This project has received funding from the European Union's Horizon 2020 research and innovation programme under grant agreement No 861111

Drones4Safety

Research & Innovation Action (RIA)

Inspection Drones for Ensuring Safety in Transport Infrastructures

Preliminary Hazard Analysis

D2.1

Due date of deliverable: 31.08.2020

Start date of project: June 1st, 2020

Type: Deliverable
WP number: WP2

Responsible institution: NEAT S.r.l.
Editor and editor's address: Simone Cabasino, NEAT S.r.l.

This project has received funding from the European Union's Horizon 2020 research and innovation programme under grant agreement No 861111

Version 1.0
Release Date: September 14, 2020

Project funded by the European Commission within the Horizon 2020 Programme		
Dissemination Level		
PU	Public	✓
CO	Confidential, only for members of the consortium (including the Commission Services)	

Change Log

Rev.	Date	Who	Site	Change
0.1	01/08/2020	Simone CABASINO	NEAT	Created initial draft.
0.2	27/08/2020	Simone CABASINO	NEAT	More content added
0.3	10/09/2020	Simone CABASINO Mario GULIA	NEAT	Candidate release presented to and shared with Technical Steering Committee members
0.4	14/09/2020	Andrea DEL SOLE Damiano TAURINO Anastasiia SOBCHENKO Martin POLOSKEY	NEAT DBL ECTL ARIC	Final internal review
1.0	14/09/2020	Andrea DEL SOLE	NEAT	First issue, reviewed with Project Coordinator

1 Executive Summary

This deliverable encompasses 4 Sections, including this one. Section 2 contains an Introduction, describing the objective of the document. Section 3 resume the Preliminary Hazard Analysis methodology used within this document, whereas Section 4 contains the Preliminary Hazard Analysis for the D4S System and, in particular, presents the identified hazards and the corresponding mitigations. Finally, Section 5 presents the future work stemming from this deliverable during the project execution.

Contents

List of Figures

List of Tables

Acronyms

Acronym	Description
AI	Artificial Intelligence
ANSP	Air Navigation Service Provider
BVLOS	Beyond Visual Line of Sight
CAA	Civil Aviation Authority
CDHA	Conceptual Design Hazard Analysis
D4S	Drones4Safety
DDHA	Detailed Design Hazard Analysis
DHA	Direct Hazard Analysis
EASA	European Aviation Safety Agency
EC	European Commission
EGNSS	European Global Navigation Satellite System
ETA	Event Tree Analysis
FMEA	Failure Modes and Effects Analysis
GNSS	Global Navigation Satellite System
GPS	Global Positioning System
HAZOP	HAZard and Operability Analysis
HDHA	Human Design Hazard Analysis
HW	Hardware
INS	Inertial Navigation System
ISO	International Standard Organisation
K_p	See “Definitions”
MHA	Major Hazard Analysis
ML	Machine Learning
NA	Not Applicable
NOTAM	Notice To AirMen
OHA	Operations Design Hazard Analysis
PDHA	Preliminary Design Hazard Analysis
PHA	Preliminary Hazard Analysis
PHR	Process Hazard Review
RAMS	Reliability, Availability, Maintainability and Safety
RDHA	Requirements Design Hazard Analysis
RFC	Request For Comments
SDHA	System Design Hazard Analysis
SIL	Safety Integrity Level
SORA	Specific Operations Risk Assessment
SW	Software
UAS	Unmanned Aircraft System
UI	User Interface
VLOS	Visual Line of Sight

Definitions

In the following, the definition of some terms used in the document is provided.

