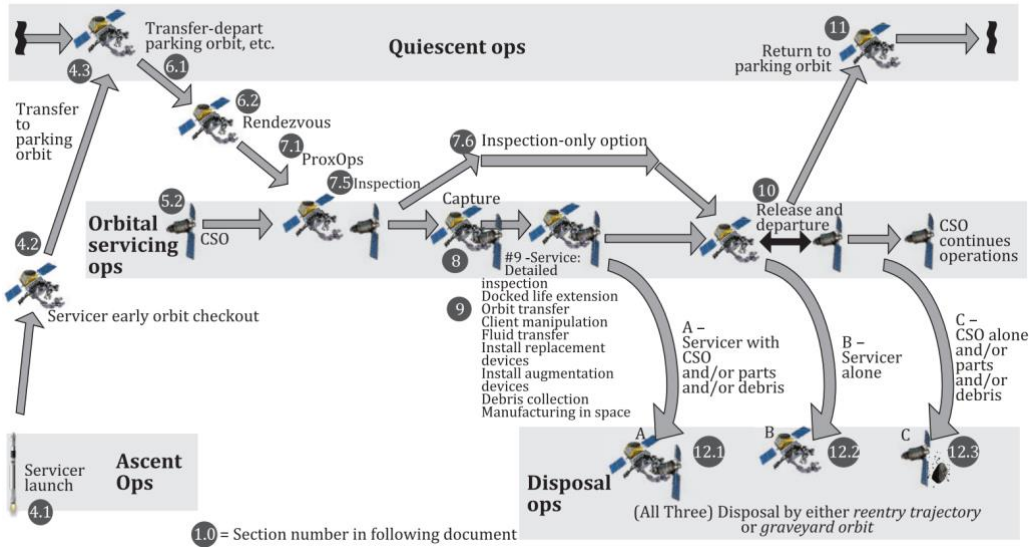

Fig. 1. Servicing mission : the servicer vehicle and a client satellite (top) and the relative path of the servicer towards the client (bottom [8])

Since the mission involves contact between satellites, the hazards are collision and debris generations, creating a risk for the orbit and the human . This is why according to the Space law and harmonization efforts for a cleaner space, these types of missions fall under Safety evaluation[8][9], within the debris hazard control and reduction effort. From the beginning, RAMS studies like hazard analysis and FMEA per phases help at determining the initiating events, controls and verifications for the former and mitigations for the latter. However due to the specificities of automation and quick reaction time for some phases, and inherently since the mission can trigger only in some configurations an avoidance manoeuver methods, it was decided to investigate this mission with a robust tool.

The demonstration of a servicing mission can address the servicing of both unprepared and prepared client satellite [7] :

- Although the servicing of an unprepared S/C is limited to inspection or lifetime extension, this class of services represents an early opportunity of service and so would allow to initiate a commercial service. In term of technologies this requires :
  - Rendez-vous without navigation aids on the client
  - Capture using an existing feature of the client (e.g. Launch adapter ring)
- Servicing of a prepared client enables more advanced services :
  - Propellant transfer (refueling) to extend lifetime or allow orbit change (e.g. deorbiting reentry)
  - installation of Orbit Replaceable Unit. This capability would allow to extend the capability of the client by adding new payload, but also to replace failed equipment, or to add some deorbiting kit.
  - A prepared client is foreseen to have approach and capture phase easier (client conceived for servicing)

The STPA has been shown already to be adapted to study hazards with missions where reaction time matters a lot in the controls, because it investigates the Safety as a control process, hence, dependent onto timings and data accuracies [7]&[9].

Each phase of STPA is applied on the servicing mission and detailed. Another space mission was STPA modelled without MBSE [8]. For specific visibility and understanding, the focus is performed on the "close rendezvous" mission phase, when the servicer approaches the client satellite. Since the number of functions and mission aspect is dense, with functions supported by complex hardware and software interactions, the decision is to use STPA with a MBSE tool, for instance the Capella tool. The objectives are to demonstrate the full scope of Safety controls, in term of requirements that the methodology can bring.

II. In orbit Servicing STPA with CAPELLA

The STPA Add-On is an experimental extension of Capella that has been developed by Thales TRT division, and it provides a model-based tool support for STPA. It can be used for standalone STPA analyses or in combination with classical Capella modelling [5]. A user guide already exists [4] , and it describes very well the transition from the STPA method to the Capella model .

Figure 2 presents the 4 phases of the STPA process integrated in the Capella framework:

- Phase 1 : identify the stakes, losses and hazards and specify safety constraints
- Phase 2 : model the control structure, in particular the controlled process and the associated data flux
- Phase 3: identify unsafe control actions (UCA), i.e. the anomalies on control actions previously determined
- Phase 4 : identify loss scenarios : identify UCA leading to hazards , and create countermeasures to control them.

