ReMAP

Real-time Condition-based Maintenance for Adaptive Aircraft Maintenance Planning

Deliverable 7.1

Hazards and Safety Barriers related with CBM technologies

This project has received funding from the European Union's Horizon 2020 research and innovation programme under grant agreement No 769288

Document History

Revision Nr	Description	Authors	Reviewers	Date
0.0	Initial Draft	P. Bieber, ONERA, J. Lee, TUD and M. Mitici, TUD with contributions from KLM and Embraer		28/01/2020
0.01	Draft – Hazard Identification		B. Santos, TUD, F. Freeman, KLM	20/05/2020
0.02	1st complete Draft		M. Mitici, TUD, J. Lee, TUD	31/05/2020
0.03	Revised Draft – with corrections from reviewers, Safety Risk Matrix added in section 5.2		B. Santos, J. Lee, TUD, F. Freeman, KLM	10/06/2020
0.04	Final Revised Draft			30/06/2020
1.0	Final Public Version			08/07/2020

Index

1. Introduction

1.1. Project Summary

ReMAP “Real-time Condition-based Maintenance for adaptive Aircraft Maintenance Planning” (hereinafter also referred as “ReMAP” or “the project”), is a European project started on the 1st of June 2018 and has a duration of four years. The project addresses the specific challenge to take a step forward into the adoption of Condition-Based Maintenance in the aviation sector. In order to achieve this, a data-driven approach will be implemented, based on hybrid machine learning & physics-based algorithms for systems, and data-driven probabilistic algorithms for systems and structures. A similar approach will be followed to develop a maintenance management optimisation solution, capable of adapting to real-time health conditions of the aircraft fleet. These algorithms will run on an open-source IT platform, for adaptive fleet maintenance management. The proposed Condition-Based Maintenance solution will be evaluated according to a safety risk assessment, ensuring its reliable implementation and promoting an informed discussion on regulatory challenges and concrete actions towards the certification of Condition-Based Maintenance.

1.2. Purpose of this Document

This document is the Deliverable D7.1 of the ReMAP Project. It addresses the identification of safety hazards related with Condition-Based Maintenance technologies investigated by partners of the project. The document also lists mitigation means (also called safety barriers) that could be used to limit the effect of the identified hazards.

The deliverable is part of Work Package 7 (Integrated Safety Risk Assessment) from the project. The work is related with the Task 7.1 (Identification of hazards and safety barriers related with CBM technologies).

1.3. Context

The usual practice when dealing with certification considerations for a new technology such as CBM technologies is to start by assessing hazards that could occur due to the introduction of this technology. Hazards should first be identified and their effects on the safety of people, goods and environment should be assessed. Mitigation means that could limit the hazard effect severity or decrease its occurrence likelihood should also be investigated.

Hazards described in this deliverable were identified by collecting the expertise of KLM aircraft maintenance specialists and by reviewing the associated literature including investigation reports and health-monitoring normative documents. A framework for assessing aircraft CBM hazard severity is proposed and potential mitigation means are listed.

The goal of Task 7.1 is to perform the hazard assessment for the CBM technologies. Other tasks of WP7 deal with the quantitative assessment of CBM technologies (Task 7.2) and with regulatory aspects of the introduction of CBM technologies (Task 7.3).

2. Identification of Hazards with Domain Specialists

2.1. Agent Based Model of the Maintenance Process

A first objective of WP7 is that participants share a common view of the maintenance process and safety/certification issues. In this section we describe models that are intended to help WP7 participants to better understand the maintenance process and to guide hazard identification activities. The models use diagrams in order to describe the main agents involved in the maintenance process and their interactions. A diagram provides a global view of the maintenance process that is easy to understand. It is also very easy to compare diagrams in order to understand the differences between various versions of the maintenance process. Two models of the maintenance process were defined, the first model describes the current process (this model is named “before ReMAP Process”) (Figure **Erreur ! Source du renvoi introuvable.**) and the second model describes a future maintenance process incorporating the novel CBM technologies investigated by the ReMAP partners (this model is named “after ReMAP Process”) (Figure **Erreur ! Source du renvoi introuvable.**). These models were developed by TUD with the help of KLM. The models are based on KLM’s practice. Other companies can follow slightly different work flows. The models were reviewed by the participants of WP7.

The following list of agents and agent teams of the maintenance process was built:

- Regulatory Body
- Manufacturer
- Maintenance Organization
    - Task Generating Team
        - Maintenance Program Engineer
        - Engineering Team
        - Reliability Engineer
        - MCC Technical Specialist
    - Task Planning Team
        - Ground-Time Planner
        - Planning Adjuster
        - Hangar Planner
    - Mechanics
    - Data Management Team
        - Data Manager
        - Prognostics/Diagnostics Team
- Airline
    - Airline Scheduler
    - Flight Crew
    - Aircraft

- Aircraft Component
- Condition Monitoring System

Agents in the Data Management Team only appear in the second model dealing with the future Maintenance Process.

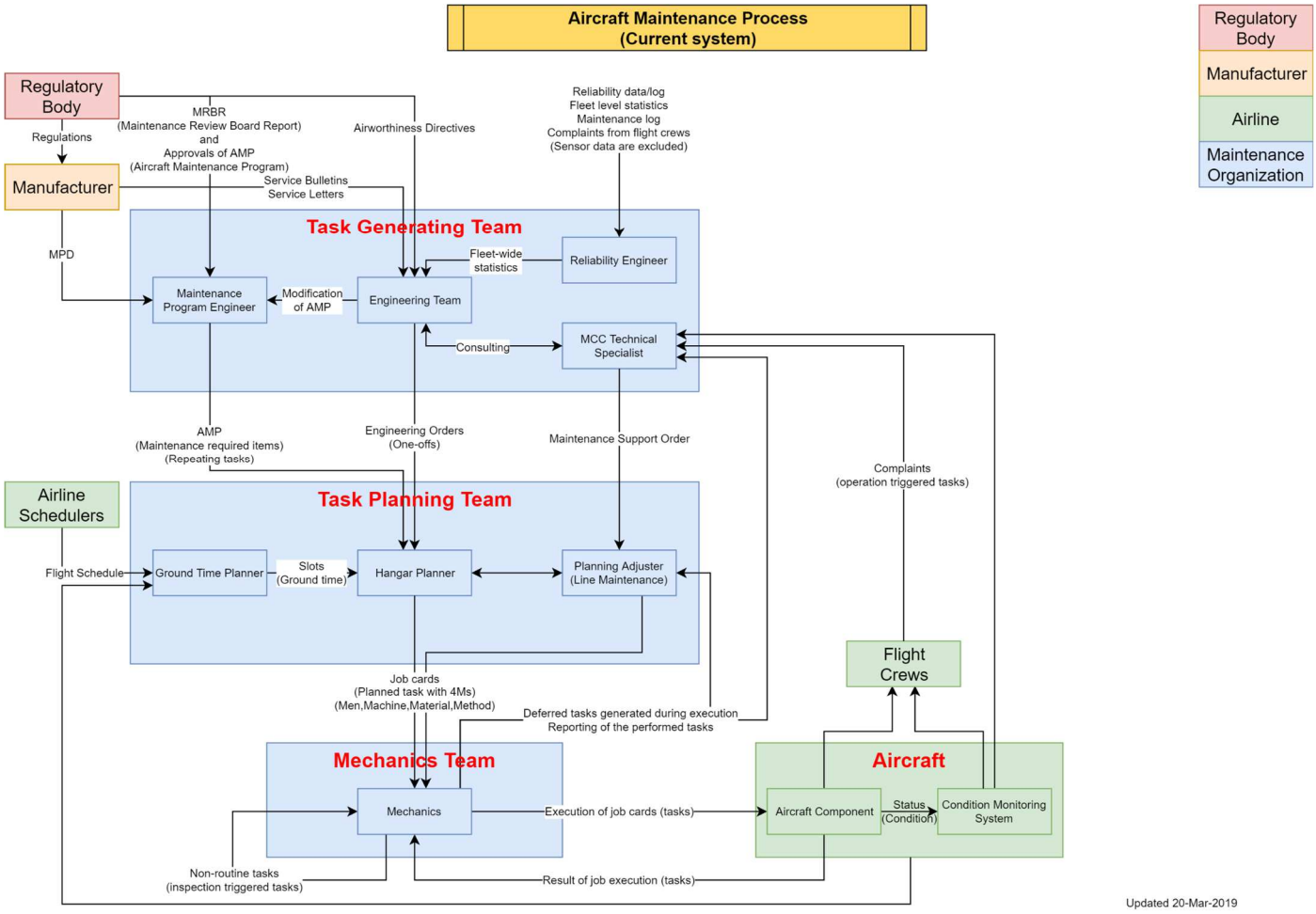

Figure 1 : Agent Based Model of Maintenance Process (before ReMAP)

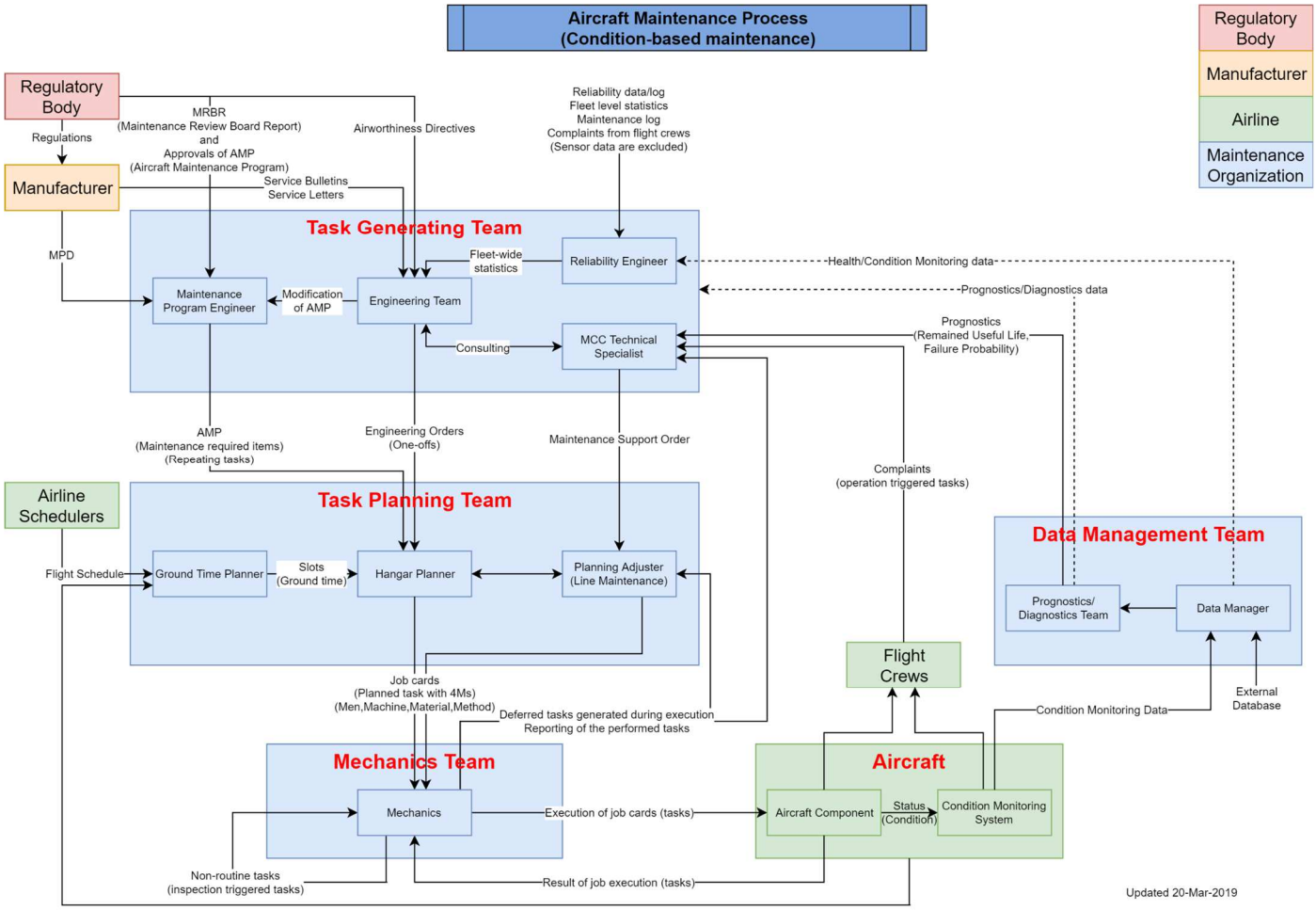

Figure 2 : Agent Based Model of Maintenance Process (after ReMAP)

In the following, we give a short description of the role of each agent and its main inputs and outputs.

