ONNX Workgroup

Statement of Work

ONNX Safety-related profile Workgroup

July 19, 2024

Contents

[1 Introduction 2](#_Toc172299667)

[1.1 Terms 2](#_Toc172299668)

[1.2 Contents 2](#_Toc172299669)

[1.3 Main objectives 2](#_Toc172299670)

[2 Workgroup Activities 3](#_Toc172299671)

[A1: Elicitation of industrial needs and requirements 3](#_Toc172299672)

[A2: Consolidate Requirements for the ONNX profile 4](#_Toc172299673)

[A3: Definition of the Scope of the ONNX Safety related profile 4](#_Toc172299674)

[A4: Analysis of the ONNX standard 5](#_Toc172299675)

[A5: Elaboration of the specification guidelines 5](#_Toc172299676)

[A6: Development of the ONNX Safety-related profile - semantics 6](#_Toc172299677)

[A7: Development of the ONNX Satefy-related profile - format 6](#_Toc172299678)

# Introduction

## Terms

The following terms are used in the document:

* **Trained ML model**: the conceptual structure of graphs and operators that maps a set of input tensors to a set of output tensors. The Trained ML Model Description (TMD) is represented using the *Trained Model Description Language* (TMDL).
* **Trained ML Model Description** (TMD: a concrete representation of the conceptual trained ML Model that can be interpreted by a human or a program.
* **Trained ML Model Description** (TMDL): The language used to represent a *Trained ML Model* (TMD).

## Contents

This document gives a first definition of the activities to be carried out by the ONNX safety-related profile workgroup. This “workplan” is aimed at being presented *and discussed* during the Workgroup kick-off meeting planned for the end of September.

## Main objectives

Provide a definition of the formalism used to represent a trained ML model...

* *... that has an understandable and non ambiguous syntax and semantics.*

The description of the ML model expressed using this formalism must be a Low level Requirement for the implementation phase in the sense that its interpretation and implementation shall not require any further information that the one given by the description of the ML model.

* *... that allows multiple levels of accuracy and precision for the description of a given model.*

The language used to describe the model (i.e., its syntax and semantics) must be non ambiguous, but a model may be ambiguous if this ambiguity is acceptable or even necessary to leave some freedom to the implementer (e.g., for optimization). The objective is to identify, control, and possibly remove this ambiguity by an appropriate refinement of the ML model description.

# Workgroup Activities

This section presents the different activities of the workgroup. Their dependencies are expressed via their inputs/outputs.

### A1: Elicitation of industrial needs and requirements

#### Objectives

* Elicit end-users needs related to the ONNX format, i.e., What are the activities using ONNX models?, What are the evidences required by certification authorities that involve the ONNX model[[1]](#footnote-1)?, How do the ONNX model impact these activities?,
* Elicit requirements applicable to the ONNX standard to satisfy the end-users needs. Those requirements shall cover all aspects of the standard, including documentation, graphs and operators semantics, file format, reference implementation, etc.

#### Rationales

Clarify the expectation of end-users. Ensure that the requirements for ONNX are traceable to one or several end-users’ needs.

#### Inputs

* Certification standards (e.g., ARP6983, ISO/DPAS 8800, ECSS-E-HB-40-02A DIR1, etc.)
* Company-specific requirements

#### Outputs

* D1.a.<x>: End users needs and requirements for domain <x>.

#### Detailed activities

The activities defined below are per domain.

##### End-Users Needs Elicitation

* UNAct1: Definition of the *Trained Model Description (TMD)* artefact (e.g., the Machine Learning Model Description (MLMD) in ARP6983)
* UNAct2: Description (overview) of the machine learning development process
* UNAct3: Description of the development process objectives and activities that:
* Produce the TMD
* Take the TMD as input
* UNAct4: Description of the development process verification objectives and activities that apply to the TMD
* UNAct5: Constraints on the TDM, that come from:
* the Development and verification activities
* the Industrial context
* UNAct6: Expression of the needs

##### *ONNX Requirements Expression*

The activities below take the end-user needs as inputs

* ORAct1: Definition of the list of the aspects to which the requirements for a safety-related ONNX profile will apply, e.g.,
* Semantics of the operators
* Semantics of the graph
* Data types
* Metamodel
* Concrete syntax (format)
* Documentation
* Traceability
* Versioning
* etc.
* ORAct2: For each aspect of the list, definition of the requirements

*Examples of requirements that may be expressed:*

* The semantics of the Trained Model Description Language (TMDL) used to describe the TMD shall be defined both informally (for documentation purposes) and formally using a mathematically-grounded language. This covers all that is needed for tooled and/or human interpretation of any valid TMD described using the TMDL (including, (e.g., operators and graphs).
* The formal definition of the TMDL shall define precisely and accurately the expected results of the interpretation of any valid TMDL model. The level of precision and accuracy may be a parameter of the description of the semantics.
* A reference implementation shall be provided for each operator. The reference implementation shall be accompanied with all the necessary information describing the execution environment used to validate compliance with the formal specification.
* In the TMD, it should be possible to indicate the meaning of each dimension of the tensors

### A2: Consolidate Requirements for the ONNX profile

#### Objectives

* Consolidate, filter, and prioritize the requirements identified for the different industrial domains in D1.a.<x>.
* Discriminate requirements aimed at the preservation of the model semantics from requirements aimed at facilitating / supporting other development assurance activities.