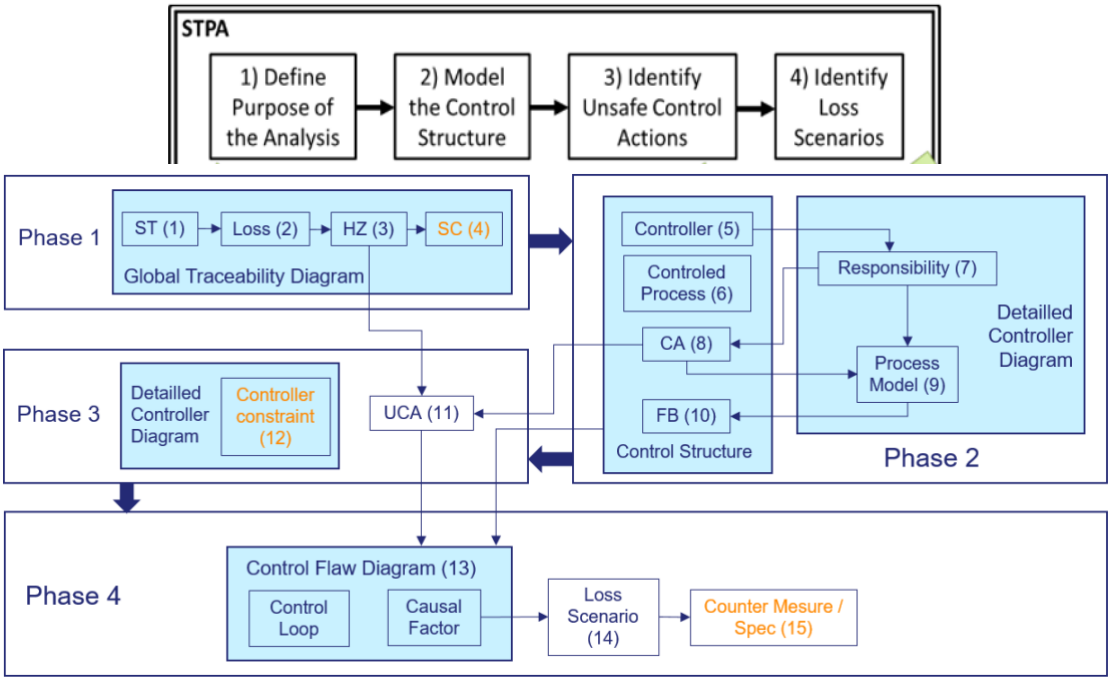

Fig. 2. simple phases (top) and detailed phases (bottom) of the STPA analysis with Capella. Analysis outputs are in orange

STPA-PHASE 1 : Hazard Definition.

The first phase of the STPA process consists in defining several safety settings like the Stakes (ST), Loss (L), Hazards (HZ) and also an output: the System Constraints (SC) that are high level specifications.

This phase allows to fill all inputs of the project that the Capella model will need in the next phases.

The **stakeholders** (SH) have interests which are **Stakes** for the servicing mission. **Stakes** can be either contractual (obtain performance) , and legal (preserve human life). The legal stakes are related to the Safety principal objective of human hazard control, but they have ties with the product being designed, hence with the contractual stakes. These stakes – at least the contractual ones- are also equivalent to high level capabilities in Arcadia MBSE [6].

TABLE I. IN ORBIT SERVICING STAKEHOLDER AND STAKES - STPA PHASE 1

	Name	Losses
(SH-01)	**Client SATELLITE Operator / Owner (Private / Space Agency)**	
(ST-01)	Expand Operationnal Lifetime of Client SATELLITE	[L-01, L-09]
(ST-02)	Respect the Orbital environment Law - Avoid becoming an uncontrolled debris	[L-09, L-08]
(ST-03)	Continue Performance mission of Client SATELLITE	[L-01, L-09]
(SH-02)	**Space Servicing Vehicle (SSV) Operator / Owner (Private/ Space Agency)**	
(ST-04)	Perform servicing mission - for the Client SATELLITE	[L-02, L-04]
(ST-05)	Ability to complete several servicing mission - minimize ressources consumption	[L-03, L-04]
(ST-06)	Respect the Orbital environment Law - Avoid becoming an uncontrolled debris	[L-07]
(ST-07)	Good Controlability over the servicing mission	[L-02, L-03, L-04]
(SH-03)	**Space Community (Users of the Space - All agencies and private companies in space)**	
(ST-08)	Have a space orbit clean, disposable and available - operate in a sustainable environment	[L-06, L-08, L-07]
(SH-04)	**Human Community (All mankind on Earth)**	
(ST-09)	Avoid being injured by a space debris reentering Earth	[L-05]

Then, **Losses** are defined in TABLE II. They are simply loss of stakes, identified as a loss of high-level capabilities that the servicer, client or ground are expected to be able to do. In the table, there are links from Loss to one or several Stakes and Hazards. Indeed, if there is a Loss in progress, there will be some Stakes jeopardized.

TABLE II. IN ORBIT SERVICING LOSSES,STAKES AND HAZARDS - STPA PHASE 1

	Name	Stakes	Hazards
(L-01)	Loss of Client SATELLITE performance mission	[ST-01, ST-03]	[H-05]
(L-02)	Loss of Servicing mission - with the current client SATELLITE	[ST-04, ST-07]	[H-04]
(L-03)	Loss of SSV ability to perform further servicing missions	[ST-05, ST-07]	[H-04]
(L-04)	Loss of SSV controlability (total loss of SSV mission)	[ST-07, ST-04, ST-05]	[H-04]
(L-05)	Loss of human life or serious injury	[ST-09]	[H-03]
(L-06)	Loss or pollution of the Client orbit	[ST-08]	[H-03, H-01, H-02]
(L-07)	Loss of SSV capacity to perform safe end of life (desorbit/reorbit)	[ST-06, ST-08]	[H-03, H-04]
(L-08)	Loss of client capability to perform safe end of life (desorbit/reorbit)	[ST-02, ST-08]	[H-05, H-03]
(L-09)	Loss of Client SATELLITE controlability (total loss of client mission)	[ST-01, ST-02, ST-03]	[H-05]

Then, the **Hazards** are defined in TABLE III. In pure STPA, a hazard is a loss expanded to the system studied. However, for a convenient use, in this application, the hazards are defined as Losses having Safety consequences. This choice to unify STPA with hazard analysis is made in purpose to answer the Safety certification process than an independent panel (European for instance) would require. In the hazard table, the links are established with the losses and **Safety Constraints**. These are high level specifications, created to prevent the hazard to happen

TABLE III. IN ORBIT SERVICING HAZARDS, LOSSES AND SYSTEM-LEVEL CONSTRAINTS - STPA PHASE 1

	Name	Losses	System-Level Constraints
(H-01)	Collision between SSV and client	[L-06, L-04, L-09]	[SC-01, SC-02, SC-04]
(H-02)	Collision of either SSV/client or stack with another space object (satellite, referenced debris,...)	[L-06]	[SC-01, SC-02]
(H-03)	Debris generation / orbit contamination	[L-06, L-05, L-07, L-08]	[SC-01, SC-02, SC-04, SC-05, SC-07]
(H-04)	SSV permanent loss control or loss of mission	[L-03, L-02, L-04, L-07]	[SC-01, SC-03, SC-04, SC-06]
(H-05)	Client permanent loss control or loss of mission	[L-01, L-08, L-09]	[SC-02, SC-05, SC-06]

Setting **Safety Constraints** in TABLE IV. as top level specifications is seen by [1] as an opportunity to dig already into the physical parameters, context in cause.
Some Safety Constraints are derived as per the STPA handbook [1]: SC-1, SC-2 SC-7 are sufficient to create “top level” constraints to all the hazards . SC-3, SC-4 , SC-5 and SC-6 are evolved constraints , meaning they are already related on cause (sub-hazard) and even control identified (fault tolerance, reactivity, datalink to operations for the SSV, safe state for the client) and so the “condition” and “link to hazards” and could be also outputs from the ultimate phase 4 Countermeasures.

