Assurance Strategy for New Computing Platforms in Safety-Critical Avionics

Håkan Forsberg, Kristina Lundqvist and Andreas Schwierz

MÄLARDALEN UNIVERSITY
SWEDEN

Technische Hochschule
Ingolstadt

New COTS-Based Computing Platforms for Avionics

Assurance Strategy for New Computing Platforms in Safety-Critical Avionics

New Types of Architectures

- **Machine learning using hardware accelerators**
  - The underlying hardware is trained to behave in a certain way
  - How do we know when it behaves sufficiently correct?
- **Approximate computing**
  - accuracy is traded for better performance or energy consumption e.g. through
    - reduced number of bits in the arithmetic operations
    - approximate findings of results from expensive function calls

Other Domains

- **ISO26262 developed microcontrollers**
  - Use of another domain's processes to ensure use in safety-critical avionics applications?
  - How?

Assurance?

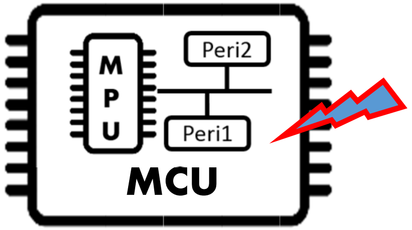
- Assurance according to SAE ARP 4754A and RTCA/DO-178C
  - *The planned and systematic actions necessary to provide adequate confidence and evidence that a product or process satisfies given requirements*
  - Reduction of the uncertainty in a correct product behavior

COTS Makes Assurance Challenging

- The whole COTS design is supplier controlled
- COTS components can be as complex as systems
- COTS integrates features for many applications (COTS = commercial-off-the-shelf for several customers)

What's the problem?

- COTS devices are not developed according to the accepted practice for avionics but the integrator still has to provide ***confidence and evidence that the product satisfies given requirements including safety***



No influence on development by avionics integrator

Development Assurance vs. COTS Assurance

- Development assurance:
  - Described in RTCA/DO-254
  - Self-developed AEH according to **system requirements**
  - Rigorous process-based approach to avoid design errors
  - → Confidence in, AEH safely performs as intended in its **system context**

- COTS assurance:
  - Described in several documents
  - Already developed HW components for a variety of applications
  - COTS assurance activities to demonstrate product integrity against **system requirements**
  - → Confidence in, COTS safely performs as intended in its **system context**

➡ **Same goal, different means**

COTS Hardware Assurance Today

- The certification authorities have produced several guidance documents for COTS assurance throughout the years
  - The early documents were activities based and consequently difficult to reuse for new components
  - The latest guidance document* (joint proposal by FAA and EASA) is objective based and supposed to address all kinds of COTS

*EASA, Notice of Proposed Amendment 2018-09, "Regular update of AMC-20:AMC 20-152 on Airborne Electronic Hardware and AMC 20-189 on Management of Open Problem Reports," TE.RPRO.00034-006.

Assurance of New COTS Technology

- The latest certification guidance documents may still be applicable but suffer from assuring new COTS technology

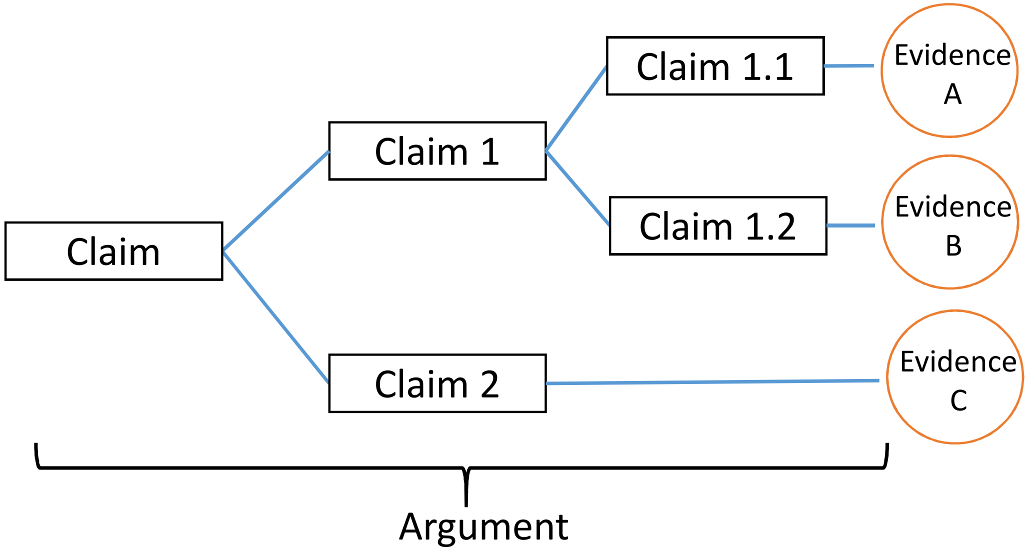
- New hardware technology has to be treated extra careful from a certification perspective

