Human-variability-aware Safety Analysis Framework for Interactive Technologies of Critical Command and Control Systems

Camille Fayollas[1], Barbara Gallina[2], Philippe Palanque[3], Daniel Rodriguez-Hernando[4], and Sandra Steere[5]

[1] Université Toulouse Capitole, IRIT, France
[2] Mälardalen University, IDD, Sweden
[3] Université de Toulouse, IRIT, France
[4] CSG, CNES, Kourou, France
[5] CST, CNES, Toulouse, France

Abstract. Command and Control Systems (CCS) are dependability-critical socio-technical systems, which encompass organizations, trained operator(s), and interactive technology designed to support the operator(s) in command and monitoring tasks. For instance, the CCS for Flight Safety Operations at the Europe's Spaceport in Kourou supports the operator(s) in the monitoring of the trajectory and flight parameters of a launcher, and in commanding the eventual destruction of the launcher if the trajectory deviates outside of the pre-defined safety envelope. To ensure dependability, the congruence between the interactive technology and the operator is key. Indeed, the interactive technology must tolerate human-variability in terms of faults which may occur at perceptive, motor, and cognitive levels and which may lead to human errors. To assess dependability of new interaction technologies, we propose a systematic human-variability-aware safety analysis framework, called P-VASA. The framework takes into account the input and output devices, their associated interaction techniques and the operator's task and is applicable to any CCS involving interactive technologies.

Keywords: Command and Control Systems · Interactive Systems · Interactive Techniques · Safety Analysis · Socio-Technical Systems

1 Introduction

Command and Control Systems (CCS) are dependability-critical socio-technical systems, which encompass organizations, trained operator(s), and interactive technology designed to support the operator(s) in command and monitoring tasks. CCS in the digital era have replaced paper-based charts, maps, etc., by providing the needed information/decision support and the power to act. CCS are used in the civilian (e.g., air/rail/see/road traffic control but also fluids or energy dynamics control) as well as in the military (e.g., combat via air, sea, land) domains. These domains exhibit different criticality. However, since catastrophic

consequences may derive from misconception or malfunctioning of the supporting technology, they all need to be designed with an holistic socio-technical perspective at higher as well as lower-level to guarantee the congruence [13] between the various entities of socio-technical system.

At the Europe's Spaceport in Kourou, as part of the CCS for Flight Safety Operations, operator(s)' tasks include the monitoring of the launcher trajectory and parameters, and the command of the destruction of the launcher if the flight trajectory deviates from the predefined safety envelope. Hence, to ensure dependability, the congruence between the interactive technology and the operator is key. Indeed, the interactive technology must tolerate human-variability in terms of faults (error precursors) which may occur at perceptive, motor, and cognitive levels and which may lead to human errors.

We propose a systematic human-variability-aware safety analysis framework, called P-VASA (for People-Variability-Aware Safety Analysis), to assess dependability of new interaction technologies. This framework supports the assessment of interactive technology in terms of tolerance to human faults and in terms of exploitation of human capabilities. Performance shaping factors have an impact on the occurrence of faults and on the degradation of the capabilities and are also accounted for in P-VASA. Addressing the dependability of such technologies is key for the development of new CCSs able of leveraging operators' capabilities and tolerating human faults. A concrete example of such interactive technologies is Brace Touch interaction technique which has been developed to tolerate human-touch faults under turbulence in aircraft cockpits [24]. While that paper proposed a concrete solution to this problem it was proposed as a one shot solution. P-VASA framework aims at providing a generic framework to assess and then engineer, dependable interactions technologies in a systematic manner.

In this paper, we also apply P-VASA to the future CCS for Flight Safety Operations of launchers at ESA spaceport in Kourou.

The reminder of this paper is organized as follows. In Section 2, we provide essential background information and related work. In Section 3, we introduce P-VASA, a novel human-variability aware safety analysis framework. In Section 4, we apply P-VASA to analyze the safety of interaction techniques used within the CCS for Flight Safety Operations of launchers at ESA spaceport in Kourou. Finally, in Section 5, we provide our concluding remarks and sketch future work.

2 Background and Related Work

In this section, first we provide essential background information pertaining to the solution space, i.e., the POISE framework, interactive systems and their specificities, HAMSTERS-XL for modelling the operator work, the operator model and its variability, safety analysis methods. Then, we discuss related work.

The POISE framework [23] includes the following elements: (P) the People, performing the tasks and the work, (O) the Organization, providing the work context for the People and being the owner of the Interactive System, (IS) the Interactive System, used to perform the work, and (E) the Environment, where

the People work, within the Organization, and where the Interactive System is deployed. These elements are connected to each other through other elements: Automation, connecting the People and the Interactive System, System Requirements, connecting the Interactive System and the Organization, and Training and Operational Procedures, connecting the Organization and the People. Finally, the Organization is refined in Work organization and Processes, and People (or operators) are refined in Tasks.

Interactive systems' specificities are well described by the MIODMIT architecture [23], first introduced in [5]. This architecture is illustrated on the FSO CCS in Fig. 4 in section 4. This architecture includes i) the *operator*, described with the human processor model [3], ii) the *interactive command and control system*, described below, and iii) the *underlying system* (e.g., an aircraft engine). This architecture shows that the interaction mainly takes place though the manipulation of *input devices* (e.g., keyboard or mouse) and the perception of information from the *output devices* (e.g., a computer screen or speaker). The software part that uses information from the input devices is called *interaction technique* (IT). ITs have a tremendous impact on operator performance. Standard ITs encompass complex mechanisms (e.g., modification of the cursor's movement on the screen according to the acceleration of the physical mouse on the desk). The software part defining the graphical rendering on the screen is the user interface layout (*UI layout*) that defines the interactive objects, their size, their colors, their emplacement... and the *rendering system*, which is in charge of updating the UI layout. The *interactive application* is the software using the events from the IT to trigger commands on the *underlying system* and using data from the underlying system to update the UI layout so that the operator can have an idea of the underlying system state. This is where HCI methods such as task analysis are needed for building usable application that fit the operators' work [6]. The human processing while interacting with computers is called the Human-Computer Interaction Loop (HCIL).