This choice of adding “educated” constraints inside the STPA process is seen as an opportunity to orient earlier the focus on some specific controls, based on the analyst experience, without losing focus on the holistic approach thanks to the other safety constraints.

TABLE IV. IN ORBIT SERVICING SYSTEM-LEVEL CONSTRAINTS - STPA PHASE 1

	Name	Hazards	Responsibilities
{c} (SC-01)	SSV must provide sufficient AOCS and propulsion control (sensing & actuation) to avoid collision to client	[H-01, H-02, H-03, H-04]	[R-01, R-07, R-08, R-02, R-04]
{c} (SC-02)	Client must be in sufficient AOCS and propulsion Safe control (sensing & actuation) to avoid collision with SSV	[H-01, H-03, H-05, H-02]	[R-03]
{c} (SC-03)	SSV proximity operations (navigation, guidance, berthing and docking) has to be supported by fault-tolerant design.	[H-04]	[R-08, R-04, R-02, R-01, R-07]
{c} (SC-04)	SSV (navigation, guidance, berthing and docking) reactivity must be fast enought to prevent collision and debris	[H-03, H-04, H-01]	[R-01, R-02, R-04, R-08]
{c} (SC-05)	Client functions during servicing must be in a safe sustained state [when client control systems are enabled]	[H-05, H-03]	[R-03]
{c} (SC-06)	SSV communication link to ground control AND/ OR client must be kept at a datarate compatible to ensure SSV controllability	[H-04, H-05]	[R-06, R-02, R-08]
{c} (SC-07)	SSV deorbitation/ reorbitation capability must be kept [after one failure]	[H-03]	[R-04, R-03, R-02, R-01, R-08]

At the end of Phase 1, the tool allow to create a *Global Traceability Diagram*, representing all the links between the STPA elements of this phase. Since the 4 previous tables contain this information, this diagram is not presented in this article.

STPA-PHASE 2 : Control Structure

This second phase allows to represent the control systems and the data links at a physical and logical level. For this study, the control structure has been adapted on the specific phases of the mission. Since the use case focuses on the close rendezvous and capture phase, the relevant focus was put on the hardware specific for this mission phase, hence this is also a preliminary and partial modelling of the whole system that is presented in Fig. 3. For this purpose, the relevant GNC sensors and actuator suite was modelled, but the robotic arm was not modelled. For an holistic STPA approach, the eventual interactions between groups of components shall be assessed (as a representation of the whole system).

In the present case, the focus is on the servicer close proximity phase to the client and so, the docking berthing sensors, navigation and guidance hardware of the SSV, with also the interacting client and ground control.

The *control structure* allows to determine the rules and relationships with several **controllers**, , that are grey rectangular boxes, and the interactions with the equipment are displayed by two types of arrows:

- the **control action** which represent the order given by the controller to the processing equipment in bold
- the **feedback** of the process return to the controller in dotted line

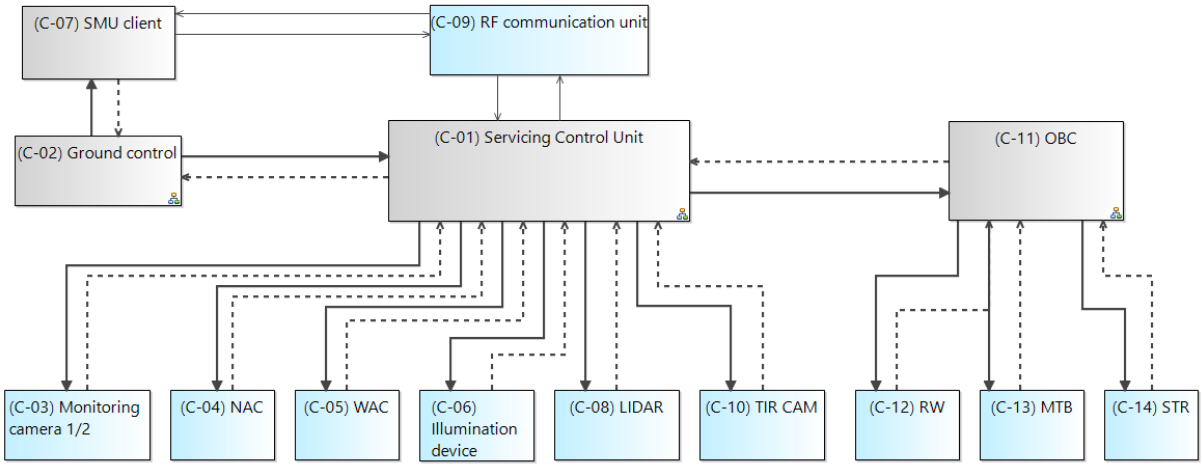

Fig. 3. Control Structure of servicing mission (simplified for the close approach and capture phase) – STPA Phase 2

For instance, per Fig. 3, the main controller of the servicer is the Servicing Control Unit (SCU). It is linked to most of the GNC (Guidance Navigation Control) sensors : monitoring cameras, light detection and ranging (LIDAR), narrow-angles cameras (NAC), wide-angle cameras (WAC). Another controller, the OBC (on board controller), is linked to the GNC actuators reaction wheels (RW) and MagnetoTorquers Bars (MTB) and the star trackers (STR).

The link to the other entities, SMU client and ground control are represented via arrows to the RF communication unit.

The following step consists in defining the **responsibilities** of the SCU **controller**, i.e. all the functional tasks that the controller must be able to manage and succeed, present in TABLE V.

TABLE V. IN ORBIT SERVICING SERVICING CONTROL UNIT RESPONSIBILITIES - STPA PHASE 2

	Name	System-Level Constraints	Control Actions	Feedback
★ (R-01)	Data reception and filtering of all SSV sensors	[SC-01, SC-04, SC-03, SC-07]	[CA-01, CA-04]	[FB-01, FB-04]
★ (R-02)	Data exchange : SSV SCU with OBC	[SC-01, SC-04, SC-03, SC-07]	[CA-06]	[FB-03]
★ (R-03)	Data exchange: SSV with Client	[SC-02, SC-05, SC-07]	[CA-03]	[FB-03]
★ (R-04)	Command and control SSV (Power, Prop,...)	[SC-01, SC-04, SC-03, SC-07]	[CA-01, CA-02, CA-03]	[FB-02]

For this Phase, the STPA Capella Add-On allows to create a *Detailed Controller Diagram*.

