

2.2.1.2 Defining understanding requirements

Practical guidance – space

Authors: ACTIONS demonstrator project

This guidance considers the understanding requirements of the ML component developed under the ACTIONS project, which carries out autonomous fire detection from on-board a small Earth observation satellite. Figure 1 shows the SUDA architecture of a RAS as outlined by AAIP.

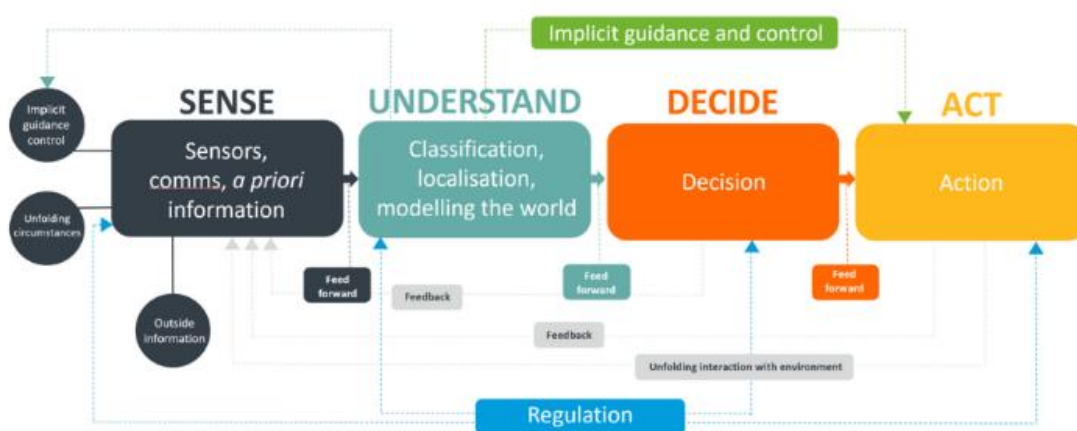


Figure 1 – Sense, Understand, Decide, Act (SUDA) model.

The emergency response service system demonstrated in the ACTIONS project is designed to **sense** Earth observation data, **understand** what level of active fire the data contains through ML classification, **decide** what kind of alert to generate, and then to **act** by delivering the alert and relevant data products.

As the **understanding** element of the SUDA architecture of the ACTIONS system, the definition of requirements allocated to the ML component is described in this guidance.

System safety requirements

To define what the ML component must achieve to ensure the system is sufficiently safe, a set of system safety requirements must first be defined. BoK section 1.3 Defining safety requirements provides guidance for defining these for a RAS.

The system safety requirements defined for the ACTIONS system necessitate that the fire alerts generated in-orbit and sent to the emergency services on the ground are accurate, truthful, and timely. These requirements were defined in response to two identified hazards:

- Services miss an emergency.
- Services are directed to a false emergency.

Missed detections, or misdirection of emergency services to attend non-fires both pose a risk to property, the natural environment, and potentially to human life. Four system safety requirements were defined in response:

- REQ-SAFE-ER-1 - The Emergency Response Service shall determine the location of a visible active fire within 200 m of its true location.
- REQ-SAFE-ER-2 - The Emergency Response Service shall inform emergency services of a visible active fire within 3 hours of it starting.
- REQ-SAFE-ER-3 - The Emergency Response Service shall positively identify 95% of all visible active fires acquired by the satellite instrument within the area of interest.
- REQ-SAFE-ER-4 - The Emergency Response Service shall falsely indicate visible active fires in the area of interest at a rate not exceeding current fire alert service.

Definition of ML component

System safety requirements must be allocated and interpreted for the ML component specifically. Understanding the makeup of the ML component and its interfaces within the system is key to this allocation. Figure 2 visualises where the ML component interfaces exist within the ACTIONS emergency response system.

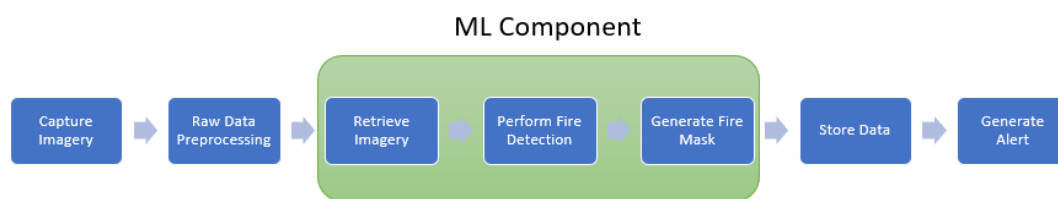


Figure 2 – System interfaces of ML component.

The neural network model developed for the ML component performs semantic segmentation, carrying out fire detection at the pixel level. The model outputs masks, where each pixel (representing a specific area on the ground) is labelled as fire or non-fire.