HAMSTERS-XL for modeling human work. Task models are good candidate to model the human work as they support gathering and structuring data from the analysis of users' activities, and recording, refining, and analyzing information about users' activities. HAMSTERS-XL (Human-Centered Assessment and Modeling to Support Task Engineering for Resilient Systems) is a graphical task modeling notation for representing human activities in a hierarchical and ordered way [20]. User goals are decomposed into sub-goals, which can in turn be decomposed into low level tasks. This decomposition results in a hierarchical tree of nodes. Nodes can be tasks or temporal operators. The notation is supported by the HAMSTERS-XLE tool which enables the editing and simulation of task models. The tool can support the analysis of work complexity and support predictive performance analysis [16] of operations of the CCS.

Modeling Human Errors, Faults, and Failures. Reason [26] formulated a working definition for error, i.e., a generic term to encompass all those occasions in which a planned sequence of mental or physical activities fails to achieve its

intended outcome, and when these failures cannot be attributed to the intervention of some chance agency.

The Reason's taxonomy of errors has been extended by Shappell et al. [28, 32] and integrated within their Human Factors Analysis and Classification System (HFACS). Within space standards (i.e., ECSS-Q-HB-30-03A [7]), Reason's terminology is often used and HFACS is recommended. The ECSS-Q-HB-30-03A also points out the performance shaping factors (PSFs) which are defined as specific error precursors or error mitigators that influence human performance and the likelihood of occurrence of a human error.

Avizieniz et al. [1] introduced the dependability concepts including the dependability threats, i.e., faults, errors, and failures, their definitions and their causality chain, i.e., a fault causes error which causes a failure, which in turn may result in a fault for a subsequent system. This paper includes a taxonomy of faults and failures that includes human errors. In [29], Reason's and Avizieniz et al. terminology were harmonized and augmented reality-induced human failures were investigated, resulting in an extended taxonomy).

Finally, [25] expands the Avizieniz et al. taxonomy for a better coverage on human faults in three ways. First, it extends the taxonomy to recognize that human faults can be induced in the operator from external causes. Second, it enables to distinguish between faults arising 1) from the operator, 2) from another person, and 3) from the natural world (including the system itself). Third, based on the Card, Moran and Newell [3] human processor model, it adds the Human capability dimension to differentiate faults in the operator's perceptual, cognitive, and motor abilities.

According to these taxonomies, a human error is considered as a failure. For instance, when considering a plane pilot, the effect of turbulences is an external natural fault affecting the human motoric system. This fault activates an error mode which leads to a failure: not being able to select the right command.

Safety Analysis Methods. To conduct safety analysis different methods have been proposed and are usually recommended within dependability/safety standards (e.g., FMECA (Failure Modes Effect and Criticality Analysis) which can be conducted on the system or on the process, FTA (Fault Tree Analysis), or HAZOP (HAZard and OPerability) Analysis, STAMP (System-Theoretic Accident Model) and its associated process STPA (System Theoretic Process Analysis)). In this paper, we focus on FMECA as ECSS-Q-HB-30-03A [7] recommends to analyse human error with an Human Error Analysis Form sheet, which is similar to process FMECA. A FMECA focuses on both the effect of the failure modes and their criticality). To perform a FMECA, analysts are expected to fill in a spreadsheet with standardized fields. The standardization may depend on the application domain. FMECA can be conducted by systematically analyzing system components and their failure modes or process steps and their failure modes and the workflow of a human can be analyzed via a process FMECA.

Related work. In the literature, predecessors, have proposed safety analysis frameworks for safety analysis of interactive systems. For instance, in [19], the authors present a table (called HEECA) with a specific focus on Human Er-

rors and their criticality and effects that may occur during the performance of tasks. Our framework builds on top of this work and explicitly encompasses the interactive technologies used to perform the tasks, their needs in terms of operators capabilities, operators capabilities degradations and how the interactive technologies can tolerate (or not) such degradations. The human-variability is explicitly modeled.

In addition, the awareness of the relevance of a socio-technical perspective while analyzing complex socio-technical systems is not new. In [11, 21], authors provide modelling and analysis capabilities targeting socio-technical systems.

However, as far as we know, this perspective has not been taken at lower-level design and specifically for analyzing the dependability of interaction techniques with respect to the operators capabilities within their organizations. Another aspect of novelty is the explicit modeling of the human variability in terms of performance shaping factors, systematically taken into consideration as guidance while conducting the process FMECA-like analysis.

Summarizing, P-VASA, similarly to [19], it includes interactive technology decomposition (devices + ITs), task modelling integration and output artefacts. However, it differs from previous approaches by adding explicit human variability modelling, explicit PSFs integration and by recommending mitigations structured according to POISE. In addition, P-VASA is structured in way that will support its extension towards POISE-VASA.

3 The P-VASA Framework

P-VASA (for People-Variability-Aware Safety Analysis) is a human-variability-aware safety analysis framework for interactive technologies of CCS. It is twofolds as it provides systematic guidance for: 1) building an operator capability model, and 2) a process enabling to conduct the human-variability-aware safety analysis.

3.1 Operator capability model

To describe the operator's model, we propose an adaption of the feature diagrams [14], where mandatory features represent human/operator desired commonalities in terms of capabilities and the variable (optional) features represent PSFs/error precursors, which could degrade or invalidate the desired capabilities. In this context we use a classical and simplified human model widely adopted in the area of Human-Computer Interaction called the human processor model [3] enriched with information about human error models introduced in section 2 and exploits in a systematic manner the classification of human faults in the Human-Computer Interaction loop proposed in [25].