#### Rationale

The ONNX Safety-related profile must be unique whereas the needs comes from different industrial domains, referring different certification standards. This activity is aimed at defining a consensual and consistent set of requirements.

#### Inputs

* D1.a.<x>: End users needs and requirements for domain <x>.

#### Outputs

* (D2.a) ONNX safety-related Profile Requirements

#### Detailed activities

##### Consolidation of requirements

* CRAct1: Consolidation and fusion of semantically equivalent requirements
* CRAct2: Grouping and prioritization of requirements

### A3: Definition of the Scope of the ONNX Safety related profile

#### Objectives

* Selection of the set of operators and constructs to be considered in the Safety-related profile.

#### Rationale

In order to keep the effort reasonable and maximize or chance to produce useful results within a reasonable time frame, we propose to work on a restricted set of operators and constructs. This set will be defined according to the actual needs of the end-users (i.e., the models they want to implement).

#### Inputs

* End user use cases

#### Outputs

* (D3.a) Safety-related Profile Scope Definition

#### Detailed activities

##### Definition of the Safety-related Standard Scope

* DSCAct1: Identification/definition of the Safety-related industrial use case reference models
* DSCAct2: Extraction of the operators and constructs from the Safety-related industrial use cases reference models
* DSCAct3: Consolidation of the TMDL operators and constructs for the Safety-related profile, from the reference models possibly augmented with necessary additional operators and constructs.

### A4: Analysis of the ONNX standard

#### Objectives

* Identify the parts of the standard that need to be updated / clarified / modified in order to comply with the Safety-related Profile Requirements defined in D2.a, for the subset of the standard identified in D3.a.

#### Rationales

Once the requirements for the format are defined, the work consists to find what needs to be described, improved, fixed,... in the existing ONNX standard. In particular, all elements that are unclear or which interpretation is left to the implementer shall be spotted, analysed, discussed, and a proposal for clarification/correction may be proposed if required. These proposals may be applicable to a whole part of the standard e.g. a recommendation may concern the documentation of all operators).

#### Inputs

* (D2.a) Requirements applicable to the ONNX profile
* (D3.a) Safety-related Profile Scope Definition

#### Outputs

* (D4.a) ONNX Analysis and Recommendations for the Safety-related Profile

#### Detailed activities

##### Analysis of the ONNX standard

* AnaAct1: Analysis of the compliance of the ONNX standard with respect to each of the requirements and identification of non-compliances.
* AnaAct2: Provision of recommendations, solutions, guidance to modify the ONNX standard.

### A5: Elaboration of the specification guidelines

#### Objectives

State of the Art and proposal of guidelines for the specification of the graph and operators to comply with D4.a.

#### Rationales

Various approaches and notations may be used to specify the graph and operators in a formal way. This activity is aimed at proposing a solution acceptable with respect to the end-users needs and requirements.

#### Inputs

* (D2.a) Requirements applicable to the ONNX profile

#### Outputs

* (D5.a) Specification Guidelines

#### Detailed activities

##### Prototype guidelines

* ProAct1: Elaborate a first set of (informal + formal) specification guidelines and apply them on a few operators (e.g., conv) and constructs in order to discussed and reviewed by the workgroup

##### Elaborate guidelines

* • ElaAct1: Elaborate the final set of guidelines (including notation, presentation of the specification, etc. to ensure a consistent presentation of the specification)

### A6: Development of the ONNX Safety-related profile - semantics

#### Objectives

Development of the ONNX Safety-related profile semantics to address issues identified in (D4.a), using the formalism and approach defined in D5.a

#### Inputs

* (D4.a) ONNX Analysis and Recommendations for the Safety-related Profile
* (D5.a) Formal Specification Guidelines

#### Outputs

* (D6.a) ONNX Safety-related profile (graph execution part)
* (D6.a) ONNX Safety-related profile (operators part)
* (D6.b) ONNX Safety-related profile reference implementation

Detailed activities *To be completed.*

### A7: Development of the ONNX Satefy-related profile - format

#### Objectives

Development of the ONNX Safety-related exchange format in compliance with the recommendations given in (D4.a).

#### Inputs

* (D4.a) ONNX Analysis for the Safety-related Profile
* ONNX standard

#### Outputs

* (D7.a) ONNX Safety-related profile format

#### Detailed activities

*To be completed.*

1. E.g., those concerning the MLMD in the ARP6983/ED-324. [↑](#footnote-ref-1)