



Deliverable D10-1-5
Version. 1-0
Date 28/02/2016
Page 1 of 14

AF3

Advanced Forest Fire Fighting

D10.1.5 Minimising misuse of research activities report (M22)

Change Control:

Version #	Date:	Change:	Name:	Company:
0.1	12.09.2015	First draft	Michael Remes	EFPC
0.2	20.09.2015	Additions	Rebecca Brodeur	EFPC
0.3	29.09.2015	Additions	Dana Remes	EFPC
0.4	7.10.2015	Additions	Michael Remes	EFPC
0.5	10.10.2015	Additions	Dana Remes	EFPC
0.6	18.10.2015	Revisions	Dana Remes	EFPC
0.7	30.10.2015	Updates following AF3 Meeting	Dana Remes, Caterina Berbenni-Rehm, All Partners	EFPC
0.8	25.02.2016	Finalising	Dana Remes, Myer Morron, Michael Remes, Caterina Berbenni-Rehm	EFPC
0.9	26.02.16	Conclusions	Dana Remes, Myer Morron, Michael Remes, Richard Gowland, Caterina Berbenni-Rehm.	EFPC
1.0	28.02.16	Finalisation	Dana Remes	EFPC

Release Approval:

Name	Role	Date
Dana Remes	WP10 Leader	28.02.2016
Cecilia Coveri	Project Manager	29.02.2016



Deliverable D10-1-5
Version. 1-0
Date 28/02/2016
Page 3 of 14

Table of Contents

<u>1.</u>	<u>INTRODUCTION.....</u>	<u>4</u>
<u>2.</u>	<u>POSSIBLE MISSUSE TABLE + DRAFT MITIGATION STEPS</u>	<u>5</u>
<u>3.</u>	<u>CONCLUSIONS AND DRAFT RECOMMENDATIONS.....</u>	<u>13</u>
<u>4.</u>	<u>REFERENCES.....</u>	<u>14</u>

1. INTRODUCTION

This Deliverable - Minimising misuse of research activities report - will be produced twice during the lifetime of the project.

The First version is delivered for Month 22 as per the amended DoW, and the Second Version is due Month 36.

This First Draft concentrates on producing 'worst case scenarios', where we ask ourselves what could the AF3 output be used for if it got into the wrong hands.

All of the Partners and Advisory Board were asked to input into this document.

The Second Version which is due at the end of the project will update the scenarios and also provide recommendations to minimize the misuse of the AF3 research activities.

As mentioned in section 2 below, it is important to note that due to the nature of the project, AF3 target users are either governments or government backed organisations. As such, the AF3 system should be protected by government security systems. This gives some level of comfort, but of course there are always holes in any security system e.g. rogue employees, hackers etc. and therefore the concept of misuse of research results will always exist and should therefore always be monitored during the use of the AF3 system, which will continue beyond the end of the project.

Misuse of research results can be considered under three categories:

- Malicious use for example, for terrorist or sabotage purposes
- Dual Use, where elements of the AF3 system could conceivably be used for military as well as civilian purposes
- Ethical and Legal issues related to, for example, data protection issues and compliance with laws and regulations in individual countries.

We do our best in this report to highlight issues of concern but we do not guarantee that all issues are identified; we live in a world where technological development is moving forward very quickly and where governments are trying to catch up by implementing new laws and regulations to protect their citizens and infrastructure. Therefore, in this respect the report should be seen as indicative of issues of concern at this moment in time and the report will be updated towards the end of the project.

2. POSSIBLE MISSUSE TABLE + DRAFT MITIGATION STEPS

The Table below contains all of the possible issues as identified by the AF3 Consortium and Advisory board to date.

It is important to note that due to the nature of the project, AF3 target users are either governments or government backed organisations. As such, the AF3 system will be protected by their own security systems.