- **Regulatory Body**
  - Role: Regulatory bodies such as EASA or a National Aviation Authority give directives on the aircraft maintenance process to ensure the safety of aviation.
  - Output for Maintenance Program Engineer
    - Maintenance Review Board Report (MRBR): MRBR is made by Maintenance Review Board (MRB) which consists of the regulatory body, manufacturers, and operators. This is based on Maintenance Steering Group-3 (MSG-3) philosophy. MRBR states the maintenance procedure of system, power plant (engines), structure, zonal and lightning
    - Approval of Aircraft Maintenance Program (AMP): Regulatory bodies also approves the modification of AMP, which is made by Maintenance Program Engineer.
  - Output for Engineering Team

        - Airworthiness Directives (AD): ADs are mandatory changes in either the maintenance program or in the aircraft configuration.
- **Manufacturer**
    - Role: Manufacturers includes Original Equipment Manufacturer (OEM) and Original Aircraft Manufacturer (OAM).They provide recommended maintenance program for their product. The recommendation is based on their experiments and analysis during the manufacturing. Because manufacturers do not have exact data on aircraft operation, the recommendations are usually conservative.
    - Output for Maintenance Program Engineer
        - Maintenance Planning Document (MPD): MPD includes maintenance tasks recommended by the manufacturers. It becomes the foundation of AMP. To be conservative, the recommended periods of tasks in MPD are usually shorter.
    - Output for Engineering Team
        - Service Bulletin (SB) and Service Letter (SL): SBs are recommended modification of aircraft, and SLs are additional advice on the tasks. These are not mandatory tasks.
- **Maintenance Program Engineer**, member of Task Generating Team
    - Role: Maintenance Program Engineers generate the repeating tasks with fixed time interval.
    - Input from the regulatory body
        - MRBR, Approval of the modification of AMP
    - Input from Manufacturer
        - MPD
    - Input from Engineering Team
        - Suggestions for the modification of AMP
    - Output for Hangar Planner
        - Aircraft Maintenance Program (AMP): AMP is a list of repeating scheduled tasks provided with the intervals (deadlines) and the proper methods. Since it has a fixed time interval (hard-time), it is called time-based maintenance (TBM).
        - Task Packaging: TBM tasks with a similar anticipated due date are packaged into blocks or letter checks (A, C, and D checks). This packaging approach makes the planning problem easier by using a fixed interval of letter checks, instead of various intervals of different tasks. As a trade-off, it has inefficiency because some tasks in a letter check are executed far before its due-date.
- **Engineering Team**, member of Task Generating Team
    - Role: Engineering Team conducts engineering analysis, maintenance data analysis, and other necessary activities to improve the aircraft maintenance process. There are various engineers who are responsible for different parts of aircraft. For instance, System Engineers, Avionics Engineers, Structure Engineers, and Engine Engineers are responsible for their own domain, but their roles are the same.
    - Input from Regulatory Body
        - Airworthiness Directive.
    - Input from the manufacturers
        - Service Bulletin and Service Letter.
    - Input from Reliability Engineer
        - Fleet-wide reliability data.
    - Output for Maintenance Program Engineer

        - Suggestions for the modification of AMP.
    - Output for Hangar Planner
        - Engineering Order (EO): EOs are the one-time maintenance tasks not included in AMP.
- **Reliability Engineer**, member of Task Generating Team
    - Role: Reliability Engineer collects fleet-wide statistics regarding the reliability of aircraft subsystems, and report this to Engineering Team.
    - Input from database of maintenance organization. In the current system, Reliability Engineers do not collect data from sensors.
        - Delay data & unscheduled ground-time that are due to technical issues, complaints from operational crews, technical incidents, maintenance data including the removals and the no-fault-founds
    - Output for Engineering Team
        - Fleet-wide statistics
- **MCC Technical Specialist**, member of Task Generating Team
    - Role: Technical Specialist (or Maintenance Specialist) in the MCC generates reactive tasks to address the complaints and report from various sources. They consult the inputs with Engineering Team and generates the reactive tasks.
    - Input from Flight Crew
        - Complaints from Flight Crew: The complaints include abnormality perceived during and after the flight.
    - Input from Condition Monitoring System
        - Condition monitoring data: When condition monitoring data indicates certain signals, Technical Specialist generates tasks to handle it. (It needs to be checked that who is responsible for downloading and managing the condition monitoring data.)
    - Input from Mechanics
        - Deferred tasks: When the mechanics face the technical issues hard to solve onsite, they report this to Technical Specialist.
    - Input from Engineering Team
        - Consulting with Engineering Team
    - Output for Planning Adjuster
        - Maintenance Support Order (MSO): MSOs are the tasks to resolve the maintenance request comes from the Flight Crew, Mechanics, and the monitoring system.
    - Output for Engineering Team
        - Consulting with Engineering Team
- **Ground-Time Planner**, member of Task Planning Team
    - Role: Ground-Time Planner makes a fleet-level plan for maintenance.
    - Input from Airline Scheduler
        - Flight schedule
    - Output for Hangar Planner
        - Slots: The duration that aircraft can stay in a hangar for maintenance is called slots or ground time. For the given flight schedule, ground times are generated by (a) excessive capacity of aircraft, and (b) buffer in turnaround time.
- **Planning Adjuster**, member of Task Planning Team

- Role: Planning Adjuster receives Maintenance Support Order (MSO) from Technical Specialist. Then, the tasks are forwarded to the Hangar Planner based on its urgency, criticality, and applicability. If the order is executable in line, it is transferred to line mechanics. Otherwise, the order is transferred to Hangar Planner to plan it for the base maintenance.
- Input from Technical Specialist
  - Tasks in MSOs
- Output for Hangar Planner
  - Tasks that is not executable in line maintenance.
- Output for line mechanics
  - Job cards: a job card is a detailed description of work that is performed for a maintenance support order. The tasks executable in line maintenance are made as job cards by the Planning Adjusters.

- **Hangar Planner**, member of Task Planning Team
  - Role: Hangar Planner makes the given tasks to be executable considering the availability of aircraft, hangar, and 4M (Man, Machine, Material, and Method).
  - Input from Maintenance Program Engineer
    - Tasks in AMP: Aircraft usage is estimated based on FH (flight hours), FD (flight days), and FC (flight cycles).
    - Task Packaging : the letter checks are planned not to pass the deadlines given in AMP.
  - Input from Engineering Team
    - Tasks in EOs
  - Input from Planning Adjuster
    - Tasks in MSOs
  - Input from Ground-Time Planner
    - Slots of the aircraft fleet, availability of hangar, men, machine, material, and methods. In practice, not only availability of hangar space, but also the work shift, holidays, availability of parts need to be considered.
  - Output for Mechanics
    - Job cards: It describes the detailed directions to execute the tasks.
- **Mechanics**
  - Role: Mechanics execute the tasks described in job cards. Also, they can generate tasks by themselves when they find the necessary tasks during their inspection.
  - Input from Hangar Planner or Planning Adjuster
    - Job cards
  - Input from Aircraft
    - Result of job execution. When the mechanics execute the tasks, they observe the status of aircraft system. Mechanics can generate the non-routine tasks based on this.
  - Input from Mechanics
    - Non-routine tasks. When the mechanics find something during the inspections, they can generate tasks by themselves. If the task is urgent and executable, it become self-input. This can be a potential cause of unexpected ground time.
  - Output for Aircraft

        - Execution of job cards (tasks): This is not information delivery as like many other outputs in this document, rather this is physical interaction with aircraft. It can change the state of aircraft systems by removal, replacement, or overhaul. Some job cards such as inspection can give feedback to the mechanics.
    - Output for Planning Adjuster
        - Deferred tasks (complaints): When the non-routine tasks cannot be executed during the planned ground time, it is reported to Planning Adjuster. Especially when the mechanics find technical difficulties that cannot be solved on-site, it is reported to MCC Technical Specialists to conduct engineering review. (The logic to determine which non-routine tasks to be executed or deferred needs to be identified further.)
- **Airline Scheduler**, member of Airline
    - Role: An airline aims to achieve the flight schedule with the minimal delay and minimal cost. In practice, the flight schedule is determined as a collaborative result of market prediction, work shift of crews, availability of aircraft, and maintenance schedule. However, in this study, the flight schedule is assumed to be defined before the maintenance process. This assumption can be relaxed in future study.
    - Output for Ground-Time Planner
        - Flight Schedule.
- **Flight Crew**, member of Airline
    - Role: Flight Crew includes pilots and cabin crews who actually operate aircraft. During the flight, they perceive various information about the status of aircraft systems. When they notice the abnormality, they report it as complaints, which are operation-triggered tasks.
    - Input from Aircraft components
        - Perception of the status of Aircraft Systems: Flight crews perceive the status of aircraft systems via various manner such a looking the instrument panel and warning signs, experiencing the abnormal reaction of aircraft during operation, and inspecting the aircraft before and after the flights. They also reports when they executed certain operations such as hard-landing, following their manual.
    - Input from Condition Monitoring System
        - State of aircraft system perceived by the Condition Monitoring System
    - Output for Technical Specialists
        - Complaints about the aircraft system is reported to Technical Specialists.
- **Aircraft Component**, member of Aircraft
    - Role: Aircraft system in an aircraft is a sub-agents of the aircraft. Any system, structure, and part that is under the scope of maintenance process simulation can be regarded as this agent.
    - Input from Mechanics
        - Execution of job cards: Depends on the type of the tasks, the state of the Aircraft System can be changed. For instance, replacement of aircraft system will change the system condition to be As-good-as-new from Working or Fail.
    - Output for Condition Monitoring System
        - Condition of aircraft system is given by sensors and data acquisition system.
    - Output for Flight Crew
        - Condition of aircraft system is given by various means.
    - Output for Mechanics

        - Condition of aircraft system is given as the result of inspections.
- **Condition Monitoring Systems**, member of Aircraft
    - Role: On-board Condition Monitoring System collects data from aircraft. As an input, it receives states of aircraft. For instance, it can monitor the size of brake pad or the fatigue of the structure, depends on the purpose of the system. In the current process, it delivers the data to Technical Specialists to generate maintenance tasks.
    - Input from Aircraft Component
        - State of Aircraft System.
    - Output for Flight Crew
        - Notification of the condition of aircraft systems
    - Output for Technical Specialist
        - Condition monitoring data
- **Data Manager**, member of Data Management Team
    - Role: Data manager is a person responsible for handling the condition data and external database. Input from Condition Monitoring System
        - Condition monitoring data.
    - Input from external agents
        - External database such as weather data, airport data, and so on.
    - Output for Prognostics/Diagnostics Team
        - Consolidated data
- **Prognostics/Diagnostics Team**, member of Data Management Team
    - Role: Prognostics/Diagnostics team process the given data to estimate such as remained useful life, failure probability, and so on.
    - Input from Data Manager
        - Consolidated data
    - Output for the Task Generating Team
        - Diagnostics data, Prognostics data such as RUL and failure probability.

The main difference between the two models is the presence of the Data Management Team in the “after ReMAP” model. As the data management team is not yet fully implemented in practice, the role of this agent group and its interactions with other agents will need to be discussed and detailed in the future. In the version of the model presented in this document, some interactions between Data Management Team and Task Generation Team are represented using dotted lines in order to show that the precise agent that will be in charge of using Diagnostics and Prognostics data has still to be decided among the various members of the Task Generation Team.

The Agent based model proposed in this section is consistent with the functional view of Aircraft Health Monitoring (AHM) found for instance in the Maintenance Programs Industry Group (MPIG) IP180 document [ReMAP_023[1]]. According to this document AHM allows the operator to do the following functions:

- **Collect** aircraft system information on aircraft,
- **Relay** system information to airline personnel on the ground,

[1] Bibliographical references identified with a identifier of the form ReMAP_XXX can be found in chapter 7

- **Analyse** the data to determine impending system degradation or failure and produce actionable alerts to be addressed by the operator,
- Resolve and track of the alerts produced and **Generate** Maintenance actions

To these AHM functions we add two functions in order to perform the generated maintenance actions:

- **Plan** the maintenance actions
- **Execute** the planned maintenance actions

The following figure links the agent based model with AHM functions and relevant ReMAP work-packages. The top line of the figure shows the main agents of the agent based model. The medium line shows the functions we have just introduced and the main flow of information between the functions. The bottom line shows ReMAP work-packages that investigate CBM technologies. Work-packages WP7 about safety assessment and WP8 about demonstration are not shown because they address the end-to-end maintenance process instead of a specific agent.

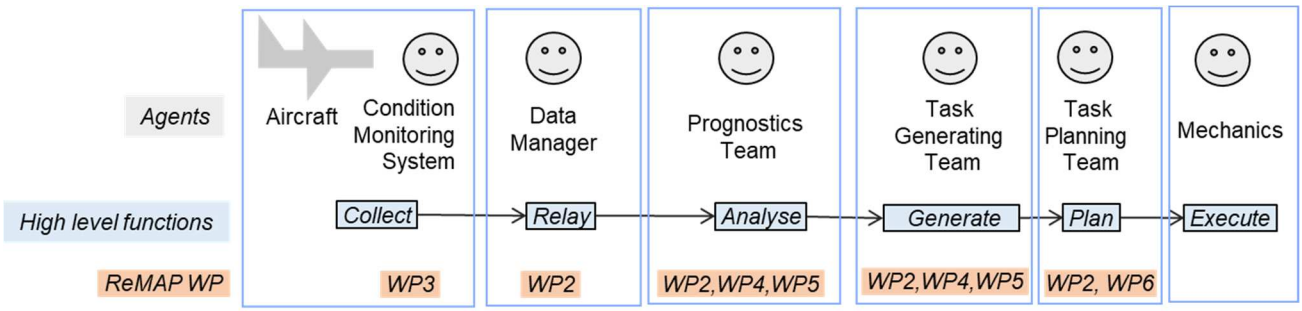

Figure 3 - Mapping of Agents, Functions and ReMAP Work-Packages

The blue rectangles show the mapping of agents, functions and WPs. Agents in a blue rectangle contribute to the realization of the function in that rectangle. The function is supported by the technologies investigated by the WPs that appear in the rectangle. For instance, the Prognostics Team contribute to the function that analyses data in order to determine system degradation and to produce alerts. This function is supported by the IT platform investigated in WP2 as well as Structure Health-Monitoring investigated in WP4 and System Health-Monitoring investigated in WP5. As the IT platform supports several functions, WP2 appears in several blue rectangles.