Term	Description
Harm	Physical injury or damage to persons, property, and domestic animals.
Hazard	Something with the potential cause harm. A hazard can take many forms, such as a substance (e.g. chemicals), an energy source (e.g. a drone flying or a train moving, or a current/voltage, or a noise, or a machinery with moving or hot parts) or an existing work practice or process (e.g. working up a ladder or a platform), etc.
Hazardous event	Any event that can cause harm.
Hazard zone	Any space within and/or around the source of a hazard in which persons, or domestic animals can be exposed to a hazard.
Hazardous state	The condition of being under a hazard.
Tolerable hazard rate	Hazar rate which guarantees that the resulting risk does not exceed a target individual risk (see [RD-1]).
Risk	Chance, high or low, that any hazard will actually cause somebody harm. In other words, risk is the probability or chance that someone may suffer injury or illness due to an existing hazard. When dealing with risks, two aspects shall be considered: likelihood and severity.
Likelihood	State of being probable or chance of a threat occurring.
Severity	Simple metric (code) assigned to hazards, or problems, or known errors, indicating the seriousness of their effects on someone.
Risk reduction	Reduction of the risk (residual risk) to an acceptable level
SIL	Safety Integrity Level: a relative level of risk-reduction provided by a safety function, or to specify a target level of risk reduction (see [RD-1])
Protective measure	Any measure intended to achieve adequate risk reduction, implemented: • by the designer (inherent design, safeguarding and complementary protective measures, information for use); and • by the user (organization: safe working procedures, supervision, training; permit-to-work systems; provision and use of additional safeguards; use of personal protective equipment).
(System) Safety	Application of engineering and management principles, criteria, and techniques to achieve acceptable mishap risk, within the constraints of operational effectiveness and suitability, time, and cost, throughout all phases of the system life cycle (see [RD-2]).
Safe state	State of the system where the tolerable hazard is guaranteed.
K_p-index	Weighted average of K-indices from a network of 13 geomagnetic observatories at mid-latitude locations. K-index quantifies disturbances in the horizontal component of Earth's magnetic field with an integer in the range 0÷9, with 1 being calm and 5 or more indicating a geomagnetic storm.
Aicraft	Any machine that can derive support in the atmosphere from the reactions of the air other than the reactions of the air against the earth's surface. This class of air vehicles includes airplanes, drones, helicopters, airships (including blimps), gliders, paragliders, parachuting, paramotors, hot air balloons, regardless to the fact that they are civil, commercial, or military.
Ground moving vehicles	Any machine that move on ground.

	This class of vehicles includes trains and other railway vehicles (such as platforms, measurements trains, service vehicles, etc), cranes, lorries, cars, etc. (moving either on or near the tracks or on the (road) bridges and viaducts).

References

Parent Documents

The Parent Documents establish the criteria and technical basis for the existence of this document. The D4S Parent Documents are listed in the following table.

Reference	Code	Title
[PD-1]	DoA	Drones4Safety Description of Action

Applicable Documents

Applicable Documents are those documents whose content are considered to form a part of this document. The specified parts of the Applicable Documents carry the same weight as if they were stated within the body of this document. The D4S Applicable Documents are listed in the following table.

Reference	Code	Title
[AD-1]	SRD	D4S – D2.3 – System Requirements Document – v1.0 – 2020-08-31
[AD-2]	RGBA	D4S – D2.2 – Regulatory Gap/Barriers Analysis – v1.0 – 2020-09-14

Reference Documents

Reference Documents are those documents that, although not a part of this document, serve to amplify or clarify its contents, or dictate work policy or procedures. The D4S specific Reference Documents are listed in the following table.

Reference	Code	Title
[RD-1]	IEC61508	International Electrotechnical Commission (IEC) – IEC 61508-1:2010 “Functional safety of electrical/electronic/programmable electronic safety-related systems - Part 1: General Requirements” – Ed. 1.0 – 2010-04
[RD-2]	MIL-STD-882D	Department of Defense Standard Practice – MIL-STD-882E: System Safety – Version E –2012-05-11.
[RD-3]	EN50126	European Committee for Standards - Electrical – EN 50126-1:2017 “Railway Applications - The Specification and Demonstration of Reliability, Availability, Maintainability and Safety (RAMS) - Part 1: Generic RAMS Process”
[RD-4]	ISO31000	International Organization for Standardization – ISO/IEC 31000:2018 “Risk management — Guidelines” – Ed. 2 – 2018-02
[RD-5]	ISO31010	International Organization for Standardization – ISO/IEC 31010:2019 “Risk management — Risk assessment techniques” – Ed. 2 – 2019-06
[RD-6]	ISO17666	International Organization for Standardization – ISO 17666:2016 “Space Systems Risk Management” – Ed. 2 – 2016-11
[RD-7]	HAT4SS	Ericson, Clifton A. – Hazard analysis techniques for system safety – John Wiley & Sons, Inc. – 2005 – ISBN 0-471-72019-4
[RD-8]	HAZOP	ISO/IEC 61882:2016 RLV “Hazard and operability studies (HAZOP studies) - Application guide” – Ed. 2 – 2016-03-10