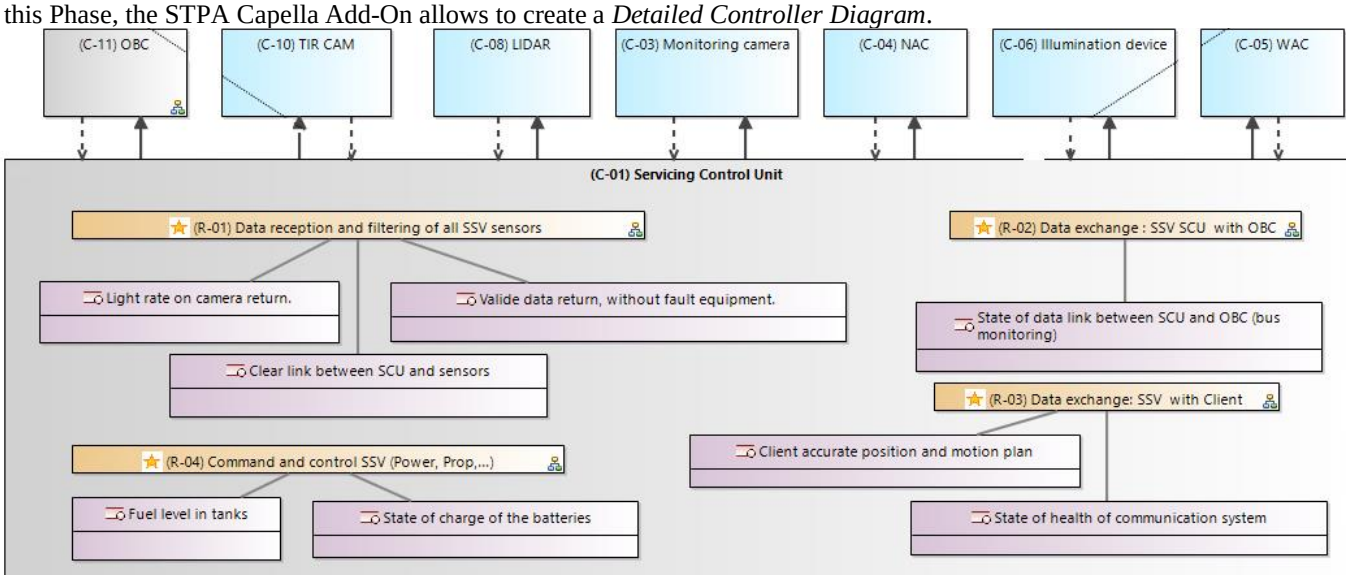

Fig. 4. Detailed Controller Diagram of servicer – STPA Phase 2

Fig. 4 represents the Servicing Control Unit controller. In the controller box, the responsibilities defined are in yellow boxes. In addition, we can define the **process models** represented by the purple boxes. Each process model is a short input that must be validated to ensure the success of each responsibility. For example, the fourth responsibility (R-04) "to ensure the proper management of the command and control of the servicer", the controller must -among other process models not fully model for the scope of this article- know the fuel level in the tanks and the state of charge of the batteries.

To conclude on this phase 2, the *control structure* allows to model adequately the physical system structure and the *detailed controller diagram* presents an overall view of each controller responsibilities and process with precision. The verification of links between responsibilities of controllers (found in phase 2) with hazards (in phase 1) via a table targets exhaustiveness . This step is very important prior going into phases 3 and 4, because the choices of modelling must be aligned to the Safety objectives.

STPA-PHASE 3 : Unsafe Control Action (UCA)

This third phase of STPA enables to identify if an hazard can be reached if the control actions realized by the controllers fail. The idea is to look at each control loop to identify systematically (repeatedly and for all the system) where the failures or mishaps can arise from. These are located in four control loop elements that can be an origin of the problem:

- the controller
- the link for sending an order **Control Action**
- the sensors or actuators/equipment
- The link from the sensors/actuators back to the controller : **Feedback**

STPA [7] identifies four categories of **Unsafe Control Action** (UCA) that are assessing the elements mishaps of the control loop:

- "Not Provided": The order or the feedback was not sent or was not received
- "Provided-false": The order is wrong or the feedback is false.
- "Wrong Timing": The control action or feedback is received too late or with a delay.
- "Stopped too soon or applied too long": The order has a fault in the duration of the application time.

In practice, a control loop and the related control action are chosen: the loop between SCU and LIDAR and the control action: "Provide distance between SSV and client". Then the control action is assumed in fault to question if it can lead to an hazard. For the example: if the control action "provide distance between SSV and client" is "Not provided", the consequences are hazards H-01 (collision with the client) and eventually H-02 (collision with a third party).
This simple case leads to identifying that the distance between the SSV and the client is crucial to avoid hazards during the close rendez-vous phase. It can be obvious from the start, but what STPA provides is that all critical parameters can be identified and then dealt with the proper care (increased SW verification, data stream priority) and the proper testing. At the first screening of STPA, Safety critical parameters arise, and their criticality is dependent on phases (for instance, in another phase "docked or far rendez-vous", the distance is not critical). At a later stage of conception, it is expected that specific conception and verification of failure detection and recovery sequences are built for these cases:

- "Not provided" is of course something that would be detected and leading to an abort of the sequence when it can be. The data providing chain must be robust.
- "Provided-false" needs a different control : increased robustness of the data via redundancy, filtering techniques and even voting can be selected to strengthen the data veracity
- "Wrong-timing" : the validation with proper model prior going into orbit for this specific sequence
- "Stop too soon" : in this case, is equivalent to not provided. "applied too long" is not leading to an hazard.

For the early STPA phase identification, however, a trade might be perform on a robustness of the mission vs. the loss of the parameter in a critical phase where reaction speed is needed. In this case, for a single interaction and for a single phase, STPA method allows raising questions linked to time, in the form of unsafe control actions. As some can be obvious, others can be tricky, and hence STPA allows to cover more than a static hazard analysis. A few UCAs derived from the CA "provide the distance between the SSV and the client" are in TABLE VI.