Potential Issues are classed as: M = Malicious, D – Dual Use, E – Ethical and Legal

What elements of AF3 project results can be misused?	Potential Issues	Risk Level	Possible Mitigation	Notes
Access to “pellet making” machine	<ul style="list-style-type: none"> Sabotage or tampering with machine Safety of those protecting machine and/or stored pellets Change the bags to something non-biodegradable/harmful? Maintenance issues 	M-Low D-Low E-Low	<ul style="list-style-type: none"> Restrict Access Only approved stations will have the ability to use the “pellet filling” machine to ensure that undesirable chemicals are not being used for negative purposes. 	Machine will be stored by government agencies and under their security.
Changing content of pellets e.g. introducing harmful chemical agents	<ul style="list-style-type: none"> Introduction of toxic chemicals to harm wildlife or people Introduction of fire accelerants to make situation worse 	M-Low D-Low E-Medium	<ul style="list-style-type: none"> Random testing of Pellet chemical composition Documents/Records produced by pellet making machine 	<ul style="list-style-type: none"> Machine will be stored by government agencies and under their security. The Pellet Making

	<ul style="list-style-type: none"> • Access to stored pellets 		<p>operators need to be signed off by authorised personnel after each production run</p>	<p>Machine is a standard machine similar to milk bag filling machines. Even if the AF3 specific machines are built in to be disabled, it will not be difficult to adapt a milk bag filling machine.</p> <ul style="list-style-type: none"> • Pellets will be Biodegradable and as such are not stored filled in. Rather, they are filled to order.
Dual Use	<ul style="list-style-type: none"> • The Government bodies themselves could use the AF3 System for dual use. 	M-Low D-High E-Low		Machine will be stored by government agencies and under their security.
Security implications of using Sparx Systems Enterprise software	<ul style="list-style-type: none"> • Malicious modification to information • Manipulating information • The tool uses a commercial or a proprietary database to store requirements? – Yes 	M-Low D-Low E-Low	<ul style="list-style-type: none"> • The tool provides security to prevent inadvertent or malicious modifications to information? – Yes • The tool provide an interface for 	From D21.2

			manipulating information? - Yes	
<p>Unmanned Ground Vehicles (Section 4.1.1)</p> <p>Ground-mobile robots can be classified into three main classes:</p> <ul style="list-style-type: none"> • Wheeled robots (W) • Tracked robots (T) • Legged robots (L) 	<ul style="list-style-type: none"> • See table of UGV possible problems on page 46 of D2.1.2 • Sabotage of UGVs • Safety of those controlling UGVs 	<p>M-Low D-Low E-Low</p>	<ul style="list-style-type: none"> • Regular maintenance of UGVs, with sign-off sheets by authorised maintenance companies • Access to all areas controlled by security passes, other forms of identification 	<p>From D21.2</p> <p>Vehicles will be stored by government agencies and under their security.</p>
<p>Nub-e Capsules act as a forestry sprinkler, scattering extinguishing agents fully automatic and controlled when a fire approaches and environment temperature is just below 100°C.</p>	<ul style="list-style-type: none"> • Introduction of toxic chemicals to harm wildlife or people • Introduction of fire accelerants to make situation worse • Access to stored capsules • Tampered with capsules once produced and placed. 	<p>M-High D-Low E-Low</p>	<ul style="list-style-type: none"> • Random testing of capsules chemical composition • Documents/Records produced by capsule making machine operators need to be signed off by authorised personnel after each production run 	<p>From D21.2</p> <p>Will these only be dispatched on private or secure areas or will the public have access such as in parks?</p>
<p>AF3 Technologies:</p> <ul style="list-style-type: none"> • Web based system for visualization • Situation Awareness tools (viewers, enhanced reality, management modules) 	<ul style="list-style-type: none"> • Hacking of web-based systems • DDoS attacks on any web-based systems • Power or internet networks failing, even for a short time • Power outages 	<p>M-Low D-Low E-Medium</p>		<p>From D21.2 (section 4.1.3)</p> <p>This is not Misuse of AF3 results</p> <p>Possible Data</p>