Fig. 2 presents a generic version of such an operator capability model. The first level of the model corresponds to the human processor model [3] and the second one develops i) the different perception capabilities (items f1.1 to f1.8), ii) an excerpt of the cognitive capabilities (item f2.1 to f2.3), and iii) an excerpt of

the motor capabilities (item f3.1 to f3.3). When performing the safety analysis, this operator capability model shall be further developed with the capabilities needed to interact with the input and output devices of the considered interactive system and with the PSFs that may affect these capabilities.

3.2 The P-VASA Process

The P-VASA process, depicted in Fig.1, is composed of four main steps:

Preliminary and high level POISE analysis. This first step corresponds to the high level analysis of the studied CCS exploiting POISE generic framework (presented in section 2) which decomposes a CCS in four interconnected components: People, Organization, Interactive System and Environment. It is important to note that depending on the CCS, the environment element might not be relevant as maybe be fully controlled, as, for instance, in en-route Air Traffic Control CCS when noise, light, temperature and humidity remain constant throughout operations. This step produces a high level POISE-based structured description of the studied CCS.

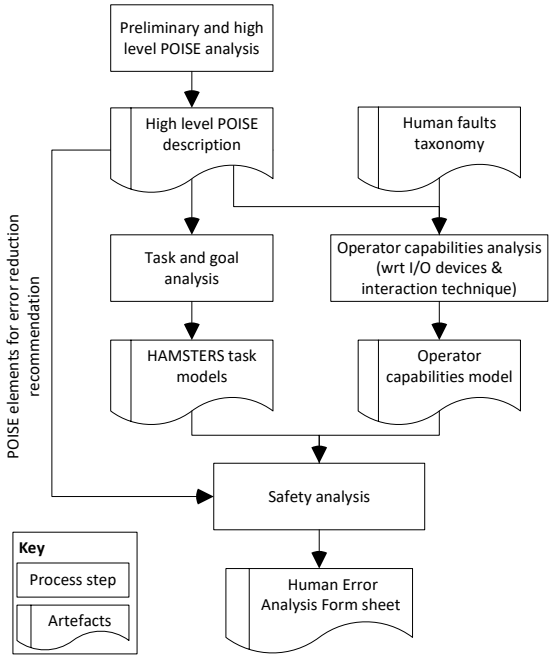

Fig. 1. The P-VASA process

Task and goal analysis. This second step takes as input the high level POISE description and, from this description perform the task and goal analysis of the

operators. To describe the operators' work, we rely on task modeling with the HAMSTERS-XL notation recalled in section 2. It is important to note that the task model refers to the interactive system description (e.g. as a task will be performed using at least one input and one output device, this is made explicit in the task model and the interactive system elements come from the MIODMIT description).

Operator capabilities analysis. This third step takes as input the high level POISE description and the human faults taxonomy from [25]. This step consists in expanding the generic operator model (presented in previous subsection and Fig. 2) with respect to the input and output devices and corresponding interaction techniques used within the CCS. This step can be performed in parallel to the second one.

Human-variability-aware safety analysis. This last step exploits the HAMSTERS taks models and the operator capability model to produce an FMECA-like table. In terms of structuring, this table is based on the Human Error Analysis Form sheet from ECSS-Q-HB-30-03A [7] as adherence to the handbook is relevant for the space agency.

A concrete example of the worksheet is presented in 9. For each goal from the task model, one table has to be filled. The table include both the user goal and the interactive systems configuration (i.e., the interaction technique exploiting specific input and output devices). The table structure (see Fig. 3) is as follows (we only describe here numbered columns in the second row of the table):

- The first column lists the user tasks to be performed to reach the goal.
- The second column exploits the information inside the human-variability feature diagram to describe the identified failure scenarios.
- The third column is filled using the classification form ECSS-Q-ST-30C [8].
- The fourth column identifies the relevant PSFs that can influence the occurrence of human errors in the identified failure scenarios.
- The fifth column presents the observable global effect (phenotype as defined in [12]) of the identified failure scenarios.
- The sixth column identifies links to additional information needed to understand the context of the failure scenarios. In the context of this work, the User Interface and the task descriptions are key.
- The seventh column identifies recommendations to reduce the occurrence and the impact of the failure scenarios. In order to be systematic, these recommendations are structured using the POISE framework: they are studied in terms of People, Organization, Interactive System, and Environment.

4 Applying P-VASA to the Flight Safety Operations CCS

In this section, we apply the P-VASA framework to the Flight Safety Operations-CCS. The first subsection describes, at high level, the current CCS with the POISE framework (first step of the process). The second subsection, explains the need for interactive monitoring and the envisioned interaction technique