TABLE VI. IN ORBIT SERVICING: DERIVING UNWANTED CONTROL ACTIONS - STPA PHASE 3

	Name	Violated C...	Hazards
CA-04	Provide the distance between the SSV and the client		
Not providing causes hazard			
UCA-03	The requested control action has not been provided, the servicer remains in its last position without applying any modification which could collide with the client or a third party.	[SC-03]	[H-01, H-02]
Providing causes hazard			
UCA-04	The provided data is faulty, its interpretation by the actuator could lead to a collision with the client or a third part.	[SC-03]	[H-01, H-02]
Wrong timing or order causes hazard			
UCA-05	The provided data is received too late : that could create a difference between the position returned and the real position. This situation could lead to a colision with the client.	[SC-03]	[H-01]
Stopped too soon, applied too long			
UCA-06	The requested control action has not been provided, the servicer remains in its last position without applying any modification; no collision	[SC-01]	[H-01, H-02]

STPA-PHASE 4 : Counter Measures

In the last phase of STPA process, the control strategies are initiated thanks to specifications called **countermeasures.** These control the UCA faults defined in phase 3. Those countermeasures allow to strengthen the system, subsystem and equipment specifications and they serve as early hazard controls.
To determine them, the steps of the STPA Add-on manual are followed [10].

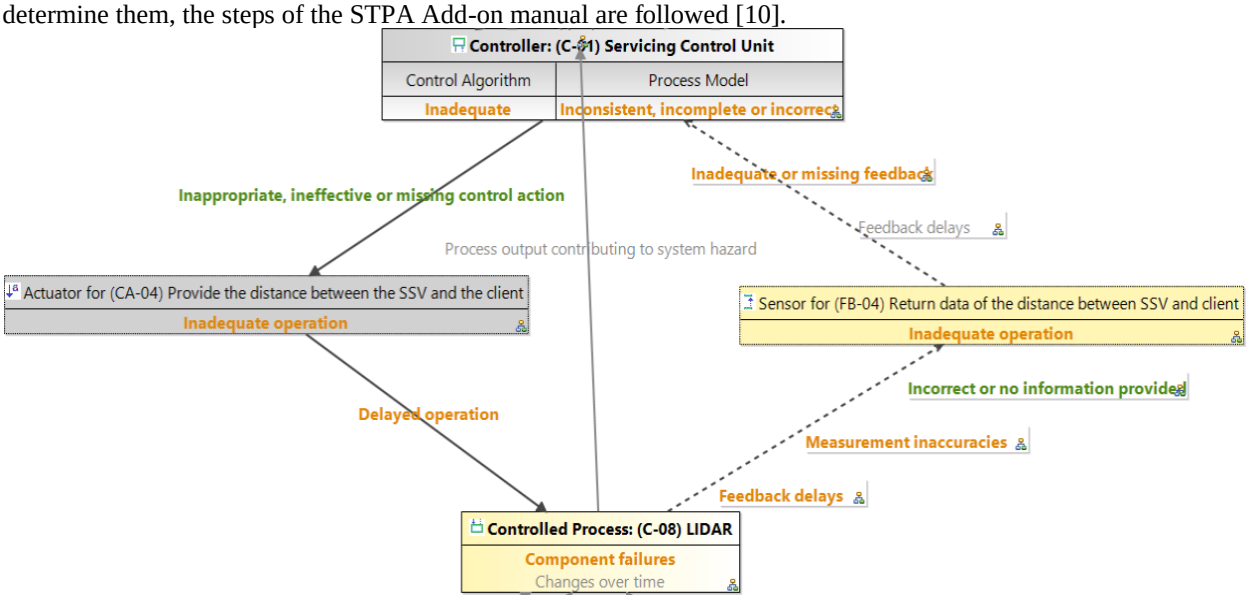

Fig. 5. Control Flaw Diagram Diagram of Servicing Control Unit – STPA Phase 4

The *Control Flaw diagram* in Fig. 5 represents a single **control action**, here the control loop between SCU and LIDAR, and the aim is to investigate causal factors from the UCA list derived in Phase 3.
Initiating faults that can happen for this loop (on the controller, process model, actuator failures, commanding control actions failures, feedback loop failures), as initiating events for the UCA. These failures are called **Causal factors** and they are in this case:

- Inadequate control algorithm or incorrect process model for the SCU SW application,
- Component failures for the LIDAR HW
- Inappropriate, ineffective, missing, delayed control action for the command link
- Delays, inaccuracies, incorrect or no information for the feedback (data from the LIDAR)

To build a proper *Control Flaw Diagram*, each **Causal Factor** is analyzed with boxes option, and associated with a proper color code in the Capella Add-On:

- Red: causal factor is not yet checked.

- Green: causal factor will not lead to an UCA and to a hazard. (OK)
- Grey: causal factor is not applicable in this case. (N/A)
- Dark red: causal factor can lead to an UCA and to a hazard. (KO)
- Orange: this causal factor is dangerous (dark red) but it was reviewed in the Loss scenario Table.

When each causal factor has an assigned color, the causal factors leading to an UCA/hazard (red /dark red) are reviewed to be assessed and connected to a **loss scenario (LS)**.

TABLE VII. IN ORBIT SERVICING: CAUSAL FACTORS FOR A CONTROL ACTION - STPA PHASE 4

	Name	Control Action	Unsafe Co...	Vio...	Hazards	Causal Factors	Countermeasures
(LS-01)	Wrong control action due to a loss of package between Controller an	CA-04	UCA-03	[]	[H-01, H-03]	[[CA-04] Actuator: Inac	[S7 : The SW errors s
(LS-02)	Delay due to an overwarming of the connection between actuator anc			[]	[H-01, H-03]	[]	[]
(LS-03)	Component failure due to the wear.	CA-04	UCA-03	[]	[H-01, H-03]	[[CA-04] Process: Fail	[S1 : The sensor shall
(LS-04)	Incorrect data due to an error process	CA-04	UCA-03	[]	[H-01, H-03]	[[CA-04] Control Algori	[S7 : The SW errors s
(LS-05)	Delay due to longer than usual sending of process data	CA-04	UCA-05	[]	[H-01, H-03]	[[CA-04] Actuator-Proc	[S5 : In case there is a
(LS-06)	Delay due to longer than usual data processing.	CA-04	UCA-05	[]	[H-01, H-03]	[[CA-04] Process-Sen	[S3 : In case sensing
(LS-07)	Incomplete feedback received by the controller due to a solar reflect (	CA-04	UCA-03	[]	[H-01, H-03]	[[CA-04] Process-Sen	[S9 : Eventually redun

The **Loss Scenario** table (TABLE VII.) is a key output. For instance, considering the causal factor "feedback delays or inadequate missing feedback" in the control flaw diagram, there is a need to define:

- **Loss scenario**: expansion from the **causal factor** in a complete sentence.
- **Counter measure**: a provision that prevents the system from falling into the loss scenario: this acts as a preliminary Safety control, and needs to be reflected in requirements.