[RD-9]	SORA	Joint Authorities for Rulemaking of Unmanned Systems (JARUS) – JARUS guidelines on Specific Operations Risk Assessment (SORA) – Id. JAR-DEL-WG6-D.04 – Ed. 2 – 2019-01-30 http://jarus-rpas.org/content/jar-doc-06-sora-package (Accessed: 14/09/2020)
[RD-10]	EASA05	European Union Aviation Safety Agency – Opinion No 05/2019 “Standard scenarios for UAS operations in the ‘specific’ category” (RMT.0729) https://www.easa.europa.eu/document-library/opinions/opinion-052019 (Accessed: 14/09/2020)
[RD-11]	EC947	European Commission – Commission Implementing Regulation (EU) 2019/947 of 24 May 2019 on the rules and procedures for the operation of unmanned aircraft of 24 May 2019 – EC 947/2019 https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A32019R0947 (Accessed: 14/09/2020)
[RD-12]	CCO	CORUS - Concept of Operations (ConOps) https://www.sesarju.eu/node/3411 (Accessed: 14/09/2020)
[RD-13]	MEDUSA	CORUS - Concept of Operations for European UTM Systems - D3.1 Initial Contingencies & Connstraints https://ec.europa.eu/research/participants/documents/downloadPublic?documentIds=080166e5bdb8e5a5&appId=PPGMS (Accessed: 14/09/2020)
[RD-14]	EIXL	Jarefors H. – “Euro-Interlocking – modified signalling hazard lists” – v. 0.2 - 2000
[RD-15]	ITS2005	Drewes J., May J., Schneider E.: “Structured approach of a generic (signalling) hazard list for railway (interlocking) systems” – Proceeding of ITS Conference 2005 in Hannover

2 Introduction

The Drones4Safety (D4S) project aims to increase the safety of the European civil transport system by building a cooperative, autonomous, and continuously operating drone system that will be offered to railway and bridge operators to inspect their transportation infrastructure accurately, frequently, and autonomously. The Drones4Safety approach will design energy harvesters to tap energy from the electricity infrastructures of railways and power lines to recharge drones. The project will use satellite and open maps to identify the parts of the transport infrastructure that lays near the electricity infrastructure and feed that information to its drones for scheduling their autonomous missions. The project will develop and improve the state-of-the-art Artificial Intelligence (AI) / Machine Learning (ML) algorithms to optimize the inspection results onboard of the drone. The project will build a swarm drone system that uses advanced long-range communication network techniques to inspect different parts of the infrastructure at the same time. Navigation based on EGNOS/Galileo GNSS will improve accuracy of geo-location of inspection events. The project outcomes will be offered to the transportation operators in forms of software services and hardware drone system. The project brings together leading industrial, research, and academic experts in infrastructure inspection, energy harvesting, AI/ML, communications, and drone technology. Two use-cases for bridge and railway inspections will be conducted to evaluate the project outcomes.

Being the project encompassing two safety[1]-related environments, railways and aviation, an analysis of the hazards[1] shall be performed (see [RD-3], [RD-4], [RD-5], [RD-6] and [RD-7]).

The causal dependencies between harm[1] (damage), potential damage (hazardous state[1]) and the hazardous events[1] (or hazardous conditions) are shown in the following picture.