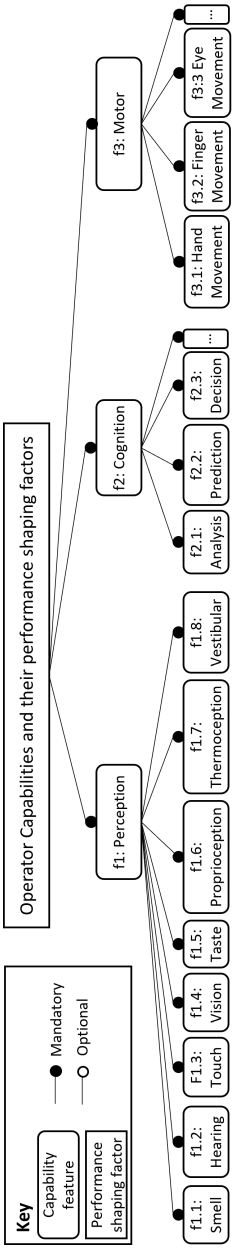

Fig. 2. Generic operator capability model

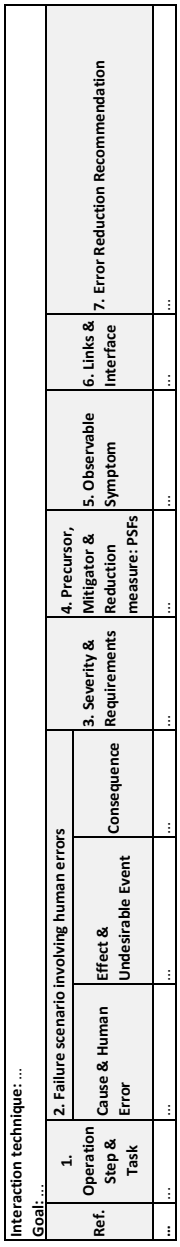

Fig. 3. Human Error Analysis Form sheet headline

(IT). The third subsection describes the task and goal analysis (second step of the process). The fourth subsection presents the operator capabilities analysis

(third step of the process). The fifth subsection presents the safety analysis of the envisioned interaction technique (fourth and last step of the process). Finally, the last subsection presents the lessons learned from this analysis and the solutions that have been envisioned.

4.1 High level Flight Safety Operations CCS POISE Description

Flight Safety Operations belong to the group of critical operations of the spaceport and can be decomposed into several missions carried out to ensure the safety of populations and properties, the protection of public health, and the protection of the environment on the Earth's surface against any damage that may result from the in-flight operation of the launch vehicle. Flight Safety Operations' goal is to ensure the safety of populations and properties, the protection of public health, and the protection of the environment on the Earth's surface against any damage that may result from the in-flight operation of the launch vehicle [4].

The Flight Safety Operations CCS is a complex socio-technical interactive system that can be, at high level, described with the POISE (People, Organization, Interactive System and Environment) framework as follows in next subsections.

People. The Flight Safety Operations team is composed of several operators. In this paper, we focus on the Flight Safety Officer (FSO). The FSO mission during the launch vehicle lift-off is to i) monitor the launch vehicle to assess its dangerousness and ii) intervene if necessary by sending an order on board to neutralize it. The FSO is trained for 3 years to be qualified.

Organization. When focusing on the FSO, the main organization involved is the spaceport leading organization (the CNES), responsible for the safety of operations and takes care of FSO selection, training, qualification, and licensing.

Interactive System. The ground segment interactive Command and Control System, dedicated only to flight safety operations, offers, as main interaction means, an interactive computing system and a physical control panel. In this paper, we focus on the interactive computing system, which exhibits as output a User Interface (UI), representing the launcher parameters, and allows the FSO to zoom in and out using a mouse.

Environment. The FSO works in a dedicated room with a limited light source i.e. under a fully controlled environment not interfering with operations.

4.2 The Need for Interactive Monitoring and Interactive System Description

In this paper, we focus on the tasks that the FSO must perform during the launch mission surveillance that typically lasts around 500 seconds (i.e., about

8 minutes). At any time, the operator is required to perform multiple tasks concurrently and in real-time. First, s/he must assess the potentially dangerous nature of the launcher by monitoring horizontal and vertical trajectories and assessing their deviations from pre-calculated trajectories. Systems providing both launcher tracking and trajectory calculation have to be monitored too. Second, s/he must intervene if necessary to neutralize the launcher. Finally, s/he must deactivate the onboard neutralization system when the total mission time (defined at mission preparation) has elapsed.

The nature of monitoring, which involves examining specific data from specific systems at specific times, makes it difficult to assess whether or not the operator has actually performed the monitoring, as these activities only take place in the operators' head. Providing assurances that the operator monitors the right information at the right time throughout the mission would improve operations' safety as demonstrated in [27].

In this paper, we envision the eye-dwell interaction technique [17] for performing interactive monitoring (defined as a set of monitoring tasks sensed by a device), while reducing to the minimum the evolution of the operators' tasks. Indeed, the eye-dwell interaction technique relies solely on the user's gaze position on a screen detected by an eye-tracking device: the target is activated when the user stares at it for a minimum amount of time.

Fig. 4 depicts the FSO CCS with the eye-dwell interaction technique following the MIODMIT architecture presented in section 2. In this CCS, the operator uses an eye-tracker as input device. The data from the eye-tracker are analyzed by the eye-dwell interaction technique with respect to the UI layout and are transmitted to the interactive application. The interactive application enables to transmit commands to the launcher and all associated ground and on-board segments, and to update the UI layout following the state of the launcher and present it to the operator on the screen (which is the output device).