An example of loss scenario is (LS-07): "Incomplete feedback received by the controller due a solar reflection" and the counter measure defined is (S9): "redundancy of sensors can be used to discriminate data"- in this case dissimilar sensing can be the option with LIDAR and camera. Note that this requirement coupled with other Safety constraints leads to have both similar redundancy (several cameras, several LIDARs) and dissimilar redundancy (the fact to have cameras and also LIDARs). The decision to implement all of them in hot configuration or warm to cold is dependent on power budget issue (technical) and phases (criticality). This is why STPA is important in the process: it allows to cross questions and specifications.
After the assessment, the causal factor under consideration changes to an orange color in the Capella tool, which means that it is hazardous but has been addressed (early controls are specified, but not verified as it belongs to the Safety traditional phase taking place after STPA)

When all the causal factors in the control flaw diagram are addressed, the defined counter measures can be added in yellow boxes into the *Detailed control diagram* in Fig. 6 defined in the Phase 2 of the STPA process. This is then a system specification viewpoint that is very appreciated for visualizing the inherent specifications needed from Safety perspective, and also to assess how these specifications could interact.

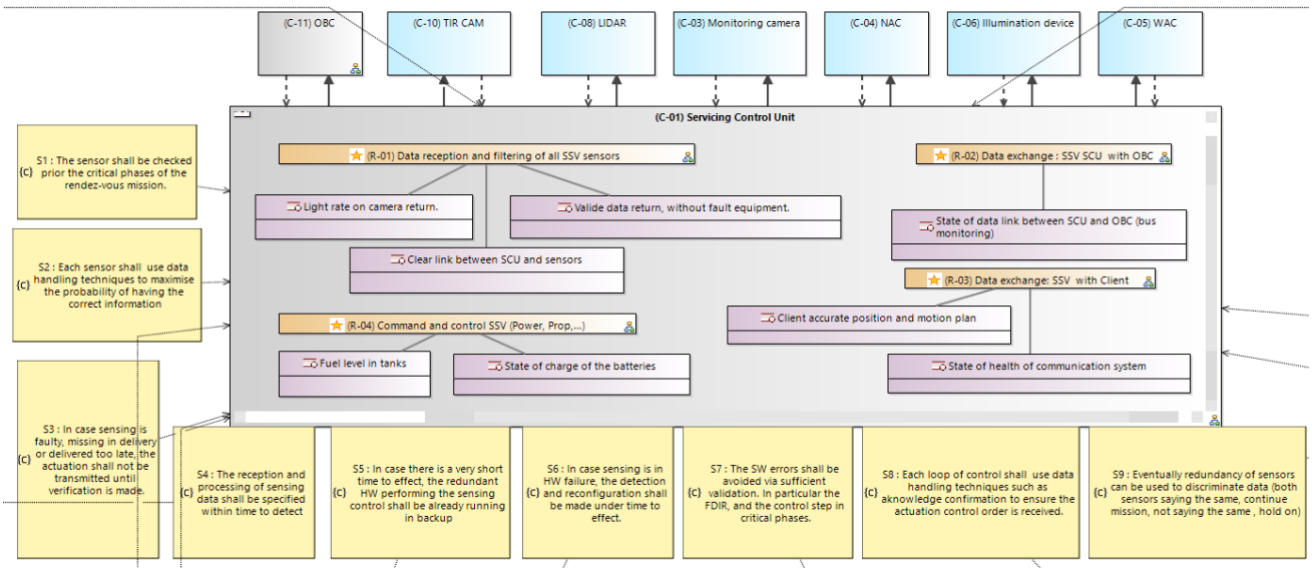

Fig. 6. Detailed control diagram with counter measures – STPA Phase 4

Some obious counter measures specifications found are known without performing STPA:

- S7 : the SW errors shall be avoided via sufficient validation

- S2 : each sensor shall use data handling techniques to maximise the probability of having the correct information
- S1 : the sensor shall be checked prior the critical phases of the rendez-vous missions.
- S8 : each loop of control shall use data handling techniques such as “acknowledge /confirmation” to ensure the actuation control is received.

However, and this is the main reason to use STPA, several specifications are found to be more mission specifics and issued thanks to the STPA process. Even from this early maturity system levels specifications, subsystem design and verifications can be derived :