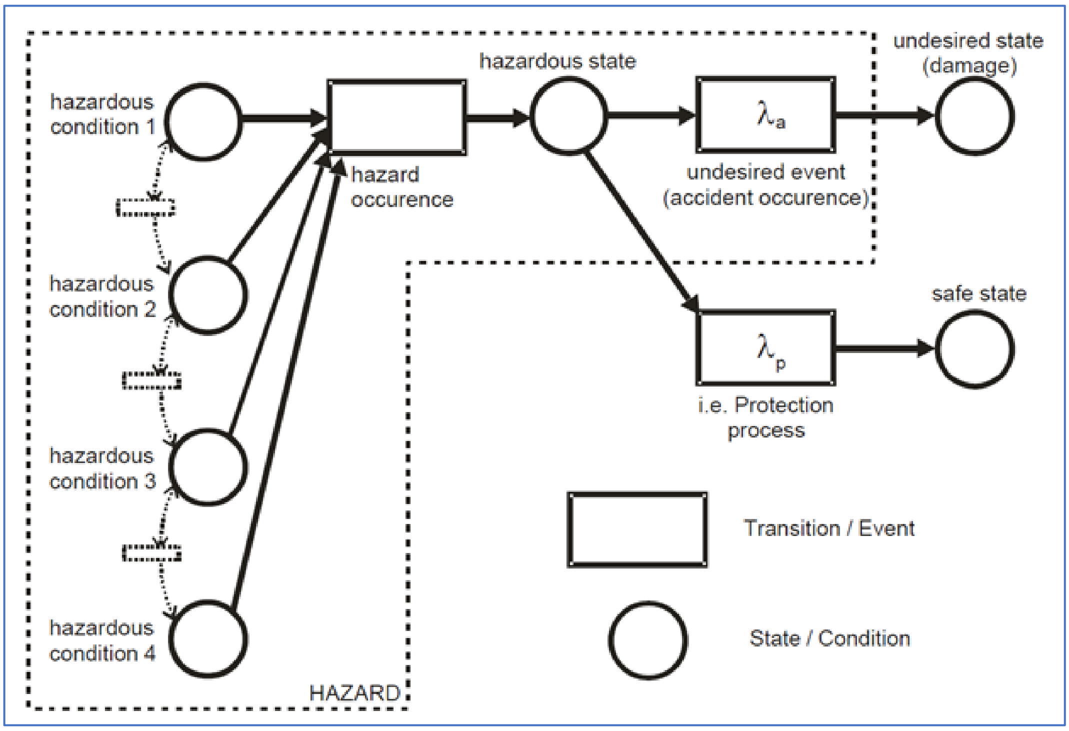

Figure 1 – Causal dependency analysis for a robust hazard definition

[1] See Definitions.

A safe system, i.e. a system which implements the diagnostic and protective countermeasure adequate to the target Safety Integrity Level (SIL[1]), shall react to a hazardous state[1] generated by malfunctioning or other hazardous events[1] by let the system go into a predefined safe state[1].

Traditionally, hazard identification has been performed by domain experts by virtue of their specific knowledge and experience of the domain itself, also coming from the study of past accidents. Today, several types of hazard analysis methodologies exist (see [RD-7]), some of general applicability, such as HAZard and OPerability (HAZOP) Analysis (see [RD-8]), Major Hazard Analysis (MHA), Direct Hazard Analysis (DHA), Process Hazard Review (PHR), Failure Modes and Effects Analysis (FMEA), Event Tree Analysis (ETA), some of specific applicability to a given domain, such as Specific Operations Risk Analysis (SORA) (see [RD-9], [RD-10] and [RD-11]) and MEDUSA (see [RD-12] and [RD-13]). All of these can be used to perform the hazard analysis at every stage of the project. In particular, during D4S Project validation, we will make use of applicable standard scenarios and SORA, MEDUSA and other methodologies (where applicable) to assess the drone operations.

Hazard analysis may be performed during specific phases of the system lifecycle, and thus we may have as Conceptual Design Hazard Analysis (CDHA), Preliminary Design Hazard Analysis (PDHA), Detailed Design Hazard Analysis (DDHA), System Design Hazard Analysis (SDHA), Operations Design Hazard Analysis (ODHA), Human Design Hazard Analysis (HDHA), Requirements Design Hazard Analysis (RDHA), etc.

By the way, domain specific hazard lists, derived from accumulated experience, do exist, such as the one for railway signalling systems (see [RD-14] and [RD-15]).

In this document we will describe and perform a Preliminary Hazard Analysis (PHA) (see [RD-7]) by applying the Major Hazard Analysis (MHA) methodology.