Understanding what the ML model development data contains is also necessary to understand what the detections represent. Important features of the data used to train the ACTIONS neural network model were:

Truth labelling:

- The process by which the training data has been labelled as containing fire or non-fire pixels determines how detection will be carried out by the model.

Data format:

- The metre per pixel resolution of the imagery will determine what level of location accuracy is possible to achieve.

Operational scenarios

The allocation of system safety requirements to the ML component also requires consideration of the defined operational scenarios and assumptions made about the operating environment. BoK section [1.1.3 – Defining operating scenarios](#) provides guidance on how to define these for a RAS.

Assumptions made about the operating environment of the emergency response system were outlined as follows:

- The satellite is in a sun synchronous orbit and will never operate in darkness.
- Data captured by sensors matches correctly with the expected ground location.
- A constellation of several satellites is in orbit, to monitor the ROI in timely intervals.

Operating scenarios of the system were defined concerning latency of the ML component:

- The ML component completes the fire detection process for each input frame (of size 2100 x 1575 pixels) at a maximum rate of 5 seconds. This is necessary for the component to successfully process the amount of data it receives as the satellite passes over the ROI at a rate of 7.14 kilometres per second.

Features that would be present in the data received by the ML component were also defined, and included various combinations of the following:

- Active fires of large, medium, and small size, and no active fires.
- Light to heavy cloud cover, and clear skies.
- Land type e.g., agricultural, temperate rainforest.

Definition of ML component requirements

Of the ACTIONS system safety requirements, three were allocated to the ML component: all except the timeliness requirement. The capability of the system to make timely alerts relies on a constellation of satellites in orbit, so this requirement remained allocated at system level.

The ML safety requirements concerning performance were defined as follows:

- **MLSR1** – All points of the mask generated by the ML component shall be less than 6 pixels outside the boundary of the area of the real fire.
 - **Rationale** – This requirement is derived from system safety requirement REQ-SAFE-ER-001. 6 pixels represents 180m, so this requirement will ensure that the actual fire is never more than 180m from a reported position.
- **MLSR2** - The ML component shall correctly identify the presence of a fire that satisfies the Schroeder¹ conditions in a frame for 95% of real fires.
 - **Rationale** – This requirement is derived from system safety requirement REQ-SAFE-ER-003. The Schroeder conditions represent the threshold for labelling of active fires in Landsat-8 data.
- **MLSR3** - The ML component shall not identify the presence of a fire in a frame where there is not a real active fire more than 52 times per month.
 - **Rationale** – This requirement is derived from system safety requirement REQ-SAFE-ER-004. FIRMS is being considered as the gold standard for FPs, therefore equivalent or better performance is safe. The main concern is that FPs don't happen so frequently that they become hazardous through diverting

¹ The sensor tuned conditions for active fire detection set out by Wilfrid Schroeder, Patricia Oliva, Louis Giglio, Brad Quayle, Eckehard Lorenz, and Fabiano Morelli. Active fire detection using Landsat-8/OLI data. Remote Sensing of Environment (Elsevier), 185:210 – 220, 2016. ISSN 0034-4257. doi:10.1016/j.rse.2015.08.032.

fire response resource or nuisance distraction to operators. There is also a hazard that frequent FPs will result in operators ignoring genuine fires or even turning the system off.

A fourth requirement was also defined concerning robustness of the ML component to data features:

- **MLSR4** - ML performance requirements shall be satisfied for all data across the range of factors identified in Table 1.
 - **Rationale** – *The factors identified in Table 1 capture the key features of the data that may be encountered during operation. Any values that were determined not to be in scope for the application are indicated in the final column of the table.*

Table 1 – Key features of data present in operational scenarios.

Element	Value	In-scope
Land type	Temperate rainforest	True
	Agricultural	True
	Urban	True
	Industrial	True
	Grassland	True
	Desert	False
	Sea	False
Fire size	Small <30x30m	False
	30x30m<=Small-medium<60x60m	True
	60x60m<=Medium-large<90x90m	True
	Large >=90x90m	True
Fire intensity	Low < Schroeder conditions ¹	False
	Medium > Schroeder conditions	True
	High >> Schroeder conditions ¹	True
Clouds	None	True
	Low coverage<25% of tile	True
	25% of tile<=Low-medium coverage<50% of tile	True
	50% of tile<=Medium-high coverage<80% of tile	True
	High coverage >80% of tile	True
Time of day	Early morning 7-9 am	True
	midday 12-14	True

Element	Value	In-scope
	late afternoon 4-6	True
	Night	False
Time of Year	Winter	True
	Spring	True
	Summer	True
	Autumn	True

Summary of approach

1. Define system safety requirements.
2. Define the **understand** element of the system (e.g., the ML component).
3. Allocate system safety requirements to the **understand** element.
4. Define safety requirements specific to the **understand** element considering the defined operational scenarios.