|  |  |
| --- | --- |
|  | Moving Picture, Audio and Data Coding by Artificial Intelligence  www.mpai.community |

|  |  |
| --- | --- |
| **Public document** | |
| N219 | 2021/04/14 |
| Source | MPAI General Assembly #7 (MPAI-7) |
| Title | Assessing Conformance of MPAI standard Implementations |
| Target | MPAI Members |

# Introduction

By reliability, robustness and fairness (in the following called Performance) of AI-based devices, services and applications (in the following called Implementations), we mean:

*Reliability*: the Implementation performs as specified by the Implementerfor the released version, e.g. within the application scope, stated limitations and the period of time specified by the Implementer.

*Robustness*: the ability of the Implementation to cope with data outside of the stated application scope with an estimated degree of confidence.

*Fairness*: means that the training set and/or network is open to testing for bias and unanticipated results so that the applicability of the system can be assessed.

The three definitions are meant to apply for data outside of the training set.

From a user’s viewpoint, Performance is a necessary characteristics. From an implementor’s view­point, Performance is a desirable characteristics because a user seeks assurance about perfor­mance before buying or using an implementation.

By Conformance (Testing) we mean the assessment that the Performance of an Implementation of a Components of an MPAI standard is above a certain threshold. The definition of Performance is application specific. The result of Conformance Testing needs not be a yes/no, as it could very well provide “grades” of Conformance.

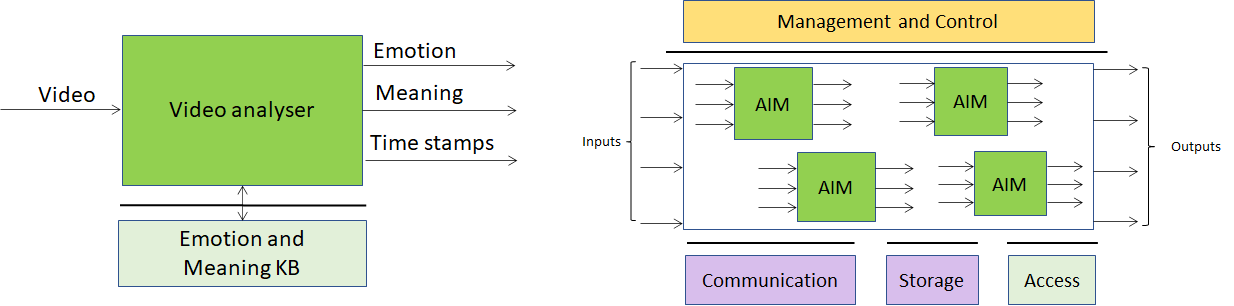
Conformance is a tool that MPAI can provide to support the needs of those who wish that an Implementation does not cross some ethical boundaries. Typically, Conformance can be used for different purposes.

This document is for public distribution. However, it is work in progress.

# MPAI’ s approach to AI system standards

MPAI identifies and describes Use Cases that can be realised as an AI system designed to achieve specified goals. Such an AI system can be implemented

1. With a set of interconnected AI Modules (AIM) whose individual functions, and input/output data formats are unambiguously specified (left-hand side of *Figure 1*).
2. Executed in a standard AI Framework (AIF) (right-hand side of *Figure 1*)



*Figure 1 – MPAI AI Module (AIM) and AI Framework (AIF)*

# MPAI and conformance

An MPAI Implementation refers to an AIM used in a Use Case or to the complete set of AIMs making up the Use Case.

In the MPAI world, testing an Implementation, i.e., a device, service or application, for Confor­mance implies providing the Means, i.e., tools, procedures, data sets etc., specific to the AIMs and, potentially, to the complete MPAI Implementation.

MPAI should not aspire to be the entity that actually tests an MPAI Implementation for conforman­ce. MPAI’ s role should be limited to the provision of Means that enable a third party to test the conformance of an AIM and of the set of AIMs that make up a Use Case. The third party can be the actual implementer or a private entity assessing Conformance using the MPAI Means.

# MPAI conformance infrastructure

With a proper infrastructure, MPAI can offer the possibility to make MPAI Implementations that are more explainable, i.e., more reliable, robust and fair than other solutions because it is possible to trace back an output from the results of AIMs, each performing a well-defined task using and producing standard data formats.

The said infrastructure can be implemented with the following steps:

1. An MPAI Implementation is uniquely associated with the following information:
   1. Identifier of Implementation provider.
   2. Identifier of Implementation.
   3. Version number of Implementation.
   4. Identifier of MPAI Use Case.
2. From the Identifiers above, a user should be able to access the following information:
   1. The AIM(s) the Implementation is using.
   2. The AI tools and modules the AIM is using.

|  |  |
| --- | --- |
| Note1 | An Implementation needs not be the full device/service/application. |
| Note2 | Identifiers need not to be assigned by a single registration entity. |
| Note3 | Registration entities should be elements of a chain of trust. |
| Note4 | A user report unsatisfactory performance to a reputation system. |

The nature and identity of the root of trust is for further discussion.

# The MPAI-instigated “market”

This is a possible sequence

1. MPAI develops the MPAI-AI standard and the Conformance Testing Means.
2. An Implementer makes an MPAI-AIF Implementation.
3. An Accredited Testing Laboratory (ATL)
   1. Acquires the right to use the Conformance Testing Means from MPAI.
   2. Tests the MPAI-AIF Implementation for conformance.
4. MPAI develops an application standard (e.g. MPAI-MMC) that specifies the AIMs and the AIM combination that supports a specific Use Case.
5. The (independent) Implementers:
   1. Develop all the AIMs required to support Implementations of the Use Case.
   2. Submit their AIM Implementations to ATL(s) providing information about operation constraints, wiring etc. but are not required to provider information about the inside of the AIM, unless they decide to do so.
6. The ATL(s):
   1. Use MPAI’s Conformance Testing Means to test AIM Implementations for conform­ance.
   2. Report Conformance Testing Results to Implementers.
7. Conformance Testing Results allow Implementers to put AIMs on sale with a Conformance seal.
8. An Implementer:
   1. Acquires different AIMs.
   2. Builds an Implementation of the Use Case.
   3. Submits the Implementation to an ATL.
9. The ATL:
   1. Tests the Implementation for Conformance.
   2. Reports Conformance Testing Results to the Implementer.
10. The Use Case Implementer may put AIMs on sale with a Conformance seal. A Conformance seal is not a requirement to put an Implementation on the market. however, consumers will know that the Implementation is not Conforming.
11. MPAI could take upon itself the task of
    1. Publishing information on (register of) Implementations.
    2. Managing their reputation.

Very often Conformance Testing will require large amounts of data. MPAI could collect those data sets and license their use for a fee. This would be *possible* thanks to Article 4.7.2 “Intellectual property rights” of the MPAI statutes:

*Through its own activities, MPAI may generate its own protectable Intellectual Property Rights (IPR), such as Technical Specifications, excluding patents. This IPR is held by MPAI. The Board of Directors shall determine how the IPR will be used.*

Of course, if MPAI engages in such an activity, its should not earn profits.