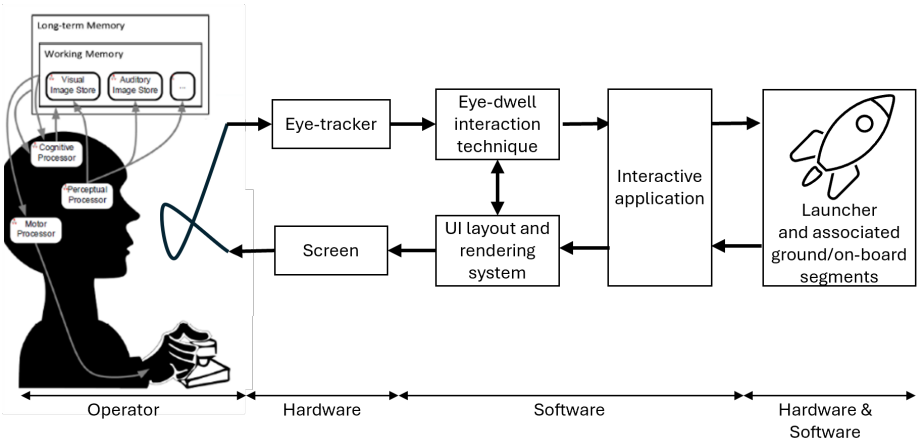

Fig. 4. Simplified architecture of the FSO CCS

Fig. 5 depicts a prototype of the UI layout used by the FSO. For the purposes of this paper, and due to confidentiality concerns, this UI prototype presented is a simplified version of the actual UI used by the operator. Yet, it is sufficiently representative of the layout and visual appearance of the original design. This UI allows the FSO to perform monitoring activities and is composed of several parts that are numbered in blue in the figure: 1) the mission timeline displaying the planned events during the launch, e.g., the separation of a launch vehicle stage, 2) the current time and the launch vehicle detailed coordinates, 3) the status indicators for the resources contributing to the mission, 4) the vertical speed triangle which displays the vertical speed of the launch vehicle, 5) the launch vehicle's horizontal position graph, which displays both the current launch vehicle's position and its nominal path, 6) the launch vehicle's vertical position graph, which displays current launch vehicle's altitude and its nominal path. This UI is decomposed in 18 area of interest (AoI) (e.g., one of the green frames labeled "LABEL") which must be monitored regularly by the operator.

Fig. 6 depicts the rendering corresponding to the eye-dwell interaction technique behavior. The green frame, labeled "LABEL", corresponds to the area of interest (AoI). Frame 1 shows the initial and default state of the AoI when it is idle. When the an operator's gaze is sensed over the AoI, the AoI enters a

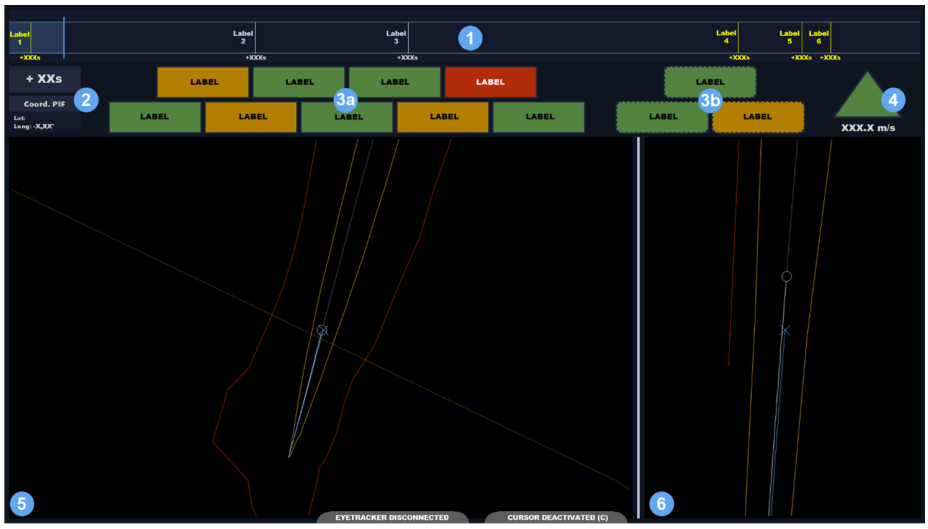

Fig. 5. Prototype of FSO user interface

Fig. 6. Visual rendering of the eye-dwell interaction technique

selected state (Frame 2). While the operator's gazes are sensed over the AoI (the number of gazes sensed over the AoI being less than 15), the visual rendering updates progressively by extending the yellow area on top of the AoI (Frame 3). If the operator's gaze is sensed outside of the AoI (at least one time), the AoI returns to its initial state (Frame 1). Otherwise, if the operator's gaze is sensed over the AoI for a minimum of 15 times, the AOI enters an activated state, meaning that the operator monitored it (Frame 4).

The requirement for the operator's gaze to be detected at least 15 times over the AoI is defined to achieve the optimal selection and activation duration of approximately 300 ms, as recommended by [18] and [22], with respect to the Smart Eye Ai-x eye tracker [30] input device that has a refresh rate of 16 ms for capturing the user's gaze.

This complex behavior requires dedicated formal description technique. Due to space constraints, we do not present the formal model of the eye-dwell IT but the same zero-default approach as in [24] has been exploited to verify safety and liveness properties of the model.

4.3 Task and Goal Analysis

At the interaction technique level, the operator performs low level tasks such as i) activate AoI, ii) during an AoI activation, switching to another AoI activation, iii) during an AoI activation, canceling this activation, ... Fig. 7 presents the low-level HAMSTERS tasks model that has been produced during the task and goal analysis step for the "activate AoI" task which is presented on top of the figure. This task is related to the eye-tracker input device, the screen output device, the FSO application, the UI layout, the eye-dwell interaction technique, and the launcher physical object. This task is composed of a sequence of tasks (represented by the ">>" operator). First the operator locates the corresponding AoI (abstract task "Locate AoI") and decides to initiate it's activation (cognitive decision task "Decide to initiate AoI selection"). Then s/he iteratively (for 15 times) look at the AoI to activate it (iterative abstract task "Initiate and continue selection"). This task is composed of: i) a sight task (" "Perceive AoI"), ii) a cognitive analysis task "Analyse AoI is selected with a progression level", iii) a cognitive decision task "Decide to maintain gaze on AoI until activation", iv) an input task "Sense gaze on AoI", v) a system task ("Compute AoI new selection progression level", and vi) an output task "Update AoI selection progression level". Then, the system activates the AoI (system task "Activate AoI") and updates the AoI rendering (output task "Show AoI activation"). This enables the operator to perceive the color change (sight task "Perceive AoI") and to analyse that is has been activated (cognitive analysis task "Analyse AoI is activated").