2.2. Brainstorming Session with KLM experts

On February 28th 2019 TUD and KLM organized a Brainstorming Meeting with KLM specialists about Hazard Identification. 10 KLM specialists participated to the session. Participants from various departments within two airlines (KLM, KLM Cityhopper) and one maintenance, repair and overhaul company (KLM E&M) have joined the workshop. The main agents of the maintenance process were represented during this session: Data Management Team, Task Generating Team (Reliability Engineering, System Engineering, Maintenance Program Engineering), Task Planning Team (Hangar Planning), Flight crew, Safety Manager.

The brainstorming session was split into two parts. During the first part, the agent based model of (current) time-based maintenance was presented and potential hazards related with this process were discussed. During the second part, the (future) condition-based maintenance model was presented and potential hazards related with this process were discussed. The raw result of the session is a list of 150 hazards, insights and obstacles related with the main activities of the maintenance process.

A first exploitation of the outcome of KLM Brainstorming Meeting was performed by TUD. Eighteen hazards related with agents operating a condition-based maintenance process were extracted from the raw results. They are operational hazards that will occur after the adoption of the CBM technologies. These hazards will need a continuous management during the entire period of aircraft maintenance. A complete table of thirty-nine operational hazards applicable to both current and future maintenance process can be found in the confidential appendix of this deliverable.

In the following table, the column labelled “Agent” indicates the agent that is the main contributor to a hazard. Agents were described in the previous section of this chapter. The column labelled “Failure Mode” indicates the failure mode associated with the operation performed by the agent contributing to the hazard. The proposed operational failure modes are:

- Missed: the operation is not done at all by the agent or the operation was tried by the agent but did not succeed;
- Late : the operation was done by the agent after deadline;
- Unclear: the operation performed by the agent resulted in an unclear communication
- Inadequate : the operation was inadequately done by the agent;

Table 1 – CBM Operational Hazards identified during the Brainstorming session

ID	Maintenance Agent Operational Hazard	Agent	Failure Mode
Op-03	*Aircraft Condition Monitoring System delays transmission of data to Data Team.* *Data Team delayed prognostics because of delay in data transmission from CM.*	Condition Monitoring System	Late
Op-04	*Aircraft Condition Monitoring System alerts when there is no fault because the monitoring parameter is above threshold. (NFF)*	Condition Monitoring System	Inadequate
Op-05	*Condition Monitoring System generates/transfers wrong/incorrect/inadequate data.*	Condition Monitoring System	Inadequate
Op-06	*Data Team generates unclear/ambiguous prognostics/diagnostics*	Data Management Team	Unclear
Op-07	*Data Team uses unreliable algorithm for prognostics/diagnostics*	Data Management Team	Inadequate

ID	Maintenance Agent Operational Hazard	Agent	Failure Mode
Op-08	*Data Team generates prognostics/diagnostics too late.*	Data Management Team	Late
Op-09	*Data Team triggers inadequate/ineffective task.*	Data Management Team	Inadequate
Op-10	*Data Team generate wrong prognostics/diagnostics*	Data Management Team	Inadequate
Op-11	*Data Team does not alert when there is a fault because the threshold is not met.*	Data Management Team	Missed
Op-12	*Data Team is not functioning, or inoperative.*	Data Management Team	Missed
Op-18-a	*Mechanics performs conventional inspection less carefully due to overconfidence in CBM*	Mechanics	Inadequate
Op-18-b	*In case of unscheduled maintenance, CBM would cause more maintenance actions to be performed leading to a higher risk of maintenance human errors by the mechanics*	Mechanics	Inadequate
Op-25	*Task Generating Team generates an ineffective task (CBM).*	Task Generating Team	Inadequate
Op-26	*Task Generating Team does not examine/verify the prognostics/diagnostics*	Task Generating Team	Missed
Op-28	*Task Generating Team generates inadequate/ineffective task for a given trigger*	Task Generating Team	Inadequate
Op-29	*Task Generating Team does not notice the alert from Data Team*	Task Generating Team	Missed
Op-30-a	*Task Generating Team does not rely on prognostics/diagnostics from Data Team (Task Generating Team does not generate a task (CBM))*	Task Generating Team	Missed
Op-30-b	*Task Generation team does not generate a task due to misunderstanding/distrust in CBM*	Task Generating Team	Missed

ID	Maintenance Agent Operational Hazard	Agent	Failure Mode
Op-31	*Task Generating Team generates a task too late.*	Task Generating Team	Late
Op-32	*Task Generating Team misunderstand alerts from Data Team.*	Task Generating Team	Unclear

The following table shows the number of hazards associated with each agent for the thirty-nine operational hazards. Agents existing in the two versions of the maintenance process, such as Task generating team and Mechanics, have a majority (22) of hazards related with their operations. This seems normal because these agents play a major role in the maintenance process and they perform several functions. For instance, Mechanics should:

- execute tasks (5 Hazards: Op-15, Op-16, Op-18-a, Op-18-b, Op-22),
- perform decisions (Hazard: Op-17),
- collect data (Hazard: Op-19),
- communicate (2 Hazards:Op-20, Op-21).

Similarly, Task Generating Team should:

- manage received alerts, diagnostics and prognostics (4 hazards: Op-26, Op-27, Op-29, Op-32)
- generate tasks (8 hazards: Op-25, Op-34, Op-28, Op-30-a, Op-30-b, Op-31, Op-33, Op-35).

Although the Data Management Team is not fully implemented in industry, a significant number of hazards (7) were related with the operations performed by this new team.

Table 2 – Count of Operational Hazards per Agent

Agent	Hazard Count
Task Generating Team	12
Mechanics	10
Data Management Team	7
Task Planning Team	4
Condition Monitoring System	3
Aircraft	2
Regulatory Body	2
Flight Crew	1
Total	**41**

Table 3 - Count of Operational Hazards per Failure Mode

Failure Mode	Hazard Count
Inadequate	20
Missed	9
Late	6
Unclear	6

The previous table shows the number of operational hazards related with a given failure mode. The most common failure mode is "*Inadequately performed operation*" that is related with 20 hazards. All agents have at least one hazard related with this failure mode. Again, Task generating team and Mechanics share the most important part of these Hazards. It might be interesting to refine the "Inadequate" failure mode in order to provide a more precise view of the hazards.

Furthermore, 21 obstacles related with the development and approval of CBM technologies were extracted from the raw results. These obstacles will need to be discussed with Certification Authorities before the adoption of CBM technologies. These obstacles cannot be directly linked with a specific agent in the maintenance process. They are often related with: the overall process and they deal with matters such as the allocation of roles and responsibilities in the new maintenance process, the integration of CBM technologies into Maintenance, Repair & Overhaul and Airline business processes, the needed skills and knowledge transfer in order to implement the CBM process. We will come back to these obstacles during task T7.3 when we will work on a roadmap for the adoption of CBM technologies.

3. Identification of Hazards in the Literature

Hazards identified during the brainstorming session with KLM experts can easily be related with the daily operations of aircraft maintenance agents. The hazards are not directly linked with the new CBM technologies investigated within ReMAP. This can be explained by the fact that KLM experts identified hazards using their knowledge of the maintenance process supported by existing technologies. It was more difficult for them to imagine new hazards related with forthcoming technologies.

In order to complement the outcome of the brainstorming session with CBM technical hazards, a literature survey was performed by ONERA. Around 50 documents were collected (see Appendix A for a list of references of these papers).

Our initial intent was to review these documents in order to directly find potential technical hazards applicable to CBM. Actually, we found limited direct information related with hazards in the collected documents. Nevertheless, we have selected three groups of documents that contained the most valuable information for the identification of hazards:

- Health-Monitoring Accident and Serious Incident Investigation Reports: these reports provide the description of real-life hazard occurrence related with Helicopter and Aircraft Health-Monitoring systems;
- Health-Monitoring Normative Document : these documents written by certification authorities such as EASA or FAA define the framework for the certification, qualification or approval processes of Health-Monitoring systems, they indirectly describe hazards that should be taken into account by these processes;
- EASA AI/ML Roadmap: this recently released document gives a list of challenges related with Artificial Intelligence and Machine Learning technologies that ReMAP partners are investigating in the context of CBM, these challenges can be viewed as hazards.

3.1. Health-Monitoring Accident and Serious Incident Investigation Reports

We searched for accidents and serious incidents reports that mentioned Health-Monitoring. We found various reports on accidents mentioning Helicopter Vibration Health-Monitoring (VHM) or Heath and Usage Monitoring Systems (HUMS) : UK AAIB reports on accident to Airbus Helicopters AS 332 L2 Super Puma in 2009 [ReMAP_046] and on a Sikorsky S-92A accident in 2016 [ReMAP_036], Norway Accident Investigation report on an Airbus Helicopter 225 accident in 2016 [ReMAP_042]. We also found one report on a serious incident mentioning Aircraft Health-Monitoring (AHM) System (see AAIB Annual Report 2018 and Report on Serious Incident Boeing 787-9 Dreamliner, G-ZBKF [ReMAP_039]).

In the following, we summarize the helicopter accident reports and then focus on the B-787 serious incident reports because this report identifies Health-Monitoring as an important contributor to the incident whereas the role of health-monitoring in the helicopter accidents is less important.

A helicopter accident in 1997 [ReMAP_048] gave arguments for making VHM systems mandatory for helicopter transport offshore. Then, the AAIB report [ReMAP_046] concerning an accident of a helicopter equipped with VHM/HUMS identified that the detection by the VHM of component degradation needed improvement. As a result of this recommendation, EASA launched a research project Vibration Health Monitoring and Alternative Technologies [ReMAP_041]. Other accidents of helicopter equipped with VHM/HUMS occurred including the Airbus Helicopter 225 accident in 2016. Again the investigation reports concluded that there was a need to improve the performance of VHM detection. Several Hazards identified during the Brainstorming session are addressing the diagnostic/detection performance problem:

- Op-10 *Data Team generate wrong prognostics/diagnostics*
- Op-11 *Data Team does not alert when there is a fault because the threshold is not met*.

The investigation report of Sikorsky S-92A accident in 2016 [ReMAP_036] made a different conclusion about VHM/HUMS. In this report, the performance of VHM/HUMS detection is not questioned but the investigation identified that the flight crew would have had opportunities to safely abort the flight if the VHM/HUMS data had been available on the helicopter in near real time. Recommendations were issued in order to improve near real-time capabilities of VHM data capture, analysis and detection and to improve the display of the result of VHM detection to the flight crew on the helicopter; the result should be displayed at least before take-off and after landing. Two hazards identified during the Brainstorming session are addressing the late provision of diagnostic:

- Op-08 *Data Team generates prognostics/diagnostics too late*.
- Op-03 *Aircraft Condition Monitoring System delays transmission of data to Data Team. Data Team delayed prognostics because of delay in data transmission from CM.*

AAIB investigation report [ReMAP_039] on the serious incident Boeing of 787-9 Dreamliner, G-ZBKF (Emergency descent due to loss of cabin pressure, en route from London Heathrow to Delhi, 29 April 2017) provides an interesting scenario illustrating CBM hazards. We first outline the chronology of events leading to this incident, then we discuss the CBM hazards contributing to the incident.

The aircraft was dispatched in accordance with the Minimum Equipment List (MEL) with the left air conditioning (AC) system inactive. Cabin pressurisation was totally lost during the flight because of the combination of the failure of a component of the right AC system and the inactivation of left AC system before flight.

The investigation established that the component of the right AC system was changed 11 days before the incident flight. The following day, when the aircraft returned to service, the AHM system sent an Alert Message to the MCC, indicating that a ‘high leakage/low inflow’ of the cabin pressurisation system had been detected. The AHM message was assessed by the MCC and 9 days before the incident flight a work request was raised to carry out a pressurisation leak check. The end date for completion of work request was set at 15 days later (so 6 days after incident occurrence). Thereafter, during all of the 15 subsequent flights, Maintenance Alert Message was sent by AHM with no other actions by MCC.

The operator considered that the poor reliability of this AHM alert message was the cause of the lack of reaction from MCC. Quoting from the investigation report [ReMAP_039]:

“*The operator later stated that the AHM system provides just over 1,200 maintenance alerts. From experience, some maintenance alert messages are inadvertently triggered, which has led to refinements to improve the robustness of the system and reduce the*

level of 'nuisance' alerts. The operator had seen alert message triggered 'intermittently' on other aircraft before and this had caused maintenance staff to question the reliability of this particular alert message."

The engineer who had inactivated the left AC system on the morning of the incident had been provided with a complete maintenance documentation that included the pressurisation leak check work request for the right AC system. The operator stated that it was not a requirement that engineers review this particular information as it was included for information purposes only.

Following this serious incident safety actions have been taken by the manufacturer and the operator: the aircraft manufacturer modified the AHM 'maintenance alert' logic in order to reduce false-alarms, the operator has revised its process for dealing with this AHM 'maintenance alert' message.