There must be **convincing arguments** that the new technology does not violate the confidence that the final product satisfies given requirements including safety

A New Assurance Concept
(for COTS Hardware)

- Based on assurance cases and overarching properties

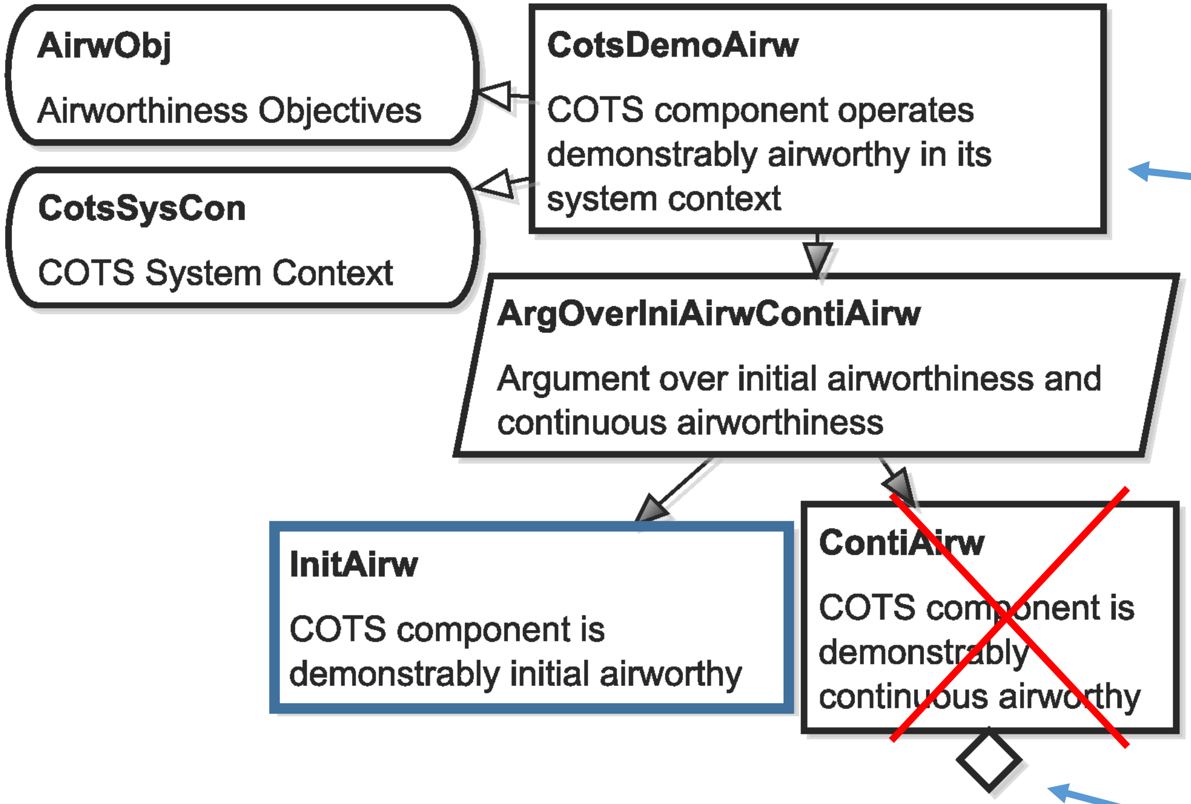
"An assurance case is an explicit argument that a system or service is acceptable for its intended use" – C. Michael Holloway, NASA Langley Research Center



The new assurance concept is suitable for emerging COTS hardware

A New Assurance Concept

Top level argument



Context

AirwObj

Airworthiness Objectives

CotsSysCon

COTS System Context

CotsDemoAirw

COTS component operates demonstrably airworthy in its system context

ArgOverIniAirwContiAirw

Argument over initial airworthiness and continuous airworthiness

InitAirw

COTS component is demonstrably initial airworthy

~~**ContiAirw**~~

~~COTS component is demonstrably continuous airworthy~~

Top-claim based on EASA's CS requirements – here derived to COTS

Goal

Strategy

Not further studied

Undeveloped Goal

Six Sub-Claims Cover COTS Demonstrably Initial Airworthiness

Must address two different levels

Isolated COTS

1. COTS component's **Intended** behavior
2. COTS component's **Correct** behavior
3. COTS component's **Acceptable** behavior