PHA is typically used to evaluate hazards in the early stage of a project, when the system design is still in its initial phase and/or its operating procedures are not yet detailed, and it represents an ancillary tool of the system design review.

With the MHA methodology we will identify the top hazards for the D4S System, provide a preliminary categorisation, analysis and description of the identified hazards/hazardous states, and also define possible countermeasures and mitigations.

3 Hazard Analysis Methodology

The method used is "top-down", applied on the black-box description of the D4S System. In the analysis, only the deviations that could have a system hazardous effect have been evaluated.

The Hazard Analysis Methodology, in particular the one used in PHA, foresees to define hazard checklist, which should include:

1. Energy sources
2. Hazardous functions
3. Hazardous operations
4. Hazardous components
5. Hazardous materials
6. Lessons learned from similar types of systems
7. Undesired mishaps
8. Failure mode and failure state considerations

The PHA process which is followed is described in the following picture:

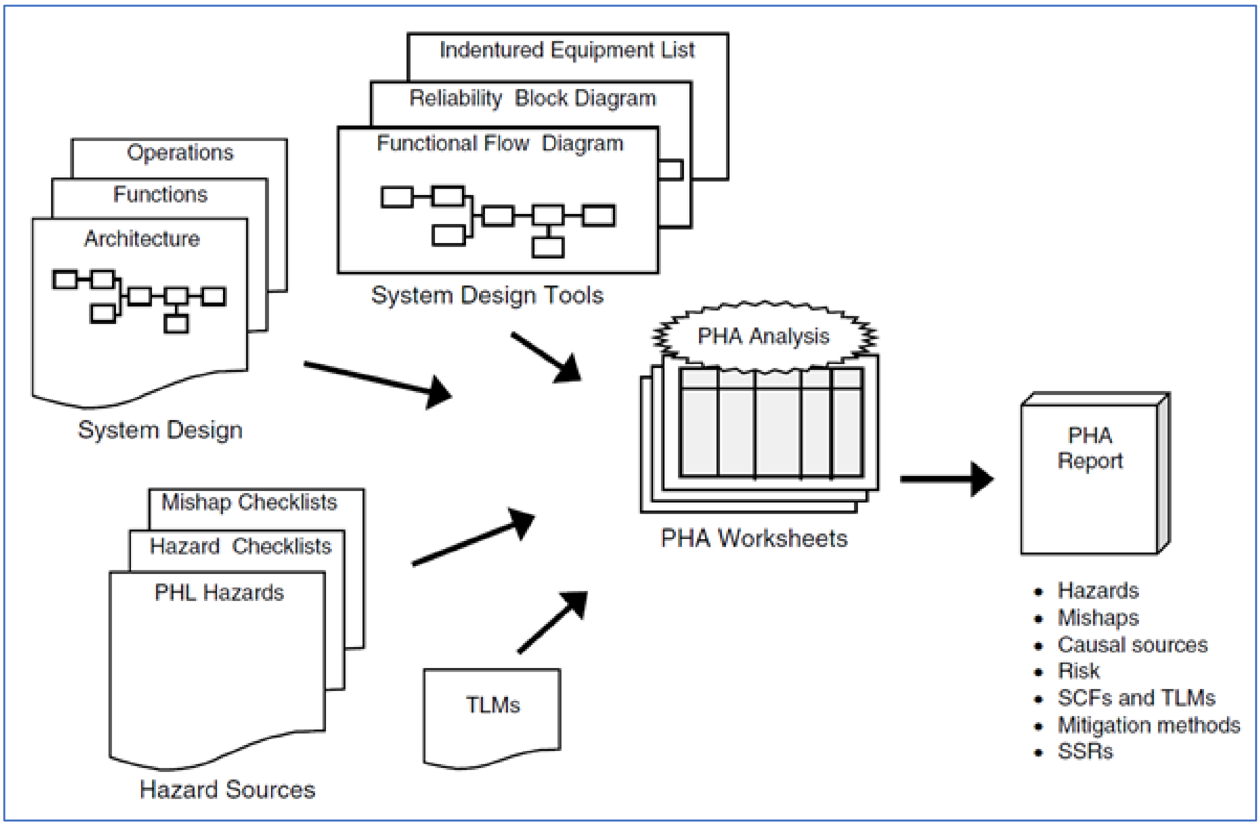

Figure 2 – Preliminary Hazard analysis methodology (see [RD-7])

The methodology foresees the following steps:

- Processes decomposition
- Process hazards and hazardous states identification

- Causes listing
- Consequences specification
- Criticality ranking
- Recommendations and/or mitigations identification

3.1 Risk Classification

The risk classification is performed in accordance with indication and procedure reported in EN 50126 standard (see [RD-3]) in terms of combination of Likelihood[1] and associated Severity[1] Levels.