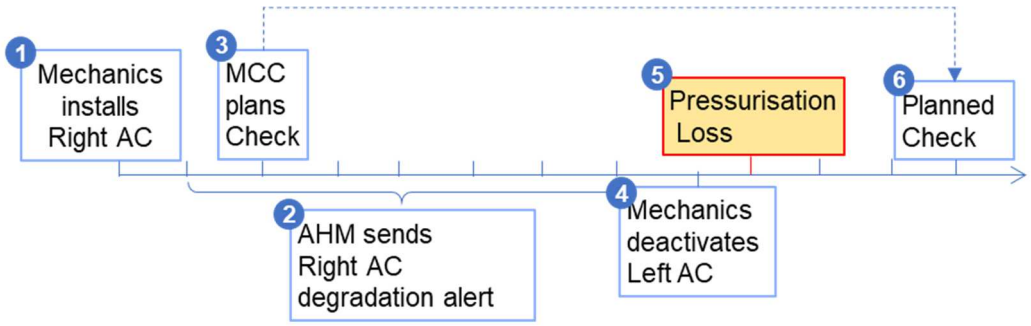

Figure 4 – Chronology of the Serious Incident on B-787 in 2017

The main events of this serious incident can be linked with hazards identified during the Brainstorming with KLM experts:

1. Mechanics installs Right AC: Op-15 *Mechanics executes a task inadequately.*
2. AHM sends Right AC degradation alert: Op-06 *Data Team generates unclear/ambiguous prognostics/diagnostics*
3. MCC Plans AC Check: Op-27 *Task Generating Team makes an inadequate deadline for deferred defect.*
4. MCC does not revise the planned check : Op-26 *Task Generating Team does not examine/verify the prognostics / diagnostics*
5. Mechanics deactivates Left AC: Op-15 *Mechanics executes a task inadequately.*
6. Mechanics perform planned check: Op-16 *Mechanics executes a task too late*

Investigation reports identified hazards such as poor performance of diagnostics, late provision of diagnostic, provision of unclear diagnostic, lack of examination/verification of diagnostic information. All these hazards were identified by KLM experts during the Brainstorming session. The investigation reports could be used in order to refine these high-level hazards. We use the suffix "-r" to identify refined hazards.

Hazards addressing the diagnostic/detection performance problem could be refined in order to explain that poor performance is the cause of the hazard:

- Op-10-r *Data Team generate wrong prognostics/diagnostics due to poor performance of the prognostics/diagnostics method and implementation*

- Op-11-r *Data Team does not alert when there is a fault because the threshold is not met due to incorrectly defined threshold*.

Hazards addressing late provision of prognostics/diagnostics could be refined by explaining the meaning of being too late. In the investigated accident, the prognostics/diagnostics was considered to be late because this information could not be used just before take-off:

- Op-08-r *Data Team generates prognostics/diagnostics too late (after beginning of flight)*.
- Op-03-r *Aircraft Condition Monitoring System delays transmission of data to Data Team. Data Team delayed prognostics because of delay in data transmission from CM (delayed prognostics arrive after beginning of flight)*.

Hazard Op-06 *Data Team generates unclear/ambiguous prognostics/diagnostics* could be refined into several more detailed hazards that either deal with the provision of diagnostic or with the provision of prognostic and also either deal with the production of a false alert (the alert is produced while the component is not faulty) or production of an ambiguous result (it is not evident which component is faulty):

- Op-06-r1 *Data Team generates unclear diagnostics causing false alerts*
- Op-06-r2 *Data Team generates ambiguous diagnostics (the cause of the alert is ambiguous)*
- Op-06-r3 *Data Team generates unclear prognostics causing false alerts*
- Op-06-r4 *Data Team generates ambiguous prognostics (the cause of the alert is ambiguous)*

Hazard Op-26 could be refined by explaining that the MCC does not look at new occurrences of alerts once it has generated a task to deal with the first occurrence of an alert:

- Op-26-r *Task Generating Team stops to examine/verify new prognostics / diagnostics information after it has generated a task*

3.2. Health-Monitoring Normative Documents

Helicopter and aircraft Health-Monitoring certification, qualification or approval guidance documents written by certification authorities but also by industrial groups as Maintenance Programs Industry Group (MPIG) were examined. We selected 4 documents:

- MPIG MAP 2019-001 Operator Qualification of Aircraft Monitoring Process for purposes of satisfying ICA requirements [ReMAP_022] (for the sake of simplicity, it will be called MPIG-AHM later in this deliverable)
- FAA AC No: 43-218 Operational Authorization of Integrated Aircraft Health Management Systems [ReMAP_029] (called FAA-IAHM in this deliverable)
- FAA AC 29 MG 15. AIRWORTHINESS APPROVAL OF ROTORCRAFT HEALTH USAGE MONITORING SYSTEMS (HUMS) [ReMAP_049] (called FAA-HUMS in this deliverable)
- EASA, AMC 29.1465 Vibration health monitoring, part of CS-29 Helicopter Airworthiness document [ReMAP_002] (called EASA-VHM in this deliverable)

Documents on Helicopter Health-Monitoring (EASA-VHM and FAA-HUMS) were recommended to us by EASA experts, while the MPIG-AHM and FAA-IAHM documents dealing with Aircraft Health-Monitoring (AHM) were recommended by Embraer and KLM. These documents have different status as EASA-VHM and FAA-HUMS are well-established documents that were already applied in industry. MPIG-AHM and FAA-IAHM are more recent documents that could still be subject to changes, they are not routinely applied in industry. Another difference between these documents is that VHM/HUMS documents provide guidance for both the helicopter manufacturer and its operator whereas the AHM documents provide guidance for aircraft operators.

In Task 7.1, we do not intend to have an exhaustive analysis of normative documents. We are just looking for hazards and potential mitigations in these 4 documents. We will have an in-depth analysis of these documents and other important normative documents when we will work on Task 7.3.

The documents share a common high level view of assurance activities to be performed. Broadly speaking, there are 3 main activities:

1. Health-Monitoring System **Integrity** Assurance: these activities aim at establishing the correctness of the developed health-monitoring system. They could be seem as mitigation means against incorrect development of the equipment and functions of the Health-monitoring system;
2. Health-Monitoring **Performance** Assurance: these activities aim at establishing the effectiveness for the developed health-monitoring system. They could be seen as mitigation means against poor performance of a Health-Monitoring system;
3. **Contingency** Operation Assurance: these activities aim at preparing the safe operation of the health-monitoring system. They could be seen as mitigation means against inoperative health-monitoring system.

A description of the intended use of the health-monitoring system should be produced before these three assurance activities are performed. This includes the description of the aircraft system (for instance, tire pressure or brake wear sensor) that will benefit from AHM use. This also includes the description of the goal of the AHM application. The AHM application usually intends to add to, replace, or intervene in industry accepted maintenance practices or flight operations. For instance, the AHM application could be used to adjust maintenance program and inspection tasks. The intended use is the basis of the criticality determination that assess the safety effect that the AHM application can have on the aircraft. This assessment is based on the severity of the end result of a AHM application failure or malfunction.

The following table gives relevant paragraphs describing the 3 main activities in the four selected normative documents.

Table 4 – Relevant paragraphs for Integrity, Performance and Contingency Assurance in selected normative documents

	MAP-AHM	FAA-IAHM	EASA-VHM	FAA-HUMS
Integrity	C. Qualification of the system and methods C.4. Data fidelity and quality assurance i. Measurement/sensor Assurance ii. Data Transmittal Assurance iii. Data Processing Assurance iv. Alerting Assurance v. Resolution Assurance	8.2 Data Transmission. 8.3 Data Analysis and Implementation. 9.5 Data Transmission 9.6 Data Security	k. VHM system installation l. Ground-Based System Architecture h. Pilot Interface i. Maintenance Personnel Interface j. Fleet Diagnostic m. Software	f. Installation approval f.2 Airborne Equipment Installation. f.3 Ground Based Equipment Installation. f.3 C Ground Based Equipment Hardware. f.3.D Software f.3.E Data Processing. f.3.F Display and Peripheral Equipment. f.3.G Data Communications.
Performance	C.2. method for providing actionable alerts as well as tracking resolution	9.7.2 Alert levels 10.3.2 The operator should explain the method of alert notification	e. System Design Considerations f. Data Management g. Alert Management n. Performance Criteria o. Performance Validation	g. Credit Validation. g.1 Description of Application and Associated Credit. g.2 Understanding the Physics Involved. g.3 Validation Methodology. g.4 Controlled Introduction to Service. g.5 Synthesis of Credit
Contingency	E. Contingency procedures to handle temporary system outages. C.3. Training of Personnel	9.4 MEL 10.5 Training.	t. Minimum Equipment List (MEL) Recommendation r. Training Suitable	h.1.C HUMS ICA Items h.1.(i).(H) Training

For each of the three main assurance activities, we have reviewed the normative documents and identified 40 hazards. We identified 19 System Integrity hazards, 14 Performance hazards and 7 Contingency hazards. They are described in three tables. The first column contains an identifier for each hazard using the name of the document, the letter I for Integrity, P for Performance and C for contingency and a sequence number. For instance, the identifier MAP-AHM-I1 is used for the first Integrity hazard extracted from document MAP-AHM. We also indicate the paragraph in the normative document which relates with the hazard. The table also indicates an AHM function (Collect, Relay, Analyse, Generate, Plan and Execute) related with the hazard. The last column of the table indicates the failure mode of the AHM function that can be related with the hazard. Failure modes considered are: Inadequate, Missed and Late.

System Integrity Assurance.

For this group of assurance activities, we looked at hazards linked with the incorrect development of the equipment and functions of the Health-monitoring system.

Section C of MAP-AHM introduces the need to define a data fidelity and quality assurance that address all areas where process or measurement hazards may occur. MAP-AHM takes into consideration hazards related with each of the main AHM functions. FAA-IAHM does not provide explicit description of hazards. It refers to the criticality of the aircraft system that will benefit from AHM use when defining system integrity requirements for data transmission.

EASA-VHM refers to other chapters of regulations CS-29 [ReMAP_002] and to documents dealing with the certification of airborne or on-ground software [ReMAP_050], [ReMAP_051] in order to describe System Integrity. From the first analysis of these chapters and other documents, we were only able to identify a limited number of hazards. Hazards identified in FAA-HUMS are quite similar to the hazards identified in EASA-VHM.

Table 5 – Health-Monitoring System Integrity Hazards

Id	Description	Paragraph	Function	Fail. Mode
MAP-AHM-I1	*The sensor or measurement data is not accurately being recorded on the aircraft*	i. Measurement/sensor Assurance	Collect	Inadequate
MAP-AHM-I2	*Data is not provided on a timely and accurate basis to the ground-based processing system.*	ii. Data Transmittal Assurance	Relay	Inadequate
MAP-AHM-I3	*Data is not evaluated accurately*	iii. Data Processing Assurance	Analyse	Inadequate
MAP-AHM-I4	*Actionable insights are not developed according to the monitoring definition*	iii. Data Processing Assurance	Generate	Missed

Id	Description	Paragraph	Function	Fail. Mode
MAP-AHM-I5	*Alerts and actions are not transmitted from the monitoring system to operator personnel*	iv. Alerting Assurance	Generate	Missed
MAP-AHM-I6	*Alerts are not reviewed in a timely manner according to the definition of the monitoring system.*	v. Resolution Assurance	Generate	Late
MAP-AHM-I7	*Alerts are not appropriately actioned in a timely manner according to the definition of the monitoring system.*	v. Resolution Assurance	Plan	Late
FAA-IAHM-I1	*Data transmission rate, speed or reliability is not acceptable for the criticality of the AHM application*	s 8.2 and 9.5 Data Transmission.	Relay	Late
FAA-IAHM-I2	*Allowable interruptions in data transmission are not acceptable for the criticality of the AHM application*	8.2 Data Transmission	Relay	Missed
FAA-IAHM-I3	*Data used by the AHM application is illicitly altered or deleted*	9.6 Data Security	Relay	Inadequate
EASA-VHM-I1	*the System Integrity of the AHM system is not implemented according to the requirements of applicable normative documents*	k. VHM system installation	All	Inadequate
EASA-VHM-I2	*Data transfer, processing or networking integrity cannot be assured*	s f. Data Management and l. Ground-Based System Architecture	Relay	Inadequate
EASA-VHM-I3	*Interactions with the AHM system adversely impacts the pilot workload*	h. Pilot Interface	Execute	Late

Id	Description	Paragraph	Function	Fail. Mode
EASA-VHM-I4	*Remote access to all data acquired by the AHM systems in the operator's fleet is not adequately implemented.*	j. Fleet Diagnostic	Relay	Inadequate
EASA-VHM-I5	*Airborne or on-ground software is not developed according to the applicable normative document*	m. Software	All	Inadequate
FAA-HUMS-I1	*Airborne equipment is not developed according to the requirements of applicable normative document*	f.2 Airborne Equipment Installation.	Collect	Inadequate
FAA-HUMS-I2	*On-ground equipment is not developed according to the requirements of applicable normative document.*	s f.3 C Ground Based Equipment Hardware, f.3.E Data Processing and f.3.F Display and Peripheral Equipment	All	Inadequate
FAA-HUMS-I3	*On-ground software is not developed according to the requirements of applicable normative document*	f.3.D Software	All	Inadequate
FAA-HUMS-I4	*On-ground data communications is not developed according to the requirements of applicable normative document*	f.3.G Data Communications.	Relay	Inadequate

Performance Assurance:

For this group of assurance activities, we looked at hazards linked with the performance of the Health-Monitoring system. Documents EASA-VHM and FAA-HUMS provide detailed information on Health-Monitoring performance criteria and validation. Although some aspects might be too much oriented towards vibration monitoring and might not be fully applicable to AHM we tried to extract generic performance hazards from these documents.