<ul style="list-style-type: none"> • Mechanisms for the interoperability and data sharing based on the abovementioned technologies • Virtual training tool • Web-service for the recording of weather parameters in real-time • Mechanisms for interoperability between training and management tools by the import of data from real scenarios to virtual 	<ul style="list-style-type: none"> • Data Protection 			<p>Protection Issues need to be looked into.</p>
<p>Emercarto-Sigueme, SatforMAP, SatforMedia, EmeRA and SLPT, form, together with the related web services, data base, systems of communication, etc., a complete platform for managing the firefighting operations at every level or responsibility in the command chain</p>	<ul style="list-style-type: none"> • Power or internet networks failing, even for a short time • Power outages • Hacking of web-based systems • DDoS attacks on any web-based systems 	<p>M-Low D-Low E-Medium</p>		<p>From D21.2 (section 4.1.3)</p> <p>This is not Misuse of AF3</p> <p>Data Protection???</p> <p>Backup power?</p>
<p>Satellite Images - Thanks to the access to Landsat archives it is possible to track</p>	<p>Loss of satellite contact due to external issues, power outages, potential hacking</p>			<p>From D21.2 (section 4.1.5)</p>

land cover changes over up to 40 years.				This is not Misuse of AF3 possibly should be removed in next Version.
Unmanned Aerial Vehicles - UAV imaging sensor	<ul style="list-style-type: none"> - Unauthorised UAVs getting in the way of official methods of fire extinction/control - Hacking of UAVs or control room for fire-prevention UAVs to stop them doing their job - Possible risks to those operating UAVs in terms of blackmail and threats to safety 	M-Low D-Low E-High		From D21.2 (section 4.1.7) T6.1.1
In order to increase public awareness on fire prevention AF3 proposes the development of a social network based service integrating the use of smartphones, internet and dedicated broadcasting. Potential for hacking and misuse.	<ul style="list-style-type: none"> - Privacy issues. - Data Protection - If app-based, possibility of malware or hacking of apps to spread false information - If computer-based, possibility of hacking to spread false information - Possible security issues with those manning official responses for social network, either via blackmail or threat - Network and communication issues could force social network to be 'down' when most needed. 	M-Medium D-Low E-Medium		From D23.1 (section 3.2.1) This needs to be looked at further for the next version.

From D23.1 (section 3.2.1) Collect location and other data (status, contact data, capability, etc.) from means in the incident area and of those available for future deployment	Privacy issues.	M-Medium D-Low E-High		
System on board planes/helicopters for dropping pellets is sabotaged. E.g. the container carrying the pellets is cracked.	<ul style="list-style-type: none"> - Pellets drop from the plane in an unplanned for manner. Could cause collateral damage on the ground. - Possible risk to ecosystem? 	M-Low D-Low E-High		
Crowd behaviour models Do these models collect private data regarding individuals? If so, how will this be handled?	Are there legal issues related to this?			Task 3.2.2 Only a model - not based on real time so not an issue.
Simulation Host The models integrated in the simulation host will make predictions using real data. Also mentioned in Task 3.3.2 is "real video distribution in real time."	How sensitive is this data? Is it subject to data protection rules? E.g. some data may not be transferrable cross-border.	M-Medium D-Low E-High		Task 3.3.1 Is this only a simulator or is real time information also provided?
Task 4.3.1 (FHG-EMI, ELBIT) due in Month 30 Safety and risk analysis for fire-fighting with pellets.			Test on the security of the equipment	Will need to be referenced for the next Version

<p>Task 4.3.2 (Pyro) due in Month 18 Safety and risk analysis for preventative fire-fighting with capsules</p>	<p>Possible hazard effects of the impact of containers (containing the preventative layer system consisting of nets and capsules), the impact of capsules, and possible effects of the nets that fix the capsules in trees and bushes)</p> <p>Effects on wildlife/ecosystem?</p>		<p>Test on the security of the equipment</p>	<p>Will need to be referenced for the next Version</p>
<p>Task 4.3.3 (ELBIT, FHG-EMI) due in Month 33 Safety and risk assessment of airborne fire-fighting platforms</p>	<p>Addresses the risks of air-borne fire-fighting platforms and their operators during active fire-fighting with pellets.</p>			<p>Will need to be referenced for the next Version</p>
<p>Task 6.2.1 Ground observation & Ancillary data</p>	<p>How is the data controlled? Who has access to it? When is the data destroyed? This question also relates to other areas of AF3 where data is collected.</p>			<p>Will need to be analysed for next version</p>
<p>Task 7.1.1 Physics and chemistry of firefighting ELBIT will analyse chemical compatibility of the pellets with new proposed fire extinguishing materials</p>	<p>What are the identified risks and how can they be mitigated? - lack of toxicological data for fire extinguishing agents - lack of data on impact of extinguishing agent on nature - only basic lab-scale environmental testing within the project possible</p>		<p>- substantial toxicological expertise up to product evaluation concerning health and environmental tolerability from environmental authority</p> <p>Material Safety Data Sheets and the</p>	