It should be noted that Likelihood and Severity Levels, presented in the following tables, are derived from analyst experience and by common sense considerations.

Likelihood Level	Description	Definition	Frequency
6	**FREQUENT**	Likely to occur frequently. The hazard will be almost continually experienced	$f \geq 100$ / year
5	**PROBABLE**	Will occur several times. The hazard can be expected to occur often	$1 \leq f < 100$ / year
4	**OCCASIONAL**	Likely to occur several times. The hazard can be expected to occur several times	$10^{-2} \leq f < 1$ / year
3	**REMOTE**	Like to occur sometimes in the system life cycle. The hazard can be reasonably expected to occur a few times over the system life	$10^{-4} \leq f < 10^{-2}$ / year
2	**IMPROBABLE**	Unlikely to occur but possible. It can be assumed that the hazard may exceptionally occurs during the system life	$10^{-6} \leq f < 10^{-4}$ / year
1	**INCREDIBLE**	Extremely unlikely to occur. It can be assumed that the hazard may not occur during the whole system life	$f < 10^{-6}$ / year

Table 1 – Hazard Likelihood Levels

Severity Level	Description	Definition	Consequence to service
4	**CATASTROPHIC**	Fatalities and/or multiple severe injuries and / or major damage to the environment	Loss of system service
3	**CRITICAL**	Single fatality and/or severe injury and/or significant damage to the environment	Loss of major subsystem
2	**MARGINAL**	Minor injury and/or significant threat to the environment	Severe subsystem(s) damage
1	**INSIGNIFICANT**	Possible minor injury	Minor subsystem damage

Table 2 – Hazard Severity Levels

The risk levels are defined in the following table:

Risk Level	Description	Definition
R1	INTOLLERABLE	Shall be eliminated
R2	UNDESIRABLE	Shall only be accepted when risk reduction is impracticable
R3	TOLERABLE	Acceptable with adequate control
R4	NEGLIGIBLE	Acceptable

Table 3 – Risk Levels

The equivalent incident for hazard consequences are obtained by combining Hazard Likelihood and Severity to obtain a Risk Ranking Matrix, as show in the following table.

Likelihood Level			Risk Levels			
6	Frequent	$f \geq 100$ / year	R2	R1	R1	R1
5	Probable	$1 \leq f < 100$ / year	R3	R2	R1	R1
4	Occasional	$10^{-2} \leq f < 1$ / year	R3	R2	R2	R1
3	Remote	$10^{-4} \leq f < 10^{-2}$ / year	R4	R3	R2	R2
2	Improbable	$10^{-6} \leq f < 10^{-4}$ / year	R4	R4	R3	R3
1	Incredible	$f < 10^{-6}$ / year	R4	R4	R4	R4
			Insignificant	Marginal	Critical	Catastrophic
			1	2	3	4
			Severity Level			

Table 4 – Risk Ranking Matrix

3.2 PHA Output

The output of the PHA process described at the beginning of this Section and depicted in Figure 2 is a Sheet, encompassing the following information.

Field	Description
ID	Unique identifier of the hazard, in the form HX.Y.Z, where X, Y and Z are integers representing the top-, mid- and low-level hierarchical organisation of the hazards.
(Hazard) Name	Brief description of the hazard.
(Hazard) Group	Group(s) which the hazard belongs to.
Operating Mode	Operating mode(s) of the system under which the hazard may occur.
(Hazard) Cause	Cause(s) of the hazard.
Failure mode or Hazardous Event	Mode of failure (i.e. manner in which the hazard occurs) or event that initiates the hazardous condition (e.g. lightning, high temperature, etc.). It is also stated whether the hazardous effect results from single or multiple failure conditions.
Harm	Type of harm caused by the hazard, such as injury, death, etc.
Initial Severity	Initial Hazard Severity (see Table 2).
Initial Likelihood	Initial Hazard Likelihood (see Table 1).