Table 6 – Health-Monitoring Performance Hazards

Id	Description	Paragraph	Function	Fail. Mode
EASA-VHM-P1	*Sensor does not provide a reliable signal with an appropriate and defined performance.*	e. System Design Considerations	Collect	Inadequate
EASA-VHM-P2	*Sensor selection, positioning and installation does not to enable efficient health monitoring*	e. System Design Considerations	Collect	Inadequate
EASA-VHM-P3	*Sensor signal sampling rate is not adequate to enable efficient health monitoring*	e. System Design Considerations	Collect	Inadequate
EASA-VHM-P4	*Sensor signal enhancement- signal-to-noise enhancement - is not adequate to enable efficient health monitoring*	e. System Design Considerations	Collect	Inadequate
EASA-VHM-P5	*The time for upload/download, retrieval of sensor data or health report is excessive to enable timely health-monitoring.*	f. Data Management	Relay	Late
EASA-VHM-P6	*The Alert processing methodology does not deliver an adequate False Alarm rate,*	n. Performance Criteria and o. Performance Validation	Analyse	Inadequate
EASA-VHM-P7	*The Alert processing methodology does not deliver an adequate Prognostic Interval*	n. Performance Criteria and o. Performance Validation	Analyse	Inadequate
EASA-VHM-P8	*The Alert processing methodology does not deliver an adequate probability of detection.*	n. Performance Criteria and o. Performance Validation	Analyse	Inadequate
EASA-VHM-P9	*Data acquired is not sufficient for complete and reliable diagnostics to be produced*	n. Performance Criteria and o.	Analyse	Inadequate

Id	Description	Paragraph	Function	Fail. Mode
		Performance Validation		
EASA-VHM-P10	*The sensitivity of the signal acquisition is not adequate.*	n. Performance Criteria and o. Performance Validation	Analyse	Inadequate
EASA-VHM-P11	*The processed signal is not capable of identifying potential incipient defects for the monitored components*	n. Performance Criteria and o. Performance Validation.	Analyse	Inadequate
FAA-HUMS-P1	*The alert limits or trending are not adequate*	s g.2 Understanding the Physics Involved and g.3 Validation Methodology	Analyse	Inadequate
FAA-HUMS-P1	*The intervention action is not adequate.*	s g.2 Understanding the Physics Involved and g.3 Validation Methodology	Generate	Inadequate
FAA-HUMS-P1	*Component is not monitored often enough for the intervention action to be effective.*	s g.2 Understanding the Physics Involved and g.3 Validation Methodology	Generate	Missed

Contingency Operation Assurance:

For this group of assurance activities, we are looking at hazards linked with the management of inoperative health-monitoring system. All selected documents have a section about MEL dealing with the situations when all or a part of the AHM system is inoperative and a section about appropriate training of AHM application users.

Table 7 – Health-Monitoring Contingency Operation Hazards

Id	Description	Paragraph	Function	Fail. Mode
MPIG-MAP-C1	*The contingency procedure to handle temporary AHM system partial or total loss is not defined.*	E. Contingency procedures to handle temporary system outages.	Generate	Missed
MPIG-MAP-C2	*Maintenance staff does not apply the contingency procedure to handle temporary AHM system partial or total loss*	C.3. Training of Personnel	Generate	Inadequate
FAA-IAHM-C1	*The MEL does not include AHM system partial or total loss.*	9.4 MEL	Generate	Missed
FAA-IAHM-C2	*The maintenance personnel does not know mitigating actions in case the AHM data is missing due to aircraft or on-ground issues*	10.5 Training.	Generate	Inadequate
EASA-VHM-C1	*The loss of AHM data is not detected by Maintenance personnel*	t. Minimum Equipment List MEL Recommendation	Generate	Inadequate
EASA-VHM-C2	*Maintenance personnel does not apply back-up standard procedures when the loss of AHM data is detected*	t. Minimum Equipment List MEL Recommendation	Generate	Missed
FAA-HUMS-C1	*There is no procedure defined when the AHM system becomes inoperative.*	h.1.C HUMS ICA Items	Generate	Missed

We identified 40 hazards: 19 System Integrity hazards, 14 Performance hazards and 7 Contingency hazards. We associated with each hazard the main AHM function contributing to the hazard and its failure mode. In some cases, all functions could contribute to the hazard, for these hazards we used the term “All” instead of the list of all functions. Functions Generate (12 hazards) and Analyse (8 hazards) have the main functions contributing to hazards. Again this can easily be explained by the central role of these functions in Aircraft Health-Monitoring.

Table 8 – Count of functions associated with technical hazards

Function	Count
All	4
Analyse	8
Collect	6
Execute	1
Generate	12
Plan	1
Relay	8

Again the most common failure mode used in the mapping is “Inadequate” (27 hazards). This can be explained by the fact that several assurance activities intend to demonstrate that the result of a function is adequate, consequently, the related hazard is that the function provides an “inadequate” result. Furthermore, we used the “inadequate” failure mode when we had a choice of several failure modes because this failure mode is considered to be more severe than the two other failure modes (Late and Missed) and we preferred to include the most pessimistic hazards in our list.

Table 9 – Count of failure modes associated with technical hazards

Failure Mode	Count
Inadequate	27
Late	5
Missed	8

3.3. EASA AI/ML Roadmap

Documents [ReMAP_026, ReMAP_027, ReMAP_034] introduce EASA AI Roadmap that discusses the impact of Artificial Intelligence/Machine Learning (AI/ML) on various domains of the aviation transport system. The Roadmap assess the need to establish new regulations or to adapt existing ones in order to cope with AI techniques.

EASA discusses the application of AI/ML in several domains of aviation. Several domains could benefit from the AI/ML data oriented approach in order to build models of physical phenomenon. Several partners of ReMAP are investigating the use of AI/ML techniques to build structural or system degradation models that could be used to compute diagnostics and prognostics. EASA identifies predictive maintenance as a promising application of AI/ML. EASA also stresses the need to adapt EU regulations in order to apply AI techniques in the maintenance domain:

“In the other domains (operations, maintenance, ATM, aerodromes), the current regulations provide an open framework for the use of AI/ML. However, it must be noted that those regulations will need to be adapted to the specific applications of AI/ML; for instance, reduced crew operation, predictive maintenance, etc.”

EASA intends to define a common policy that can be applied to any domain-related regulations rather than issuing domain-specific guidance. Hence this common policy should be applicable to the CBM technologies investigated in ReMAP that are using AI/ML algorithms.

EASA identified challenges with respect to the use of AI/ML in the aeronautics domain. These challenges can be viewed as AI/ML technical hazards:

- AI/ML Integrity challenges:
  - "**Traditional Development Assurance frameworks are not adapted to machine learning**": the usual process for the development of an AI/ML application includes steps such as selection of data sets, training of the model using the selected data and the deployment of the trained model. These steps are not considered by the traditional development assurance framework (see [ReMAP_003] and [ReMAP_031] for an analysis of the incompatibilities between AI/ML and traditional software assurance);
  - "**Difficulties in keeping a comprehensive description of the intended function**": the intended behaviour of an AI/ML application is given by the data used during the training of the model, the result of the training is an approximation of the expected function of the system. This is quite different from the traditional software development method where intended function is captured by the software requirements. Software requirements are traditionally reviewed in software assurance, reviewing a huge data set does not seem possible;
  - "**Complexity of architectures and algorithms**"; traditional process for aeronautics software development tend to be rather conservative and promote simple software architecture that can be thoroughly assessed, AI/ML applications rely on complex learning frameworks that cannot be exhaustively assessed;
  - **Lack of "Adaptive learning processes**": AI/ML application development offers the possibility to continuously train an already operational model using new datasets in order to adapt the application to an evolving context. This possible evolution of the AI/ML application is not covered by traditional development assurance that usually considers that the software is frozen once it has been reviewed.
- AI/ML Performance challenges
  - **"Lack of predictability and explainability of the ML application behaviour";** for any new input, the result of AI/ML application depends on the correlation between the input with the data set that was used for the training process, this can lead to unpredictable outputs that may be difficult to explain to the user.
  - **"Lack of guarantee of robustness and of no 'unintended function''** as stated in [ReMAP_007], *"many properties of the system may either be entirely 'learned' from data, or otherwise partially specified by the data. In either case, small changes in this data may produce significant changes to a system's functional behaviour*." Conventional testing methods do not offer any guarantee with respect to the robustness of an AI/ML application.**;**
  - **"Lack of standardized methods for evaluating the operational performance of the ML/DL applications"** There is no consensus on performance metrics to be used to evaluate accuracy or error rate of an ML/DL application**;**
  - **"Issue of bias and variance in ML applications"** if the data sets used for training or the important parameters for the training are not properly selected there is a risk that the trained model has poor performance on the real data**;**

Table 10 – EASA AI Roadmap Challenges

Id	Description	Function
EASA-AI-I1	*"Traditional Development Assurance frameworks are not adapted to machine learning"*	Select, Train
EASA-AI-I1	*Difficulties in keeping a comprehensive description of the intended function;*	Select, Train
EASA-AI-I2	*Complexity of architectures and algorithms*	Train, Deploy
EASA-AI-I3	*Lack of Adaptive learning processes*	Select
EASA-AI-P1	*Lack of predictability and explainability of the ML application behavior*	Deploy
EASA-AI-P2	*Lack of guarantee of robustness and of no 'unintended function'*	Train, Deploy
EASA-AI-P3	*Lack of standardized methods for evaluating the operational performance of the ML/DL applications*	Train, Deploy
EASA-AI-P4	*Issue of bias and variance in ML applications*	Select, Train

We associated the EASA AI Roadmap challenges with three new AHM functions:

- Select: that is in charge of selecting data from the collected data for the AI/ML algorithms;
- Train: that is in charge of performing the model training
- Deploy: that is in charge of validating the trained model and preparing the trained model for the analysis activities

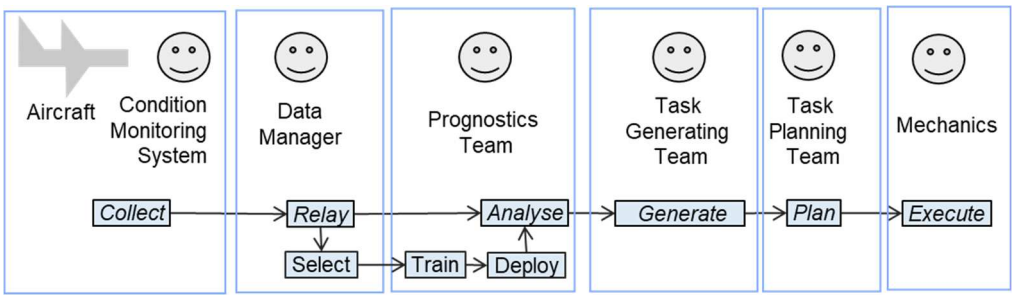

Figure 5 – Extended AHM Functions

4. Hazard Assessment

In this section we propose a framework to assess the effect of hazards that were previously identified. We first define various safety effects of the Aircraft Health-Monitoring application that is implemented using the various functions described in figure 5. It is our intent that the safety assessment is able to deal with all the CBM technologies investigated in project ReMAP. And, although we use the term AHM, we also intend to deal with both structural and system health monitoring hazards. Then we introduce a classification of the severity of the safety effect that is based on existing normative documents. Finally we explain how to relate hazards with their safety effect and severity using the notion of failure propagation.

4.1. Safety Conditions

The intended use of the AHM application is mainly to avoid unscheduled maintenance and operational interruptions or to reduce scheduled maintenance by adjusting the maintenance tasks intervals. Document FAA-IAHM [ReMAP_029] lists other intended uses of the global AHM function such as remote verification of systems functions without direct component access and assistance to MMEL procedures.

For all these intended uses, the AHM application should correctly monitor the health of a given component. The following figure from [ReMAP_020] helps to understand the various ways that the AHM application could fail to achieve this objective. The curve shows the degradation over time of the monitored component health. We use three coloured circles to describe the component health: green circle when the component is working correctly, orange circle when the component has a degraded behaviour and red circle when the component has failed.

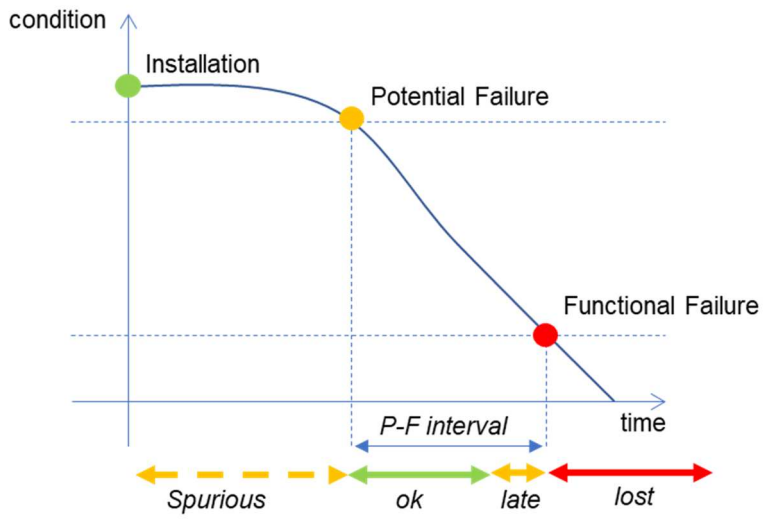

Figure 6 – Levels of degradation of a component condition and Timing deviations

The previous figure shows a temporal interval called the P-F interval that illustrates the moment when the AHM application is expected to produce alerts, to generate and to plan relevant maintenance actions. The current analysis is restricted to the case of

alerts that lead to immediate actions. The case of prognostics alerts that lead to future actions is not directly covered by now, future work in task T7.3 will deal with prognostics alerts. To define the safety conditions we consider various temporal deviations of the AHM application with respect to the P-F interval: before, at the beginning, at the end, after the end.

We also consider whether the component failure is easily detected by the flight crew or the cabin personnel. Following the MSG-3 definitions [ReMAP_033], failures that are easily detected are called evident failures and other failures are called hidden failures.

Finally, we consider various cases for the outcome of the AHM application such as correct outcome (alerts and actions are produced when the component is degrading), false outcome (alerts or actions are produced when the component is working correctly), lost outcome (alerts and actions are not produced when the component is degrading) or erroneous outcome (alerts are produced when the component is degrading but erroneous actions are produced that will not improve the component health).