Deliverable D10-1-5
Version. 1-0
Date 28/02/2016
Page 12 of 14

	<ul style="list-style-type: none">- commercial products do not disclose composition- lab scale test provides results which might be not realistic- interaction of decomposition products of plants and firefighting chemicals could create unexpected substances		registration of Fire Retardants for use by relevant authorities. Environmental Issues Report 10.2.2	Chemical and Environmental Issues Report 10.2.1
--	--	--	--	---

3. CONCLUSIONS AND DRAFT RECOMMENDATIONS

This section is to show the way of thinking for this draft, however, this will be completely reworked in the next Version.

- 1) Restrict Access to pellet machines - Only approved stations should have the ability to use the “pellet filling” machine to ensure that undesirable chemicals are not being used for negative purposes.
Recommendation: Criteria required to determine the meaning of an “approved station”.
- 2) Random testing of Pellet chemical composition
Recommendation: Standard operation Procedure (SOP) required indicating how testing should be done, so all testing is carried out the same way and results can be compared. Also need to determine time intervals for random testing, and data recording procedures and storage of results.
- 3) Documents/Records produced by pellet making machine operators need to be signed off by authorised personnel after each production run
Recommendation: Criteria for authorising personnel e.g. vetting procedure. Perhaps two signatures should be required as a precautionary measure. How to prevent falsifying signatures at a timepoint well after a production run?
- 4) Recommendation: Contingency measures need to be considered for the following potential harmful events on the AF3 system: Hacking of web-based systems; DDoS attacks on any web-based systems; Power or internet networks failing, even for a short time; Power outages; Data Protection
- 5) Unauthorised UAVs getting in the way of official methods of fire extinction/control
Recommendation: Procedures should be put in place whereby a no fly zone is created and implemented at a moment’s notice in case of a fire disaster situation.
- 6) Collect location and other data (status, contact data, capability, etc.) from means in the incident area and of those available for future deployment
Recommendation: How will this data be protected? Some of this data may relate to people, other data could have the potential of causing mass panic. This issue needs to be looked into and considered very carefully to avoid ethical and legal issues and also potential panic that may lead to casualties.
- 7) Pellets drop from the plane in an unplanned for manner. Could cause collateral damage on the ground.
Recommendation: Development of scenarios, simulations and training exercises where these events could occur. This will prepare for these kind of events and enhance subsequent training activities.

4. REFERENCES

Al-Qaida in the Arabian Peninsula calls for supporters to start wildfires:
<https://publicintelligence.net/inspire-magazine-wildfires/>,
<http://wildfiretoday.com/2012/05/02/al-qaeda-magazine-encourages-forest-fire-arson-in-the-us/>

Bags used are biodegradable within 3 months: <http://www.helicomag.com/2014/07/19/return-of-%E2%80%98water-bombs%E2%80%99/>

Dangers of hobbyist UAVs: http://www.nytimes.com/2015/07/20/us/hobby-drones-hinder-california-firefighting-efforts.html?_r=1,
<http://www.techtimes.com/articles/70307/20150720/personal-drones-prevented-firefighter-helicopters-putting-out-forest-fires.htm>,
<http://www.latimes.com/local/lanow/la-me-ln-drone-california-wildfire-20150625-story.html>,
<http://www.firerescue1.com/fire-products/technology/articles/1964470-Wildfire-managers-Drones-a-threat-to-firefighters/>,

Weather modification concerns: <http://www.weathermodification.com/>,
<http://www.globalresearch.ca/weather-warfare-beware-the-us-military-s-experiments-with-climatic-warfare/7561>,
http://www.wanttoknow.info/war/haarp_weather_modification_electromagnetic_warfare_weapons, <http://www.geoengineeringwatch.org/>