Field	Description
Initial Risk	Initial Risk Level (see Table 3).
Mitigating Provisions	Mitigation that may be applied that reduce the Risk.
Final Severity	Fina Hazard Severity (see Table 2).
Final Likelihood	Final Hazard Likelihood (see Table 1).
Final Risk	Final Risk Level (see Table 3).
Note	Additional notes on the hazard, such as references to Safety Technical Reports, drawings, schematics, design guidelines, software references, or other information that may help in the understanding of the current state of the hazard under assessment (e.g. how the hazardous condition has been solved or the effects of the hazard occurrence mitigated).

Table 5 – Fields of the Hazard Sheet

4 D4S Preliminary Hazards Analysis

We focus our PHA of the D4S System to single drones and swarm of drones, each with weight less than 4kg, and we consider in this PHA only three Operational Modes, as reported in the following table:

Label	Description
OP.MDF	Man-driven single drone VLOS flights
OP.AF	Autonomous drones' swarm BVLOS flights
OP.R	Drone(s) recharge

Table 6 – D4S Operating Modes

The top hazards we identify are all conditions that potentially can cause injuries or death of humans, so that this column is not reported in the tables extracted from the hazard sheet.

[H1] Mid-air collision with aircrafts[1]
[H2] Failure condition resulting in unsafe, uncontrolled landing
[H3] Mid-air collision with vital infrastructure
[H4] Mid-air collision with ground moving vehicles[1]

In the following table, we list these top hazards as an inverted hierarchic tree, including specific hazards belonging to the top ones.

ID	Name	Group	Operational Mode	Cause	Initial Likelihood	Initial Severity	Initial Risk
H1	**Mid-air collision with aircrafts**		**OP.MDF** **OP.AF**	**TOP HAZARD: mid-air collision potentially could lead to catastrophic damage**	**-**	**-**	**-**
H1.1	Human Guidance Error	HG1	OP.MDF	Drone Pilot, due to lack of experience, planning, information moves one or more drones outside the Operational Volume	2	4	R3
H1.2	Procedural Error (Wrong NOTAM)	HG2	OP.MDF OP.AF	The Operational Volume is wrongly defined or it is well defined but the CAAs, ANSPs, airspace users and other involved entities are wrongly informed about it (allowing traffic inside)	1	4	R4
H1.3	Wrong planning	HG2	OP.MDF OP.AF	The autonomous flight rules contain planning error such that the drones / drones' swarm enter into wrong zones	1	4	R4
H1.4	Equipment malfunctioning (INS, GPS, Radio link…)	HG3	OP.MDF OP.AF	One subsystem failure causes a drone to move outside the Operational Volume	3	3	R2
H1.5	Adverse environmental conditions (wind, electromagnetic or solar interference)	HG4	OP.MDF OP.AF	Strong wind moves the drone outside the Operational Volume	4	3	R2