4.4 Operator Capabilities Analysis

Fig.8 depicts the model of the operator capabilities and their performance shaping factors that has been produced during the operator capabilities analysis step. The three first lines decompose the operator capabilities following the human

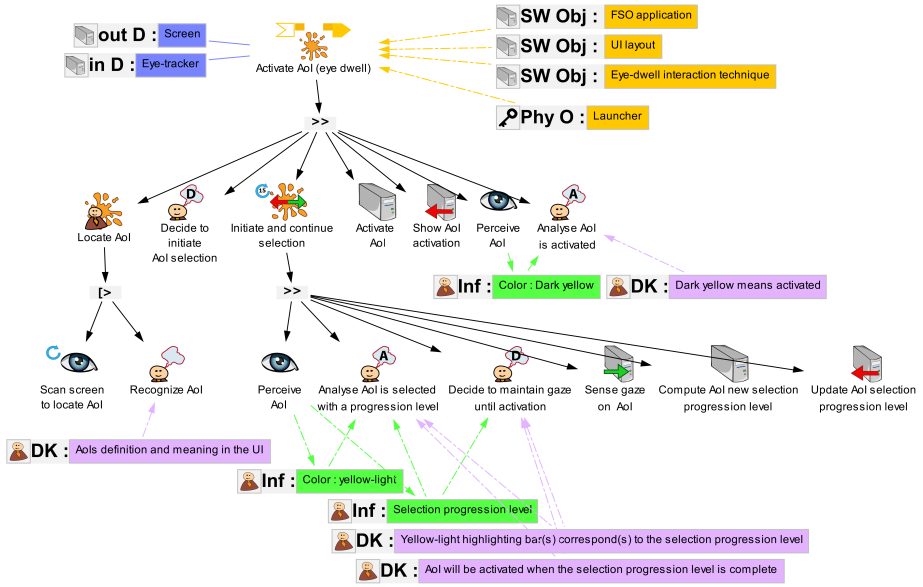

Fig. 7. HAMSTERS task model for "AoI activation" task with eye-dwell IT

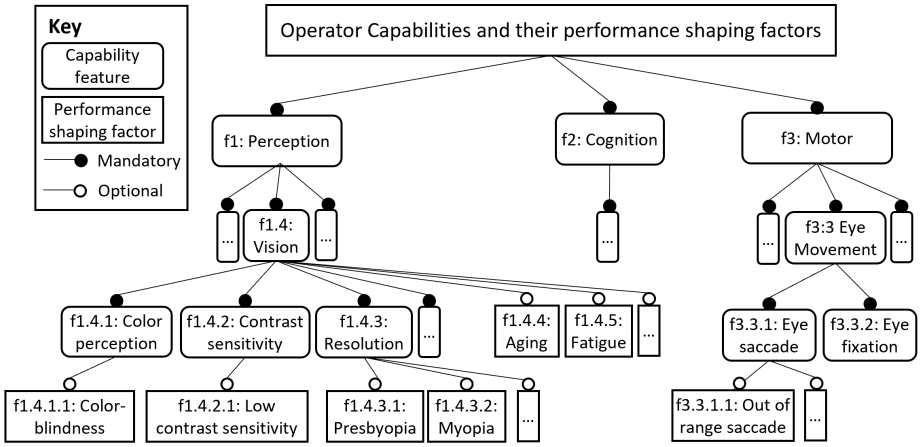

Fig. 8. Operator capabilities and their PSFs feature model-like

processor model [3] and the fourth line describes the performance shaping factors (PSFs) that may impact them. In this illustrative example, we focus on the capabilities that can influence the interaction using the eye-tracker input device: mainly the vision (perception) and the eye movements (motor), we thus only detail these capabilities and their PSFs. In this study, the PSFs that may impact the operator capabilities are classified as internal natural perceptive and

motor non-malicious and non-deliberate faults following [25] classification. The vision is composed (among others) of color-perception, which can be impacted by color-blindness, contrast sensitivity which can be impacted by a low contrast sensitivity and resolution which can be impacted by PSFs such as presbyopia or myopia. Finally, the vision might be impacted by PSFs such as aging and fatigue. On the motoric side, the eye movements are composed of two types of movements: the eye saccade and the eye fixation [2]. The eye saccade can be impacted by an out of range saccade.

4.5 Safety Analysis of the Eye-Dwell Interaction Technique

When considering the AoI activation task, we identified three potential failures: i) *wrong target activation*: the operator activates the wrong AoI, ii) *missed target activation*: the operator does not succeed in activating the AoI, and iii) *loss of situation awareness*: the operator is not aware of the state of the AoI with respect to its activation.

Fig. 9 presents an excerpt of the application of the human-variability aware safety analysis framework for this task. The user task studied here is the first sight task "Perceive AoI" from the task model in Fig. 7.

We detail here only the first white row as an illustrative example; the following rows present other failure scenarios applied to the same task. For this task, we inspect the operator model and see that eye movements are composed of eye fixations and eye saccades. According to this, we envision a failure scenario caused by an eye saccade, where an unintended saccade implies that the operator's gaze is sensed outside of the AoI. In that case, the effect and undesirable event is the fact that, when one gaze is sensed outside of the AoI, the progression towards activation is canceled. This implies that the operator does not succeed in activating the AoI and the possible related observable symptoms are i) a slower work performance: the operator need to re-start the AoI activation, or ii) an attention tunneling on the AoI activation: the operator is stuck in trying to activate the AoI and thus have less time to focus on the launcher trajectory. The first consequence would have a minor impact on the mission and could be classified as "4. Minor", however, the second consequence could have a catastrophic impact if the operator does not perform correctly the monitoring of the launcher trajectory. This is why this failure scenario is classified as "1. Catastrophic". As error reduction recommendation, we propose to act on i) the operator (P) via training to have less saccade, ii) the organization (O) by checking the means to mitigate the PSFs impacting eye saccade, and iii) the interactive system (IS) by adding eye saccade tolerance inside the interaction technique.

4.6 Lessons Learned

The P-VASA framework enabled us to identify, with a systematic approach, the operators' capabilities involved when interacting with the CSS and their possible variabilities. This identification enables us to assess the safety of the CSS with respect to these capabilities and their variabilities.