We consider the following safety conditions:

- **Spurious AHM:** false alerts and maintenance actions are produced before the P-F interval when the component is working properly. These alerts and actions are useless and might create operational interruptions in order to check that the component is not faulty.
- **Correct AHM:** correct alerts and relevant maintenance actions are produced at the beginning of the P-F interval
- **Late AHM**: correct alerts and actions are produced at the end of the P-F interval when there is no sufficient time to perform the maintenance actions before the failure, this leads to operational interruptions or to flying with a faulty component during a limited time.
- **Lost AHM:** alerts and actions are not produced during and after the P-F Interval or correct alerts and actions are produced after the P-F Interval then the aircraft might be operated with a hidden faulty component during a potentially unlimited time.
- **Erroneous AHM:** correct alerts are produced but erroneous actions are performed, the component health is not improved and this might lead to the component failure.

These safety conditions are summarized in the following table. The table omits the Correct AHM situation as it is not a safety situation. There are two lines for the Lost AHM situation, each line describe one case of deviations leading to the loss of the AHM application.

Table 11- Safety Conditions of the global AHM function

AHM Safety Condition	**Timing Deviation** w.r.t P-F Interval	**Alerts and Actions Deviation**	**Detection of component failure**
Spurious	*Before*	*False*	*Hidden or Evident*
Late	*At the end*	*Correct*	*Hidden or Evident*
Lost	*During and after*	*Lost*	*Hidden*
Lost	*after*	*Correct*	*Hidden*

Erroneous	*Anytime*	*Erroneous*	*Hidden or Evident*

4.2. Severity Classification

To assess more precisely the severity of 4 AHM safety conditions one has to take into account the safety effect of the failure monitored by the global AHM function. MSG-3 define five Failure Effect Categories (FEC), two of them are related with safety: Evident Safety (Category 5) and Hidden Safety (Category 8). Other non-safety categories are: Evident Operational (Category 6), Evident Economic (Category 7) and Hidden Non-Safety (Category 9). Failures in category FEC 5 have a direct adverse effect on safety. Safety is adversely affected if the consequences of the failure condition would prevent the continued safe flight and landing of the aircraft and/or might cause serious or fatal injury to human occupants. To be direct the functional failure must achieve its effect by itself, not in combination with other functional failures (no redundancy exists). The Hidden Function Safety Effect category FEC 8 deals with hidden failures that can have an adverse safety effect when they occur in combination with one additional failure.

It is interesting to relate this classification with the failure condition classification used for system development in ARP-4654A (see [ReMAP_052]). The following table introduces the 5 severity levels (No Safety Effect, Minor, Major, Hazardous and Catastrophic) that are defined by their effect on people, on the flight crew workload and on the safety margin (e.g. remaining redundancies).

Table 12 – Classification of Safety Effects according to ARP-4654A and MSG-3

Classification	People	Workload	Safety Margin	FEC
CATASTROPHIC	loss of crew and passengers	prevent continuous safe flight and landing	prevent continuous safe flight and landing	5
HAZARDOUS	serious or fatal injuries to a relatively small number of passengers	High, physical distress	large reduction	5
MAJOR	discomfort to occupants possibly including injuries	significant increase	significant reduction	8 or Not-Safety
MINOR	some inconvenience to the occupants	slight increase	slight reduction	8 or Not-Safety
No Safety Effect (NSE)	No effect	No increase	No reduction	Not-Safety

The definition of direct adverse effect used in MSG-3 for FEC 5 directly refers to parts of the definition of Catastrophic (*prevent the continued safe flight and landing*) and Hazardous (*serious or fatal injury to human occupants*) severity levels. The definition for FEC 8 can be indirectly related with severity levels MINOR and MAJOR. In usual aircraft system designs, combinations of MINOR or MAJOR failures would lead to an adverse effect on safety as defined by MSG-3. Consequently, this notion of failure combinations is common to MSG-3 and ARP-4654A. But there are two differences between the classifications. First of all, FEC 8 is restricted to hidden failures whereas MAJOR and MINOR level can be applied to both evident and hidden failures. Secondly, as noticed by FAA in AC 25-19A [ReMAP_045], MSG-3 restricts the combinations to pairs of failure. The size of combinations considered in safety assessment defined in ARP-4654A is not limited. For systems with a high level of redundancy such as flight control system, combinations of 4 or 5 failures can be considered. A consequence of this difference is that MSG-3 would not include in FEC 8 some MINOR or MAJOR failures.

Appendix 2 of document IP-180 (see [ReMAP_023]) about the integration of AHM in the MSG-3 process provides examples of components that could benefit from AHM monitoring. A component considered by one example is the Inertial Unit (IU), the failure of this component belongs to the Hidden non-safety category 9. There are 4 (IU) per A/C, three operative IUs are sufficient but combinations made of the failure of three or more IUs would lead to a HAZARDOUS or CATASTROPHIC effect. It is likely that the classification of the loss of one IU is at least MINOR. Other examples in this appendix deal with brake wear sensor, hydraulic fluid level indicator, Air pressure regulator filter. These component failures belong to category FEC 9 but as the components are part of safety critical systems, it is very likely that these component failures are classified MINOR or MAJOR.

In order to assess the severity of AHM Safety Conditions we prefer to use the classification used in aircraft system development rather the 2 levels of the MSG-3 classification that are not precise enough. The following table gives a suggestion for the severity classification of AHM Safety Condition based on the severity classification of the failure of the monitored component. Columns give the severity of the failure of the monitored component. We restrict ourselves to No Safety Effect, MINOR and MAJOR because in modern Aircraft a single failure of a component is almost never classified HAZARDOUS or CATASTROPHIC. The lines give the AHM Safety Conditions.

Table 13 – Suggested Classifications of AHM Safety Conditions

Safety Condition	***Severity of monitored failure***		
	NSE	**MINOR**	**MAJOR**
Spurious	NSE	MINOR- -	MINOR- -
Late	NSE	MINOR-	MINOR-
Lost	NSE	if hidden then MINOR else MINOR-	if hidden then MAJOR else MINOR-
Erroneous	NSE	MINOR	MAJOR

When the monitored component failure has no safety effect then we consider that AHM safety Condition has no safety effect because, in the worst case, the AHM application would cause the component failure and this is classified NSE.

Spurious AHM should not have a safety effect as it occurs when the monitored component is not faulty. Nevertheless, as the investigation on the Serious Incident on B787 showed, false alerts could contribute indirectly to incidents because they lead the AHM operator to distrust the alert and discard any potentially correct alert. Furthermore, these alerts increase the number of human interventions and consequently increase the risk of human error when executing the maintenance actions. We consider that false alerts could slightly reduce the safety margins. So we propose to introduce intermediate levels for situations that have no effect on people or on the flight crew workload but that could reduce the safety margins (MINOR- - for slight reduction) and (MINOR- for a significant reduction). Spurious is classified MINOR- -.

Similarly, Late AHM should not have a safety effect as the failure is detected before occurring. The main effect should be either operational interruption in order to perform maintenance actions or flying with the faulty component deactivated if the maintenance actions can be deferred. But, if we take into account again the report on the serious incident of the B787, an important contributor to the incident was an incorrect decision to defer maintenance. We consider that, in the case of deferred maintenance that could be incorrectly executed, Late AHM reduces the safety margins significantly. Consequently Late AHM is classified MINOR-.

Table 14 - Definition of Proposed Classification Levels

Classification	People	Workload	Safety Margin	FEC
MINOR-	No effect	No increase	**significant reduction**	Not-Safety
MINOR- -	No effect	No increase	**slight reduction**	Not-Safety
No Safety Effect	No effect	No increase	No reduction	Not-Safety

If we assume that it is not easy for the maintenance staff to detect that the AHM application is lost then Lost AHM might lead to operate the aircraft with a hidden faulty component during a potentially unlimited time. For a hidden failure, the classification of Lost AHM should be similar to the classification of the monitored failure. If the failure is evident then the flight crew should be able to detect the failure and the effect should be similar to Late AHM. In that case, Lost AHM is classified MINOR-. If it is easy to detect the loss of the AHM application then it should be possible to fall back to a conventional maintenance practise such as periodic inspection. In that case, the safety effect of Lost AHM could be decreased.

In the worst case, Erroneous AHM could lead to performing a maintenance action that would cause the component failure. Hence the classification of Erroneous AHM should be similar to the classification of the monitored failure.

4.3. Failure Propagation

Hazards presented in the previous chapter can be viewed as the failure of one or several AHM functions described in figure 5. We have considered several failure mode: missed, failed, late, unclear and inadequate. These failure mode define the local effect of the hazard on a function. For instance, according to table 1 operational hazards Op-06 "*Data team generates unclear/ambiguous prognostics/diagnostics*" and Op-12 "*Data team is not functioning/operative*" are related with agent "*Data Management team*" and with AHM function *Analyse*. The failure mode related with Op-6 is *inadequate* whereas the failure mode related with Op-12 is *missed*. In order to assess the global effect of these hazards on the AHM application one has to consider the propagation of failure across the AHM functions. Such a propagation is described in the following figure. The origin of the failure propagation is the function associated with the considered hazard. In figure 7, function *Analyse* is the origin of the propagation. The propagation path goes from the origin function to a destination function used to assess the global effect of the hazard. Here, function *Execute* is used to assess the global effect because this is the function that has an actual effect on the Aircraft. The propagation path follows the information flow from function Analyse to function Execute (via functions Generate and Plan).

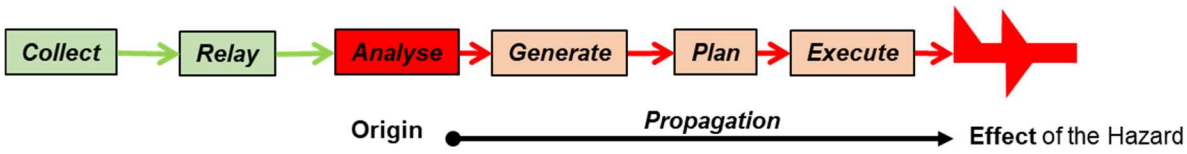

Figure 7 – Failure Propagation across AHM Functions

In a basic propagation path, all functions have the same failure mode. For instance, if function Analyse provides a late prognostic, then function Generate will not produce maintenance actions in a timely manner and function Plan will not be able to include these actions in the current plan and function Execute will not be able to take into account the actions at the right time. So the global effect of this hazard should be Late AHM.

Some intended uses of the AHM application might introduce simpler propagation path that bypass some AHM functions. For instance, let's consider that the AHM application is used in order to replace tasks such as:

- Visual check of the Central Maintenance Systems for maintenance messages
- Visual check of the Brake Wear Indicator
- Check of the Tire Inflation Pressure

For this intended use, the function Analyse (and possibly functions Generate and Plan as well) are not necessary for the Mechanics to perform the task. In that case, the failure propagation would bypass function Analyse. Hence, hazards related with Analyse would not have any impact.

Figure 8 - Failure Propagation with bypassed functions

A more complex propagation path has to be considered when data-oriented algorithms are involved. In that case we have to consider the role of functions Select, Train and Deploy in the propagation path. The following figure shows a propagation where a hazard related with function Select such as (EASA-AI-P4 - *Issue of bias and variance in ML applications*) potentially leads to an AHM Safety Condition. For instance, the selection of data only considered data collected during flight over in Europe. The data-oriented algorithm were trained on this set of data and deployed in order to analyse flights in a different geographical area with another distribution of temperature and humidity. If the degradation depends on these parameters then it could be the case that the alerts computed by function Analyse are late and leading to Late or Lost AHM.

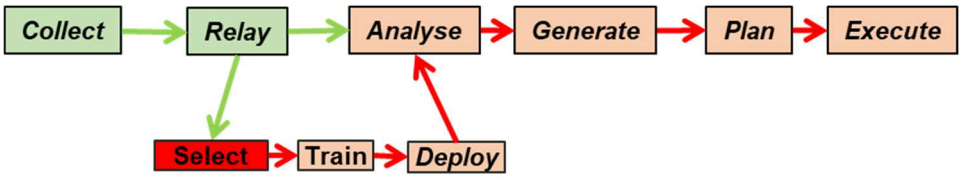

Figure 9 –Failure Propagation Path for data-oriented algorithms

The methodology presented in this chapter could be used to assess all the hazards previously identified for a given intend use of AHM application and a given classification of the monitored failure. This would require for each hazard to:

1. analyse its failure propagation (according to the intended use) and define the outcome of the propagation;
2. relate the propagation outcome with one of the 4 AHM safety conditions
3. use table 13 to classify the severity of the hazard

Once a hazard is assessed, either it is classified NSE and, with respect to safety, nothing needs to be done or it is in the other categories ranging from MINOR- - to MAJOR and the hazard should be mitigated using safety barriers.

5. Safety Barriers

In this chapter we discuss safety barriers that mitigate Aircraft Health Monitoring hazards. The role of mitigation means is either to limit the severity of the effect of the hazard or to decrease its likelihood of occurrence. Let's consider a hazard such as Op-11 "*Data Team does not alert when there is a fault because the threshold is not met*" the effect of this hazard is Lost AHM. According to table 13, the severity classification could be at most MAJOR. Several mitigations could be relevant for this hazard:

- H1: *keep in the maintenance programme a classical human inspection task with an escalated interval*. Consequently, a maintenance operator performing this inspection could detect the degradation even if the threshold used by the AHM application is not met. The effect of Op-11 when barrier H1 is taken into account would be NSE so this would be less severe than MAJOR.
- A1: *improve the definition of the threshold and check that the new thresholds are efficient*. Using barrier A1 would decrease the likelihood of not detecting a fault.
- T1: *use in parallel an alternate algorithm to compute degradation and compare produced alerts.* As in the case of barrier T1, using the alternate algorithm could lead to an improved degradation detection and could decrease the severity of the effect of Op-11.