ID	Name	Group	Operational Mode	Cause	Initial Likelihood	Initial Severity	Initial Risk
H1.6	Autonomous Guidance Error	HG5	OP.AF	The flight plan, or the contingency measure (e.g. fail-safe return to home altitude) are wrongly planned moving the drone outside the Operational Volume	3	3	R2
H1.7	Security issue	HG6	OP.AF	Malicious actions (hijacking, tampering, spoofing)	2	4	R3
H2	**Failure condition resulting in unsafe, uncontrolled landing**		**OP.MDF** **OP.AF** **OP.R**	**TOP HAZARD: uncontrolled landing could potentially injure people or lead to catastrophic accident**	**-**	**-**	**-**
H2.1	Mid-air collision (birds, trees, infrastructures)	HG1, HG3, HG4, HG5, HG6	OP.MDF OP.AF	During flight operation any collision could cause an uncontrolled landing	4	2	R2
H2.2	Equipment malfunctioning (including erroneously programmed fail safe return and collision sensors malfunctioning)	HG3	OP.MDF OP.AF OP.R	Several subsystems failure causes uncontrolled landing during flight, e.g. propellers, motors, batteries etc. During recharge an uncontrolled landing could dangerously interfere with railway operation or cause directly injuries to personnel	4	3	R2
H3	**Mid-air collision with vital infrastructure**		**OP.MDF** **OP.AF** **OP.R**	**TOP HAZARD: critical static railway infrastructures (e.g. electronic equipment and signals) could be dangerously damaged by a collision with a drone**	**-**	**-**	**-**
H3.1	Human Guidance Error	HG1	OP.MDF	-	4	3	R2
H3.2	Adverse environmental conditions (wind, electromagnetic or solar interference)	HG4	OP.MDF OP.AF OP.R	-	4	3	R2
H3.3	Autonomous Guidance Error	HG5, HG6	OP.AF		3	3	R2
H4	**Mid-air collision with ground moving vehicles**		**OP.AF** **OP.R**	**TOP HAZARD**	**-**	**-**	**-**

ID	Name	Group	Operational Mode	Cause	Initial Likelihood	Initial Severity	Initial Risk
H4.1	Wrong planning	HG2	OP.AF OP.R	Procedure prevent flight operation near moving train	3	3	R2
H4.2	Equipment malfunctioning	HG3, HG6	OP.R	During recharge there are moving trains	3	3	R2

Table 7 – Hazards

Hazard groups are defined in the following table.

Hazard group	Title	Hazards	Note/Description
HG1	Human Guidance Error	**H1.1, H2.1, H3.1**	
HG2	Procedural Error	**H1.2, H1.3, H4.1**	
HG3	Equipment malfunctioning	**H1.4, H2.1, H2.2, H4.2**	
HG4	Environmental conditions	**H1.5, H2.1, H3.2**	
HG5	Autonomous Guidance Error	**H1.6, H2.1, H3.3**	
HG6	Security issue	**H1.7, H2.1, H3.3, H4.2**	

Table 8 – Hazard Groups

For each Hazard Group and for each hazard in the Hazard Group, in the following table we identify the key factors to be controlled in each mission to mitigate the hazard. After these mitigations, all the Risks are reduced to a Tolerable or Negligible level in the Hazard Sheet, so that they are not reported in the following table.

Hazard Group	Hazard Group Description	Mitigation
HG1	Human Guidance Error	Assure Drone Pilot experience level
		Assure training on specific mission equipment and rules
		Assure Drone Pilot physical and mental conditions
		Verify that he geofencing system is active and correctly programmed
		Verify that the collision avoidance sensors are correctly working
HG2	Procedural Error	Procedure have been validated by an independent entity
		The persons involved in the procedure and planning have specific experience
		The procedure has been used in other missions
HG3	Equipment malfunctioning	The systems have been qualified
		The systems are proven in use
		The system is under a continuous maintenance program
HG4	Environmental conditions	The meteo conditions are favourable
		The meteo forecast are favourable
		The K_P index is low or very low
HG5	Autonomous Guidance Error	The autonomous guidance system has been tested and qualified
		The autonomous mission rules have been checked

Hazard Group	Hazard Group Description	Mitigation
HG6	Security issues	The security and sanity of the involved computers has been checked
		The involved computing systems are manged using adequate security practice
		The computing system are insulated from the network during the operations

Table 9 – Mitigation of the Hazards

5 Future work

The hazards identified in the PHA should be verified and maintained during the project lifecycle in order to:

1) Identify and manage additional hazards which may arise as soon as the knowledge of the D4S System increase during the detailed design and development.
2) Check how the hazards are "apportioned" among the different subsystems / components /modules into which the D4S System is decomposed (see [AD-1]);
3) Identify and manage additional hazards which may arise as soon as the knowledge of the D4S operational scenarios are known with greater details.

It is worth mentioning that, during the project validation, Drones' and Drones' Swarm operations will be analysed using the SORA Methodology (see [RD-9], [RD-10] and [RD-11]) and MEDUSA (see [RD-12] and [RD-13]). The outcomes of this analysis will be published in D2.2 (see [AD-2]).