Interaction technique: eye-dwell basic (input devive: eye-tracker ; output device: screen)
Goal: Activate AoI

Ref.	1. Operation Step & Task	2. Failure scenario involving human errors			3. Severity & Requirements	4. Precursor, Mitigator & Reduction measure: PSFs	5. Observable Symptom	6. Links & Interface	7. Error Reduction Recommendation
		Cause & Human Error	Effect & Undesirable Event	Consequence					
1	Perceive AoI	Eye saccade & the operator performs an unintended eye saccade outside of the AoI	One gaze sensed outside of the AoI by the system cancels progression towards activation	Missed target	1 - Catastrophic	All PSFs influencing saccade and fixation point (e.g., fatigue)	i) slower work performance, or ii) attention tunneling on AoI	Task model UI layout	**(P)** Train operator to have less saccade **(O)** Check means to mitigate PSFs impact **(O)** Select people with mimimum saccade **(IS)** Add saccade tolerance inside the interaction technique **(E)** N/A
2	Perceive AoI	Resolution issue(s) & the operator wears glasses to correct them	The interactive system is not able to sense the operator gazes	Missed target	1 - Catastrophic	All PSFs influencing resolution issues and glasses wearing (e.g., fatigue)	More time than needed to activate an AoI - Slow work performance	Task model UI layout	**(P)** Remove glasses if possible **(O)** Disqualify the operator **(IS)** Choose an interaction technique without eye-tracker input device **(IS)** Use an eye-tracker technology tolerant to glasses **(E)** N/A
3	Perceive AoI	Color-blindness & the operator does not perceive correctly AoI colors	The operator is not able to see the highlighting progression towards AoI activation	Loss of situation awareness	1 - Catastrophic	N/A	More time than needed to activate an AoI - Slow work performance	Task model UI layout	**(P)** Train operator to work without the colors **(P)** Wear glasses to correct the color-blindness **(O)** Disqualify the operator **(IS)** Set appropriate highlithing color **(E)** N/A
4	Perceive AoI	Low contrast sensitivity & the operator does not perceive correctly AoI colors	The operator is not able to see the highlighting progression towards AoI activation	Loss of situation awareness	1 - Catastrophic	N/A	More time than needed to activate an AoI - Slow work performance	Task model UI layout	**(P)**Train operator to work without contrast **(O)** Disqualify the operator **(IS)** Increase the contrast **(E)** N/A
...	...	...	...	...	...	...	...	...	...

Fig. 9. Excerpt of the Human Error Analysis Form sheet of the safety analysis of the eye-dwell IT

In this illustrative example, we identified, thanks to the P-VASA framework, that the eye-dwell interaction technique as defined here is impacted by natural eye saccades of the operator. Several error reduction recommendations were identified, in a systematic manner, in terms of operator (P), organization (O), interactive system (IS),and environment (E).

Some identified error reduction recommendations require evolutions on the operator and/or the organizations. However, changes on the operator are sometimes impossible to perform as demonstrated in the case of interactions with touch screens under turbulence [24]. In the same way, disqualifying the operator may result in losing the competencies of the existing users and might not be feasible neither. This often leaves the interaction technique the only place where error tolerance can take place.

In this illustrative example, we focused on the interaction technique and investigate how to make it tolerant to eye saccades. This lead to the identification of novel interaction techniques such as the gaze-lock interaction technique [27].

5 Conclusion and Future Work

In this paper, we proposed a novel safety analysis framework, called P-VASA (for People-Variability-Aware Safety Analysis) which focuses on the People side of the POISE framework. The generic objective of the framework is to assess interactive systems in the context of critical operations. More specifically, P-VASA supports the assessment of interactive technologies and their capability to prevent and tolerate human errors at operation time. In order to do this analysis in an exhaustive manner, we proposed to structure the analysis according to the tasks that the operators have to perform on the interactive system. For each task, we assess the operators' capabilities involved, the possible variability of operators' in terms of perceptive, cognitive and motor behaviors as well as how interactive technologies are able to tolerate (or not) operators' errors.

This framework can also support the design of new interactive technologies by providing requirements on the types of human errors that need to be accounted for to avoid operators' failures and thus improve safety of the overall operations.

We applied our framework to analyze the future Command and Control System (CCS) for Flight Safety Operations of launchers at ESA spaceport in Kourou. More precisely we focused on monitoring tasks and on the benefits of using eye-tracking technologies to capture operators' activities while monitoring launchers. This analysis lead us to the definition of possible improvements to include fault-tolerance at the interaction technique (IT) level and demonstrated the importance of the low-level behavior of the IT in terms of dependability of the entire CCS which we describe using a Petri-net based zero-default approach. We have only shown a small subset of the analysis (due to space constraints) but the analysis covers several ITs (with and without eye-tracker) for the entire set of operators' monitoring tasks.

Assessing the effectiveness of the P-VASA framework is a real challenge as it is for similar approaches (e.g., FMECA). However, it does not prevent such ap-

proaches to be widely used as the information provided supports safety analysis work. In terms of hazard coverage, the P-VASA framework provides, by design, a systematic coverage all the relevant aspects of human errors related to the use of input/output devices and their associated interaction techniques. This systematic coverage is ensured by the fact that the proposed operator capabilities model is based on an exhaustive human error and fault taxonomy [25].

Future work, aims at covering the other parts of the POISE framework and especially the Organization component because it is a significant source of faults leading to human failures in operations as demonstrated in [31]. In a long-term future, this would lead to POISE-VASA, where the modelling of the variability would become explicit within the different POISE elements.

Given the rising awareness of the importance of considering fitness to work (see for instance [9]) and the rising awareness related to mental harm (see, for instance, [15, 10]), in future we also intend to develop the characterization of the cognitive variability, since we strongly believe that mental harm will be taken into consideration during the risk management process.