These examples illustrate three categories of safety barriers: H1 belongs to human safety barriers; A1 belongs to assurance barriers and T1 belongs to technical barriers. These categories can be found both in the EASA AI/ML roadmap and in health-monitoring normative documents.

EASA AI/ML Roadmap defines the following mitigations categories:

- **Human-System interaction** and **Explainability of AI,** it covers the interactions between AI system and the user, and it deals with the capability to explain to human operators how an AI application is coming to its results and outputs;
- **Learning Assurance** whose objective of is to gain confidence at an appropriate level that an ML application supports the intended functionality;
- **AI safety risk mitigation** is based on the anticipation that assurance activities might not always be applicable because AI systems cannot be opened to a sufficient extent, in that case a technical component that would supervise the AI application may be necessary.

The health-monitoring normative documents define the following mitigation categories:

- **Intended use of AHM** and **Contingency** planning: that defines the role of the AHM application in the maintenance tasks and prepares the safe operation of the AHM application
- Health-Monitoring **Performance** and System **Integrity Assurance** that aims at gaining confidence in the efficiency of the AHM application and the correctness of its development.

The health-monitoring normative documents do not discuss technical barriers and the AI roadmap mentions AI safety risk mitigation but does not detail this category of barriers. Certification Authorities are generally reluctant to mandate a particular technical solution to mitigate hazards. They prefer to define assurance objectives that aim at limiting the hazard. In the following of the chapter we will focus on human safety barriers and assurance activities

5.1. Human Safety Barriers

EASA roadmap considers several intended uses of AI/ML techniques and it defines levels of autonomy of these intended uses. The levels of autonomy includes: human assistance role, human-machine collaboration and more autonomous machines. More autonomous machines would perform functions with no human intervention in operations but human stays in the loop at design-time and oversight-time. The roadmap indicates that human-assistance role seems less risky than the more autonomous role. Unfortunately, the roadmap does not provide assess of the impact of levels of autonomy in order to reduce or increase the effect of hazards.

The US FDA (Food & Drug Administration) in its document “Proposed Regulatory Framework for Modifications to Artificial Intelligence/Machine Learning (AI/ML)-Based Software as a Medical Device (SaMD)” [ReMAP_018] defined several intended uses of the AI/ML applications in the medical domain The FDA considers three levels of intended use:

1. to inform clinical management: the outcome of the AI/ML algorithm does not trigger an immediate or near term action, it is used either to inform of options related with a disease or to aggregate relevant information;
2. to drive clinical management: the outcome of the AI/ML algorithm is used to aid in treatment, diagnoses, triage of patients, identification of early signs of a disease;
3. to treat or diagnose : the outcome of the AI/ML algorithm is used to take an immediate or near term action in order to treat or to diagnose a disease

In the health domain, the severity of hazard is primarily based on the health condition of the population targeted by the software application. Three levels of health condition are used: Non-serious, Serious and Critical. A related document [ReMAP_038] considers that intended uses can reduce the severity of hazards. If the intended use is to treat or diagnose then there is no severity reduction, if it is to drive clinical management then severity is decreased by one level, and if it is used to inform clinical management then severity is decreased by two levels.

The decrease of severity is a recognition of the implicit role of human as safety barriers. When the application is used to inform or to drive clinical management, human have time to analyse and potentially correct the outcome of the application whereas in an application that such an Intensive Care Monitoring application nurses and doctors have to react immediately when a potentially false-alarm rings.

There is a direct analogy between human health and maintenance as it deals with aircraft health. In the aircraft maintenance process described previously we can find examples of three intended levels of use proposed by FDA:

1. to inform aircraft maintenance: the AHM application is used by the Reliability Engineer in order to collect fleet-wide statistics regarding the reliability of aircraft subsystems and to produce report for the Engineering Team.
2. to drive aircraft maintenance: the AHM application is used to aid the MCC Specialist and the Maintenance Engineers in selection of maintenance actions, diagnoses of failures, identification of early signs of a component degradation ;
3. to execute maintenance actions : the AHM application is used by the Mechanics to execute maintenance actions on the aircraft

If the AHM application is only used to inform maintenance management then only the Spurious AHM condition seems relevant. So in that case, according to table 13, if the monitored failure is classified MAJOR the classification of an AHM application would be decreased to MINOR- -.

Assessing the potential severity decrease when the AHM application is used to drive maintenance management is more difficult. We would need to know more precisely how the AHM application and the classical time based tasks are used in conjunctions. It could be, as in the case of barrier H1 presented in the beginning of this chapter, the case that AHM application does not replace the current maintenance tasks. In another approach the AHM application could be used to adjust some inspection intervals.

For many intended uses, it should be possible to decrease the severity of effect of hazards thanks to the role of human operators. This means that it is important that the future aircraft process maintenance process recognizes the role of human operators as safety barriers. The roles of human users of the AHM application should be extended with activities aiming at checking the outcome of the AHM application and reacting to possible degradations of the AHM application. Such roles are partly covered by the Health-Monitoring contingency planning that is recommended by the normative documents described in section 3.

5.2. Assurance-based Safety Barriers

Assurance activities allow to decrease the likelihood of occurrence of technical hazards. In section 3.2, we have already introduced assurance activities proposed by Health-Monitoring normative documents. The main activities are Performance Assurance that aims at establishing the effectiveness for the developed health-monitoring system and System Integrity Assurance that aims at establishing the correctness of the developed health-monitoring system.

We will not detail in this section all the assurance activities applicable to AHM. The column labelled “Paragraph” in tables 5 and 6 of chapter 3 provides references of the paragraph in the normative documents describing the assurance activities that should be applied. In the following we first explore a few difficult cases for assurance based safety barriers such as levels of performance assurance, system integrity assurance when Components Off-The-Shelf (COTS) are used and system integrity assurance when AI/ML algorithms are used. Finally, we suggest a preliminary Safety Risk Matrix that defines the acceptable assurance activities for the proposed classification levels

According to the normative documents described in chapter 3, Performance Assurance aims at demonstrating how the AHM system provides an acceptable defect detection performance. This includes proving that:

- Alert processing methodology can deliver an adequate False Alarm rate, Prognostic Interval and probability of detection.
- Data acquired in a flight is sufficient for complete and reliable diagnostics to be produced ,
- The sensitivity, dynamic range and bandwidth of the signal acquisition are adequate.
- That the processed signal-to-noise ratio is acceptable and that it is capable of discriminating the features required to identify potential incipient defects for the monitored components

Evidence should be provided in order to show that the mechanisms of failure or degradations are understood. This includes how a failure occurs and/or at what rate the degradation progresses and a determination of the point where intervention action is

necessary. At development time, either direct or indirect evidence can be used for Performance assurance. At operation time, controlled introduction to service can be used for Performance assurance.

Direct Evidence for Performance assurance includes:

- Actual service experience on AHM equipped aircraft of the same or of similar type and configuration, including information from component removals, inspections and other investigations which is relevant to the review of AHM system performance.
- "Seeded tests" (where the wear, defect, or deterioration is introduced, allowed to develop, and the technique response verified), Tests should be representative of the aircraft for which the credit is being sought and of test conditions representing the flight regime that would prevail when data is normally gathered (e.g., cruise). It should be established that the evidence gathered from on-aircraft ground trials or rig based seeded tests is valid in flight
- On- aircraft trials, investigating cause and effect.

Indirect Evidence for Performance assurance includes:

- Model based analytical methods for predicting damage progression may allow for a validation by claiming analogy with 'direct' evidence generated for other aircraft types or equipment. However, to validate this analogous data set, a degree of direct evidence for the actual equipment being monitored is still likely to be necessary to prove similarity of application. This might be achieved by performing an appropriate number of seeded defect tests.
- Reference to adequate performance in other applications

Full validation of performances might not be possible during the development period. A controlled introduction to service may be necessary to fully validate the performance. During this controlled introduction period, data is accumulated by operational aircraft, and from this data, validation can be performed. This period may also allow a proposed AHM application intended use to be operated in parallel with standard procedures when it is necessary to gain additional in-service validation by way of back-to-back comparison.

System Integrity Assurance activities are well-established for airborne systems. They generally require an in-depth analysis of system requirements, design and implementation. It is not always possible to achieve the same level of analysis for on-ground systems due to the lack of openness of its implementation especially when Components Off-The-Shelf (COTS) are used. Any ground based implementation using COTS must have satisfactory service history and an independent means of verifying the results of the processing. The intent of independent verification is to gain some degree of confidence in the COTS operational reliability. One approach would be to compare AHM proposed actions to actual maintenance performed as a result of inspection. This approach would require data collection on the system prior to applying AHM. The amount and duration of data collection should be planned at the beginning of the project. This independent verification means may be discontinued after significant quantities of the processed data consistently agree with the verifying means.

Another problem is assurance for implementations using AI/ML techniques. We have seen in section 3.3 that the traditional development assurance is not adapted in that case. So other assurance approach should be used in that case. In document [ReMAP_034], it is proposed to extend the traditional Development Assurance with the following Learning Assurance steps.

- Data management covers the identification of the various datasets used for training and evaluation and the dataset preparation. It also addresses the validation objective of completeness and correctness of the datasets with respect to the intended use, it also address the quality of the datasets. It should cover objectives on the independence between datasets and an evaluation of the bias and variance inherent to the data.
- Learning process management prepares the training phase. It selects key elements which could influence the performance of the training. The training environment is also selected and analysed for potential risks. The metrics that will be used for the various validation and verification steps should be selected and justified.
- Model training executes the training algorithm in the conditions defined in the previous step, using the training dataset originating from the data management process step. Once trained, the model performance, bias and variance are evaluated, using the validation dataset.
- Learning process verification evaluates the trained model performance on the test dataset.
- Model implementation consists of transforming the training model into an executable model that can run on a target hardware. The software tools necessary to perform this transformation should be identified and any associated assumptions, limitations or optimizations captured and validated.
- Inference model verification aims at verifying that the inference model behaves adequately compared to the trained model.
- Data verification is meant to close the data management life-cycle, by verifying with independence that the datasets were adequately managed.

Table 15 – Preliminary Safety Risk Matrix

	Performance	**Contingency**	**Integrity**
NSE	Not Required	Not Required	Not Required
MINOR - -	Required	Not Required	Not Required
MINOR -	Required	Required	Not Required
MINOR	Required & Reinforced	Required & Reinforced	Required
MAJOR	Required & Reinforced	Required & Reinforced	Required & Reinforced

Table 16 provides a preliminary Safety Risk Matrix that defines acceptable levels of (performance, integrity or contingency) assurance activities to be achieved for each severity classification. For instance, for a situation classified NSE assurance activities are not required.

We propose acceptable assurance activities associated with the new MINOR- - and MINOR- levels. As these levels are associated with Spurious AHM and Late AHM, performance assurance activities are required in order to limit the likelihood of false alarms or late interventions. For these classification levels it should be acceptable to rely only on indirect evidences for performance assurance. No Integrity assurance activities are required for these severity levels.

No contingency assurance is required for level MINOR- -. For level MINOR –, a basic contingency assurance activity is required: it should be checked that the loss of AHM data can be detected by Maintenance personnel

For higher classification levels such as MINOR and MAJOR performance assurance is required and should be reinforced using some direct evidence or a controlled introduction to service. Contingency assurance should also be reinforced with checking that back-up standard procedures are defined and that they could be applied by maintenance personnel when the loss of AHM data is detected. Integrity Assurance is also required for these levels. Assurance activities applicable for level MAJOR are reinforced with respect to activities applicable for level MINOR.

Assurance activities contribute to decreasing the likelihood of occurrence of hazards. At this stage of the project, we have not measured precisely how much each assurance activity could decrease likelihood. By now, we can compare likelihood reductions offered by assurance activities. We consider that a required and reinforced assurance activity will decrease likelihood more than a required activity. For a situation classified MAJOR all activities are required and reinforced, whereas for level MINOR- -, only Performance assurance activities are required. Consequently, the likelihood reduction will be greater for a situation classified MAJOR than for a situation classified MINOR- -.The preliminary safety risk matrix will have to be refined later during the project in order to provide quantitative values for the acceptable likelihood of situations classified in the various severity levels.

6. Concluding Remarks

The main results obtained by Task 7.1 that were reported in this document are:

- An Agent Based Model of the Aircraft Maintenance Process that helps to understand the roles of the main agents of this process and the interactions between agents. This model was built using inputs from KLM Maintenance organisation.
- The identification of Hazard related with CBM technologies
    - A set of thirty-nine Operational Hazards were identified thanks to a brainstorming session with KLM Maintenance specialists, the panel of specialists represented adequately the main agents of the Agent Based Model,
    - Another set of forty Technical Hazards was identified by reviewing accident investigation reports, Health-Monitoring normative documents and the recent EASA AI/ML roadmap.
    - The hazards were all linked with agents and with ReMAP Work-packages investigating the CBM technologies supporting the agents.
- A framework for hazard effect safety assessment was produced. This framework includes failure propagation analysis, safety conditions representing four safety relevant deviations of Aircraft health-monitoring and a proposed classification of these conditions using two new classification levels.
- A discussion of potential hazard mitigation including Human Safety Barriers, Assurance Safety Barriers.
- A preliminary safety risk matrix that defines acceptable levels of (performance, integrity or contingency) assurance activities to be achieved for each severity classification.