- S3 : *In case the sensing is faulty, missing or delivered too late, the actuation shall not be transmitted until verification is made* :
  - Subsystem specification would define further on the detection and mitigation of incorrect sensing data on format, brutal change of data value, missing data streams
- S4: *the reception and processing of sensing data shall be specificed within time to detect*
  - System would refine the evolving time to detect vs. the time line of the critical phase : in the close approach, the time to detect is extremly low at the end phase vs. at the beginning, because of the distance between satellites. Depending on the collision avoidance manoeuver possibility and readiness, the system will use either a worst case or a filtered approach dependant on the sensing processing time. If there is a blackout area for a certain distance/ relative orbital/ flight dynamics parameters,(meaning not sufficient time to react), this limitation would be spotted in the design and the remaining risk should be precisely assessed in term of least hazardous control action (continue relative motion without change or other)
  - The STPA focusing on the control loop – it might be also pratical to consider the reaction time on the global loop for some failures i.e.LIDAR and SCU two ways impacting failures (wrong command, wrong sending back of data because of the wrong commands). Therefore the time analysis on STPA might need interaction but the scope of local and global control loop needs to be considered prior redacting specifications.
- S5: *In case there is a very short time to effect [to the hazards], the redundant HW performing the sensing control shall be already running in backup.*
  - The redundant HW real availability is what in focus, depending on the HW nature, it might necessitate more or less operationnal anticipation to be active : a thruster is reacting faster than a RW
  - A dissimilar strategy might even be proposed for actuators, at subsystem or system level if worth.
- S6: *in case the sensing HW is in failure, the detection and reconfiguration shall be made under time to effect*
  - As per specification S4 comments
- S9: *redundancy of sensors can be used to discriminate data (both sensors saying the same, continue mission, not saying the same : stay in hold point)*
  - The mission continuation or hold point is dependent on sensors, but sensors are dependent on their availability. If sensors are unavailable or in disagreement, because there is either no redundancy implemented nor strategy to elucidate which sensor has the correct input, the mission becomes impaired. Without redundancy, one solution is that the controller software does nothing, meaning the safe path without collision in this context is to impair the actuation. The other case is that actuation is needed to avoid a collision, and a CAM (collision avoidance manoeuver) is performed, but here the question of performing a CAM without sensors can be problematic. In the end, the detailed risk assessment on trajectory/ design capability will issue recommendations based on the point of no return definition and the safety discussion would consider the remaining risk acceptance.

The specifications are then turned into efficient controls and verifications : the standard Safety follows the STPA analysis. This follow-up Safety process is not evaluated in this article. However, from the specification of controls derived in STPA phase 4, this seems to be a rather classical approach.

IV. COMPARISON WITH STPA PERFORMED WITH EXCEL

The purpose of this section is to compare the two approaches and to show the benefits of using the Capella Add On. Initially prior the MBSE tool, the STPA method was performed with a Excel tool based on the emerging literature on STPA applied to space [8] and [9]. In particular the focus is to compare phases 3 and 4 outcomes on the two approaches (Phase 1 kept mostly similar and phase 2 to a classical block diagram for the controller) . The Excel template used was inspired by [3].

PHASE 3 performed with Excel : Unwanted Control Actions (UCA)

To control the unwanted control action - UCA, each scenario present in the table TABLE VIII. is analyzed and verified:

- If the case is filled in green, the UCA doesn’t lead to a hazard specified in first phase.

- If the case is filled in yellow or orange, the UCA may lead to a hazard by following one of the specified loss scenario, which are :
  (1) : The servicer will drift out of the capture position, in combination with no activation command or late one, the servicer will remain a free-flying object that could collide with the client.
  (2) : The arm will move without position control return that could collide with the client
  (3) : Servicer will move with wrong information which can lead to a collision with client
  (4) : The arm will move with wrong information which can lead to a collision with client

Although the Excel format presents in two dimensions the list of expected control actions on the HW vs their UCA considered, it falls to the analyst to think of the command and feedback links and to have in mind the responsibilities. It provides some early relevant controls, but is not helping the completeness nor the readability of the control process whereas the STPA tool allows it.

TABLE VIII. A FEW UNWANTED CONTROL ACTIONS DURING CAPTURE PHASE - STPA BASED ON EXCEL

Control Action with :	Not Provided	Provided			Incorect Provided			
		To early	To late	False data	Abort/Retreat/Hold CAM	Free drift	Arm motion unintended	Thrust unintended
AOCS sencors	UCA-1 : If AOCS sencors control is not provided to GNC : (1) The servicer will drift out of the capture position. In combination with no activation command or a late one, the servicer will remain a free-flying object that could collide with the client.	UCA-2 : If AOCS sencors control is provided to early to GNC. No problem	UCA-3 : If AOCS sencors control is provided to late to GNC. The servicer will continue to move witout control return during a moment. If the control return is so late : (1)	UCA-4 : If AOCS sencors control povided false data to GNC. The servicer will follow the order of the false return, (3) Servicer will move with wrong information which can lead to a collision with client.	UCA-5 : If an Abort/Retreat/Hold command is provided. The mission will end up imcomplete or the capture process will have to be started over.	UCA-6 : If a free drift command is provided. (1)	UCA-7 : If a arm motion unintended command is provided. (2) The arm will move without position control return that could collide with the client.	UCA-8 : If a Thrust unintended command is provided. (1)
NAC	UCA-9 : If NAC control is not provided to the SCU. No problem because the WAC control is more important at short range.	UCA-10 : If NAC control is provided to early to the SCU. No problem because the WAC control is more important at short range.	UCA-11 : If NAC control is provided to late to the SCU. No problem because the WAC control is more important at short range.	UCA-12 : If NAC control provided false data to SCU. The both control of NAC and WAC are different wich can lead to a problem : (3)	UCA-5	UCA-6	UCA-7	UCA-8
WAC	UCA-13 : If WAC control is not provided to the SCU. We can use the NAC return until the WAC return come back.	UCA-14 : If WAC control is provided to early to the SCU. No problem	UCA-15 : If WAC control is provided to late to the SCU. We can use the NAC return until the WAC return come back.	UCA-16 : If WAC control provided false data to SCU. (3)	UCA-5	UCA-6	UCA-7	UCA-8

PHASE 4 performed with Excel : Counter measures

The following UCA groups were defined to find counter measures easier:

- Sensing Not Provided
- Actuator Not Provided
- Sensing delayed
- Actuator delayed
- Sensing False data
- Actuator Incorrect order

Grouping the UCA with the loss scenarios and affecting a counter measure was found practical because they were numerous UCA to deal with. Then, several specifications were found similar to those expressed in §III- Phase4, but to a maturity that was focused on a generic format.

In conclusion, performing the STPA method without Capella is quite messy, and the MBSE tool provides a guidance support, several pertinent visuals schemes and allows to be more exhaustive. The comparison was done of course only on the STPA analyst point of view .