Acknowledgments. This work was partially funded by the project CNES 21055/00. B. Gallina was funded by a CIMI grant and Software Center (project#60).

References

1. Avizienis, A., et al.: Basic concepts and taxonomy of dependable and secure computing. transactions on dependable and secure computing **1**(1), 11–33 (2004)
2. Bahill, A., et al.: The main sequence, a tool for studying human eye movements. Mathematical Biosciences **24**(3), 191–204 (1975)
3. Card, S.K., et al.: The Psychology of Human-Computer Interaction. L. Erlbaum Associates Inc., USA (1983)
4. CNES: French space operations act. n° 2008-51
5. Cronel, M., et al.: Miodmit: a generic architecture for dynamic multimodal interactive systems. In: Int. Conf. on Human-Centred Software Engineering. pp. 109–129. Springer (2018)
6. Diaper, D., Stanton, N.: The handbook of task analysis for human-computer interaction (2003)
7. European Cooperation for Space Standardization (ECSS): ECSS-Q-HB-30-03A, Space product assurance - Human dependability handbook. (2015)
8. European Cooperation for Space Standardization (ECSS): ECSS-Q-ST-30C, Space product assurance - Dependability. (2017)
9. Folke, F.: Fit for flight? Working conditions and mental health as integrated safety risks in European aviation. Tech. rep., Karolinska Institutet (4 2026)
10. Gallina, B.: Safety of the Intended Functionality: What about Mental Harm? In: CARS@EDCC2024 Workshop - Critical Automotive applications: Robustness & Safety. Leuven, Belgium (Apr 2024), https://hal.science/hal-04558509
11. Gallina, B., et al.: Towards safety risk assessment of socio-technical systems via failure logic analysis. In: 2014 IEEE Int. Symp. on Software Reliability Engineering Workshops. pp. 287–292. IEEE (2014)
12. Hollnagel, E.: The phenotype of erroneous actions. Int. Journal of Man-Machine Studies **39**(1), 1–32 (1993)

13. Hollnagel, E.: From function allocation to function congruence. Ashgate (1999)
14. Kang, K., et al.: Feature-oriented domain analysis (foda) feasibility study. Tech. Rep. CMU/SEI-90-TR-021 (Nov 1990)
15. de La Vara, J.L., Gallina, B., Fernández-Caballero, A., Molina, J.P., García, A.S., Ayora, C.: Assurance of software-intensive medical devices: What about mental harm? In: 53rd IEEE/IFIP Int. Conf. on Dependable Systems and Networks - Supplemental Vol. (DSN-S). pp. 168–172 (2023)
16. Lacaze, X., et al.: Performance evaluation as a tool for quantitative assessment of complexity of interactive systems. In: Int. Workshop on Design, Specification, and Verification of Interactive Systems. pp. 208–222. Springer (2002)
17. Majaranta, P., Räihä, K.J.: Twenty years of eye typing: systems and design issues. In: Proc. of the 2002 symposium on Eye tracking research & applications. pp. 15–22 (2002)
18. Majaranta, P., et al.: Fast gaze typing with an adjustable dwell time. In: Proc. of the sigchi conf. on human factors in computing systems. pp. 357–360 (2009)
19. Martinie, C., et al.: Task model-based systematic analysis of both system failures and human errors. IEEE Trans. on Human-Machine Systems **46**(2), 243–254 (2015)
20. Martinie, C., et al.: Analysing and demonstrating tool-supported customizable task notations. Proc. ACM Hum.-Comput. Interact. **3**(EICS) (Jun 2019)
21. Montecchi, L., Gallina, B.: SafeConcert: A metamodel for a concerted safety modeling of socio-technical systems. In: Int. Symp. on Model-Based Safety and Assessment. pp. 129–144. Springer (2017)
22. Mutasim, A.K., et al.: Pinch, click, or dwell: Comparing different selection techniques for eye-gaze-based pointing in virtual reality. In: Acm symposium on eye tracking research and applications. pp. 1–7 (2021)
23. Palanque, P.: Poise: a framework for designing perfect interactive systems with and for imperfect people. In: IFIP Conf. on Human-Computer Interaction. pp. 39–59. Springer (2021)
24. Palanque, P., et al.: Brace touch: A dependable, turbulence-tolerant, multi-touch interaction technique for interactive cockpits. In: Computer Safety, Reliability, and Security - 38th Int. Conf., SAFECOMP 2019, Proc. LNCS, vol. 11698, pp. 53–68. Springer (2019)
25. Palanque, P., et al.: A classification of faults covering the human-computer interaction loop. In: Computer Safety, Reliability, and Security - 39th Int. Conf., SAFECOMP 2020, Proc. LNCS, vol. 12234, pp. 434–448. Springer (2020)
26. Reason, J.: Human error. Cambridge Univ. Press (1990), iSBN: 9780521314190
27. Rodriguez-Hernando, D., et al.: Tracking monitoring activities of operators to ensure operations safety: Application to monitoring & control of launcher tracking activities at europe's spaceport (2025)
28. Shappell, S.A., Wiegmann, D.A.: The human factors analysis and classification system–HFACS. Tech. rep., Civil Aeromedical Institute (2000)
29. Sheikh Bahaei, S., Gallina, B.: Augmented reality-extended humans: towards a taxonomy of failures – focus on visual technologies. In: European Safety and Reliability Conf. (ESREL). Research Publishing, Singapore (2019)
30. SmartEye: Smart eye ai-x eye tracker webpage, https://www.smarteye.se/ai-x/
31. Sujan, M.: An organisation without a memory: a qualitative study of hospital staff perceptions on reporting and organisational learning for patient safety. Reliability engineering & system safety **144**, 45–52 (2015)
32. Wiegmann, D.A., Shappell, S.A.: A human error approach to aviation accident analysis: The human factors analysis and classification system. Routledge (2017)