These results will be useful for the next steps for WP7 that will be dealing with dynamic quantitative assessment of CBM technologies (Task 7.2) and with regulatory aspects of the introduction of CBM technologies (Task 7.3). Task 7.2 will benefit from the work on the Agent Based Model in order to structure the model used to perform quantitative evaluations. These evaluations could be regarded as indirect evidence for Health Monitoring Performance Assurance. Task 7.3 will benefit from the work performed on Health Monitoring normative documents. The proposed framework for hazard effect safety assessment will be experimented in Task 7.3 and it will be discussed with maintenance stakeholders including Maintenance operators, Certification Authorities and National Aviation Authorities.

These results will also be useful for the next steps for other Work-Packages of ReMAP. We can use the mapping between Agents and ReMAP Work-Packages presented in Figure 3 in order to relate the identified hazards with the technologies developed in ReMAP WPs. The hazards and associated mitigations will be discussed with other Work-Packages in order to improve the relevance of identified hazards and the efficiency of mitigations.

Table 16- Description of milestone MS.6

Number	Title	Lead Beneficiary	Due Date	Means of verification
MS.6	Identification of hazards and safety barriers related with CBM technologies	WP7	M24	*List of aircraft maintenance hazards, safety risk matrix, and safety barriers is presented to the partners (D7.1);*

With the production of deliverable D7.1, the ReMAP project has reached milestone MS.6 "*Identification of hazards and safety barriers related with CBM technologies"* with a slight delay. The slight delay was caused by the COVID pandemic that forced some companies such as ONERA to partially close during April and May 2020.

The milestones was successfully reached because deliverable D7.1 that was distributed to ReMAP partners include

- List of aircraft maintenance hazard: table 1 gives a list of Operational Hazards identified during the Brainstorming session, table 5 gives a list of Health-Monitoring System Integrity Hazards, table 6 gives a list of Health-Monitoring Performance Hazards and table 7 gives a list of Health-Monitoring Contingency Operation Hazards.
- safety risk matrix: table 15 of the deliverable provides a preliminary safety risk matrix that defines acceptable levels of (performance, integrity or contingency) assurance activities to be achieved for each severity classification.
- safety barriers: chapter 5 presented safety barriers that mitigate Aircraft Health Monitoring hazards, they either limit the severity of the effect of the hazard or they decrease its likelihood of occurrence.

7. References

Id.	Bibliographical ref.	Category	Domain
001	B. Larder, M. Davis, HUMS Condition Based Maintenance Credit Validation, American helicopter Society 63rd Annual Forum, Virginia Beach, May 2007.	Reviewed Paper	Aeronautics
002	EASA, Certification Specifications and Acceptable Means of Compliance for Large Rotorcraft CS-29 , Amendment 5, 14 June 2018	Normative Text	Aeronautics
003	JM Faria, Non-determinism and Failure Modes in Machine Learning. In proceedings of IEEE International Symposium on Software Reliability Engineering Workshops (ISSREW), 2017	Reviewed Paper	Generic
004	D. Amodei, C. Olah, J. Steinhardt, P. Christiano, J. Schulman, and Mané, D., Concrete problems in AI safety. arXiv:1606.06565, 2016.	Technical Report	Generic
005	IJCAI-17 Workshop on Explainable AI (XAI) Proceedings, 20 August 2017, Melbourne, Australia	Reviewed Paper	Generic
006	JM Faria, Machine Learning Safety: An Overview, unpublished report, 2019	Technical Report	Generic
007	M. Douthwaite, T. Kelly, Establishing Verification and Validation Objectives for Safety-Critical Bayesian Networks, In proceedings of IEEE International Symposium on Software Reliability Engineering Workshops (ISSREW), 2017	Reviewed Paper	Safety-Critical
008	FAA report, Verification of Adaptive Systems, DOT/FAA/TC-16/4, 2016	Technical Report	Aeronautics
009	H. Alemzadeh, Dependable AI Systems, presentation at IFIP Working Group 10.4 Dependable Computing and Fault Tolerance 72nd Meeting, Longmont, Colorado, USA, June 22-25, 2017, 2016	Presentation	Generic
010	A. Rudolph, S. Voget, A.Mottok, A consistent safety case argumentation for artificial intelligence in safety related automotive systems - An Evaluation of a New Conceptual Functional Safety Approach, in proceedings of the European Real-Time Systems Symposium, Toulouse, 2018	Reviewed Paper	Safety-Critical
011	S. ten Zeldam, A. de Jong, R. Loendersloot, T. Tinga Automated Failure Diagnosis in Aviation Maintenance Using eXplainable Artificial Intelligence (XAI), Vol 4 No 1 (2018): Proceedings of the European Conference of the PHM Society	Reviewed Paper	Aircraft Maintenance
012	M. Buderath, P. P. Adhikari, Simulation Framework and Certification Guidance for Condition Monitoring and Prognostic Health Management, European Conference of the Prognostics and Health Management Society, 2012.	Reviewed Paper	Aircraft Maintenance

Id.	Bibliographical ref.	Category	Domain
013	D. Alexander, INTEGRATED VEHICLE HEALTH MANAGEMENT: RELIABILITY, SAFETY AND MAINTENANCE CREDITS, presentation at SAE Advanced Engineering UK, 2015	Presentation	Aircraft Maintenance
014	A Saxena, J Celaya, B Saha, S Saha, K Goebel, Metrics for offline evaluation of prognostic performance, International Journal of Prognostics and Health Management 1 (1), 20, 2010	Reviewed Paper	Aircraft Maintenance
015	Hölzel N., and Gollnick V. (2015), Cost-benefit Analysis of Prognostics and Condition-based Maintenance Concepts for Commercial Aircraft Considering Prognostic Errors, Annual Conference of the Prognostics and Health Management Society, 2015.	Reviewed Paper	Aircraft Maintenance
016	Adhikari P. P., Makhecha D., Buderath M.(2014), A Certifiable Approach towards Integrated Solution for Aircraft Readiness Management, Second European Conference of the Prognostics and Health Management Society, Nantes, France.	Reviewed Paper	Aircraft Maintenance
017	B. Verna, Condition Based Maintenance –A Regulator's Perspective, presentation at SAE 2015 Aerospace Standards Summit, 2015	Presentation	Aircraft Maintenance
018	US FDA, Proposed Regulatory Framework for Modifications to Artificial Intelligence/Machine Learning (AI/ML)-Based Software as a Medical Device (SaMD) - Discussion Paper and Request for Feedback	Normative Text	Safety-Critical
019	M. Wicker, M. Kwiatkowska, Robustness of 3D Deep Learning in an Adversarial Setting, April 2019, arXiv:1904.00923v1	Reviewed Paper	Generic
020	Tim Shaver, Aircraft Health Monitoring - FAA Perspective, IATA Conference, 13 November 2017	Presentation	Aircraft Maintenance
021	Miles Brundage et alter, The Malicious Use of Artificial Intelligence: Forecasting, Prevention and Mitigation, February 2018	Technical Report	Generic
022	Maintenance Programs Industry Group (MPIG)-MPIG Agreed Position (MAP) 019-001, Operator Qualification of Aircraft Monitoring Process for purposes of satisfying ICA requirements, January 2019	Normative Text	Aircraft Maintenance
023	International Maintenance Review Board Policy Board (IMRBPB) Issue Paper (IP), IP-180, Aircraft Health Monitoring (AHM) integration in MSG-3, April 2018	Normative Text	Aircraft Maintenance
024	AC No: 120-17B - Reliability Program Methods—Standards for Determining Time Limitations	Normative Text	Aircraft Maintenance
025	Gary McGraw, Harold Figueroa, Victor Shepardson, Richie Bonett, AN ARCHITECTURAL RISK ANALYSIS OF MACHINE LEARNING SYSTEMS: Toward More Secure Machine Learning	Technical Report	Generic
026	EASA Artificial Intelligence Roadmap 1.0 - A human-centric approach to AI in aviation	Normative Text	Aeronautics

Id.	Bibliographical ref.	Category	Domain
027	Guillaume Soudain, EASA Artificial Intelligence Roadmap, ISCLP Workshop, DGA TA, Toulouse, October 16, 2019	Normative Text	Aeronautics
028	Ralf Schneider, SHM/AHM in the context of aircraft maintenance programme development, 07-08/05/2019, SAE International AISC -SHM Technical Committee, Meeting #26	Normative Text	Aircraft Maintenance
029	AC No: 43-218 - Operational Authorization of Integrated Aircraft Health Management Systems	Normative Text	Aircraft Maintenance
030	IP170 - International Maintenance Review Board Policy Board (IMRBPB), Issue Paper Rotorcraft (IPR) - HUMS for credit	Normative Text	Aircraft Maintenance
031	E. Jenn et alter, Challenges to the Certification of Machine Learning for Safety Critical Systems, ERTS2 Conference, 2020	Reviewed Paper	Safety-Critical
032	Oliver WEISS, Maintenance of TomorrowThe AHM path from Airbus' Perspective, 5th Paperless Aircraft Operations and RFID Conference, November 26th, 2018	Presentation	Aircraft Maintenance
033	A4A, MSG-3, Operator/Manufacturer Scheduled Maintenance Volume 1 – Fixed Wing Aircraft	Normative Text	Aircraft Maintenance
034	Jean Marc Cluzeau, Xavier Henriquel, Georges Rebender, Guillaume Soudain, Dr. Luuk van Dijk, Dr. Alexey Gronskiy, David Haber, Dr. Corentin Perret-Gentil, Ruben Polak, Concepts of Design Assurance for Neural Networks (CoDANN), March 2020	Normative Text	Aeronautics
035	M. Feldman, S. A. Friedler, J. Moeller, C. Scheidegger, S. Venkatasubramanian, Certifying and Removing Disparate Impact, KDD'15, August 10-13, 2015, Sydney, NSW, Australia.	Reviewed Paper	Generic
036	Z. Lipton, The Mythos of Model Interpretability, 2016 ICML Workshop on Human Interpretability in Machine Learning (WHI 2016)	Reviewed Paper	Generic
037	Air Accidents Investigation Branch, Annual Safety Review, 2018	Normative Text	Aircraft Maintenance
038	International Medical Device Regulators Forum, "Software as a Medical Device": Possible Framework for Risk Categorization and Corresponding Considerations, 2014	Normative Text	Safety-Critical
039	AAIB Bulletin: 7/2018, Serious Incident of Boeing 787-9 Dreamliner, G-ZBKF	Normative Text	Aircraft Maintenance
040	A. Burt, B. Leong, S. Shirrell, X. Wang, Beyond Explainability: A Practical Guide to Managing Risk in Machine Learning Models	Technical Report	Generic

Id.	Bibliographical ref.	Category	Domain
041	M. Greaves, F. Elasha, J. Worskett, D Mba, H. Rashid, R Keong, Final Report EASA_REP_RESEA_2012_6 - Research Project: (VHM) Vibration Health or Alternative Monitoring Technologies for Helicopters, 2012	Technical Report	Aircraft Maintenance
042	AIBN, REPORT ON THE AIR ACCIDENT NEAR TURØY, ØYGARDEN MUNICIPALITY, HORDALAND COUNTY, NORWAY 29 APRIL 2016 WITH AIRBUS HELICOPTERS EC 225 LP, LN-OJF, OPERATED BY CHC HELIKOPTER SERVICE, 2018	Normative Text	Aircraft Maintenance
043	K. Fernandes, Aircraft Health Monitoring& Maintenance Costs, IATA MCC 2016	Presentation	Aircraft Maintenance
044	D. Virovac, A. Domitrović, E. Bazijanac: The Influence of Human Factor in Aircraft Maintenance, Promet – Traffic&Transportation, Vol. 29, 2017, No. 3, 257-266	Reviewed Paper	Aircraft Maintenance
045	FAA, AC 25-19A, Certification Maintenance Requirements, Mar. 2011.	Normative Text	Aircraft Maintenance
046	AAIB (2011): Report on the accident to Aerospatiale (Airbus Helicopters) AS 332 L2 Super Puma, registration G-REDL 11 nm NE of Peterhead, Scotland on 1 April 2009. Aircraft Accident Report 2/2011.	Normative Text	Aircraft Maintenance
047	AAIB (2014): Report on the accidents to Eurocopter EC 225 LP Super Puma G-REDW 34 nm east of Aberdeen, Scotland on 10 May 2012 and G-CHCN 32 nm southwest of Sumburgh, Shetland Islands on 22 October 2012. Aircraft Accident Report 2/2014.	Normative Text	Aircraft Maintenance
048	AIBN (2001): Report on the air accident 8 September 1997 in the Norwegian sea approx. 100 NM west north west of Brønnøysund, involving Eurocopter AS 332L1 Super Puma, LNOPG,operated by Helikopter Service AS. Air Accident Report 7/2001.	Normative Text	Aircraft Maintenance
049	AC 29 MG 15. AIRWORTHINESS APPROVAL OF ROTORCRAFT HEALTH USAGE MONITORING SYSTEMS (HUMS)	Normative Text	Aircraft Maintenance
050	RTCA / EUROCAE. Software Integrity Assurance Considerations for Communication, Navigation, Surveillance, and Air Traffic Management (CNS/ATM) Systems, DO-278A/ED-109A, 2011.	Normative Text	Aeronautics
051	RTCA / EUROCAE. Software Considerations in Airborne Systems and Equipment Certification, DO178C/ED-12C, 2011.	Normative Text	Aeronautics
052	Society of Automotive Engineers. Guidelines for Development of Civil Aircraft and Systems, SAE ARP 4754A, 2010.	Normative Text	Aeronautics

8. Confidential Appendix – Hazards identified with KLM specialists

For the sake of confidentiality, the table in this appendix is deleted in the Public version of the deliverable.