V. SYNTHESIS OF STPA USE FOR IN ORBIT SERVICING (IOS)

The STPA Add-on with Capella has been reviewed for a space context of In Orbit Servicing mission [7] [8]
The main positive outcomes of using STPA are the following:

- **Generating controls on a new space hazardous system with specificities that were not spotted on a classical "failure/causal" Safety analysis**- it is true that when the specificities are known, telecom satellites for instance considered alone, there is no need for STPA. Clearly on IOS, the specificities are the inherent proximity of two satellites, the remote distance, the level of autonomy, the time reaction for collision hazards. Applying only the classical hazards causes would be a failure of the Safety purpose.
- **Generating outputs that allow to think and build mission and system Safety control together:**
  - The "**Loss Scenarios table**": with all the source scenarios that can lead to a "UCA", and the "Countermeasure" associated with these loss scenarios for each dangerous "Causal Factor" on a control loop: this is the main output for

Safety control perspective. Proposing this table to a Safety board, in addition to the normative hazards reports might even be considered.
- The "**Detailed controller diagram**": with all the countermeasures related to a controller (here SCU), the breakdown of controls onto software and hardware components is apparent. This is the main output from system perspective, and seen as a collaborative tool on the project.

- **Sharing MBSE up to date content for Safety accurate picture**: this was not fully evaluated but it is foreseen that the fact to use a shared network MBSE model for performing the viewpoint might ease the maturation. Here, the STPA analysis is rather seen as a tool for the beginning phases, but it can also be used for refining the specification of controls and system/units details requirements in the consolidated design phases.

The drawbacks-judged acceptable by the authors- are the following:

- Complexity for a non MBSE practitioner or a non STPA practitioner : it is mitigated by first reading on STPA references, and then practicing the MBSE tool. One analyst had previous MBSE modeling small experience and the other had more STPA experience, so it is true both MBSE and STPA need some hands-on that seems reasonable in regard to the benefices acquired.
- Limited understanding of project collaborators to MBSE and Safety culture: it is mitigated thanks to outputs diagrams for discussion and the fact that MBSE visuals are generally quite appreciated to think on components and functions. Here the dimension of Safety brought with the loss scenarios tables is useful for Safety perspective.
- The number of steps (15 with 3 outputs) are intense and need focus. It is true that the analyst must maintain a correct focus on the whole process : elaborating the adequate control structure with its failures and anomalies and then deriving countermeasures as a prelude to Safety control and verifications. However by making pauses on the tool and coming back several days after, the analyst encountered no big issues (much less than on Excel).

Of course, it is our choice, from educated Space Safety point of view, to use the STPA tool for only specific phases of the servicing mission . Using STPA for new areas where Safety controls and design are not with full-heritage is worth the try.

The recommendations after this evaluation for space of STPA are the following:

- **R1-** model an adequate control system for the Safety purpose. Insist on what elements traditionnal Safety controls (from FTA/ causal analysis) do not consider : data link, relation between elements, time and delivery issues.
- **R2-** Define causal factors and loss scenario at the good level of granularity : details are necessary to focus controls on dedicated parameters.
- **R3-** align 7 (or more) of the 15 STPA concepts on the concepts on the Safety and Arcadia used in the space industry, by making a correspondance between the specific STPA concepts translated into Space System Engineering and traditionnal Safety. This is clearly an adaptation of STPA phase 1 and 4, but phase 2 and phase 3 are kept as is.
    - ST- stakes: capabilities
    - Loss: loss of capabilities
    - HZ – hazards : Safety consequences of losses (human, material)
    - SC -system constraints : system specifications high-level
    - Loss scenario : hazard description containing initiating events : causal factors
    - Counter measures : Safety controls -system specifications and subsystems specifications

- **R4-** The 3 outputs needs convergence: the counter measures are more powerful since at the end of the process, however they must be checked vs. the earlier derived Safety constraints and controller constraints. It means that these system and controller constraints can be seen as Safety design objective, and as part of the Safety reviews on controls and verifications , external reviewers might need to have them as Safety design objective .

III. CONCLUSION

The STPA process allows to model a control structure equivalent to the real system and to check all the data links between each controller and equipment. From the UCA considered on control structures, the counter measures found with causal factor and loss scenario allow to specify and control the hazards in a more exhaustive manner.

For this IOS space methodology assessment, STPA is used for the phases when the hazard time to effect is short. Also, the UCA allows to assess different ways of failures or incorrect data delivery according to the chronology. This focus allows expansion of the coverage of the Safety analysis.
From this perspective, STPA presents an added value compared to traditional studies, especially when the missions are involving several vehicles, complex in operations and the reactivity in some phase is needed.

Furthermore, the STPA - Add-on with Cappella eases the exhaustive process, thanks to the associated tables and diagrams more precise than a traditional paper/Excel STPA study. In particular, specifications and discussions on technical controls are being raised in a more efficient way. It has been found that connecting to the MBSE brings a lot of advantages:

- clarity and visibility of the controls functions , loss scenario and countermeasures
- connection to a live project that can be evolving –the control structure modelled evolution would lead to delta STPA process that are more evident to identify than without a MBSE tool
- multi-users use (several STPA analysts and MBSE analysts can work on the same model)

Finally, the connection to system via MBSE, making STPA a living tool, and the exhaustive methodology deployed seems more powerful to find safety controls and reduce the complexity, by allowing to understand well the control process and ask questions on controllers parts and data link, especially in early design phases.

ACKNOWLEDGEMENT

The authors would like to thanks the Thales Research and Technology (TRT) and the Thales Safety Expertise group for the support given during for this present study on feasibility of STPA applied to In Orbit Servicing Space systems, in particular Olivier Constant and Patrice Rodrigues.

REFERENCES

[1] Nancy G. Leveson, John P. Thomas, STPA Handbook, 2018

[2]Nicholas C. Dunn, “Satellite System Safety Analysis Using STPA” , 2013, available at https://dspace.mit.edu/handle/1721.1/85777

[3] Ishimatsu et al. "Modeling and Hazard Analysis Using STPA", Proceedings of the 4th IAASS Conference, Making Safety Matter, 19–21 May 2010, Huntsville, Alabama, USA SP-680 (September 2010)

[4] User Guide for the STPA Add-On to Capella, 2023, available at https://github.com/labs4capella/stpa-capella/blob/main/doc/STPA-AddOn-UserGuide.docx

[5] Eclipse™ Capella , Features and Benefits, available at https://mbse-capella.org/features.html

[6] Arcadia Datasheet available at https://mbse-capella.org/arcadia.html

[7] On-Orbit Satellite Servicing Study, NASA report, 2010

[8] ISO 24330 Space systems — Rendezvous and Proximity Operations (RPO) and On Orbit Servicing (OOS) — Programmatic principles and practices

[9] ESA Guidelines on Safe Close Proximity Operations, Issue 2.0, 28/09/2021