Integrated COTS

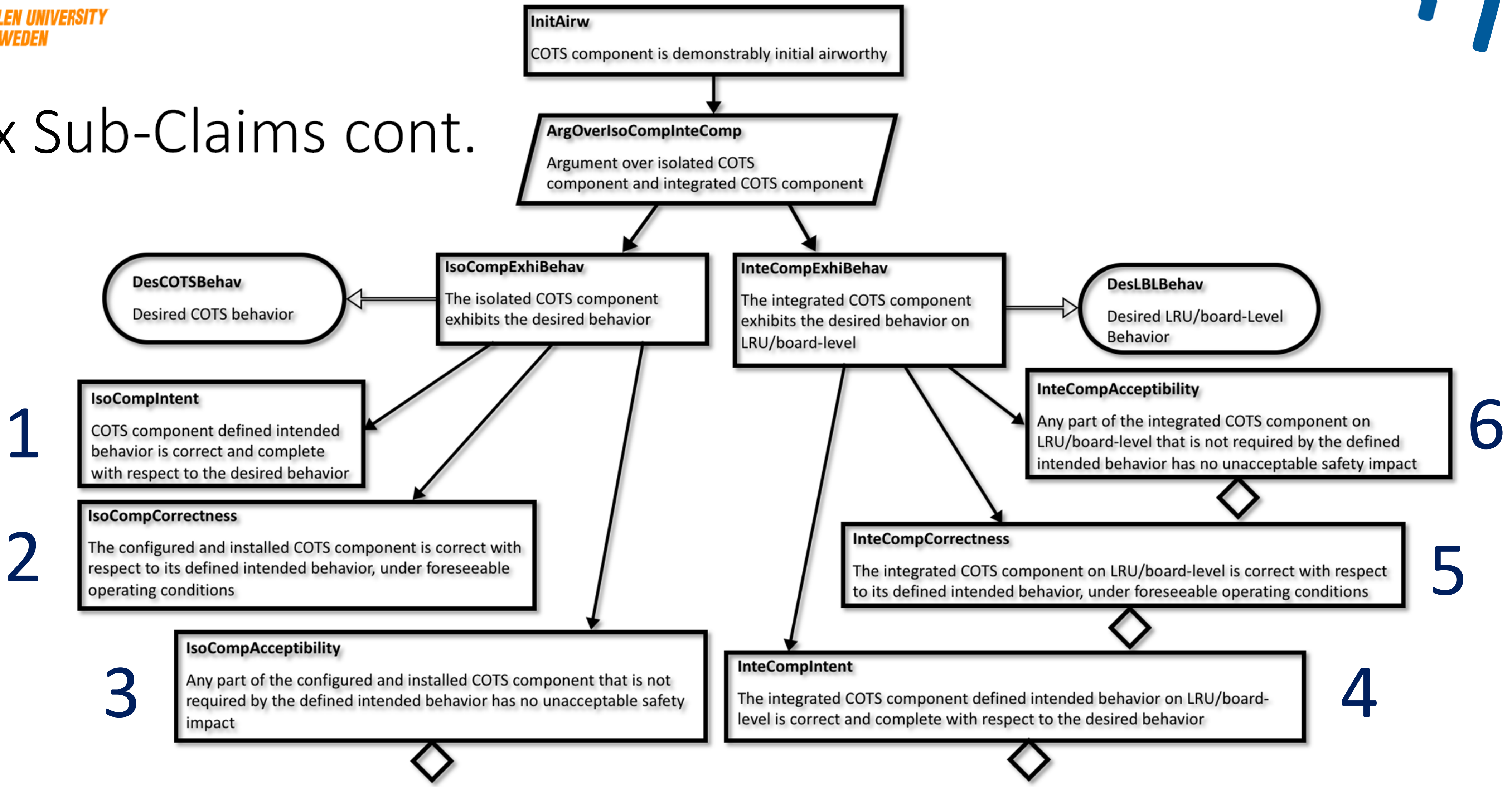
4. The integrated COTS **Intended** behavior on LRU/Board Level is correct and complete
5. The integrated COTS **Correct** behavior
6. The integrated COTS **Acceptable** behavior

Informal meaning of FAA's overarching properties

- **Intent:** "What the product is supposed to do is properly captured."
- **Correctness:** "The product does what it is supposed to do."
- **Acceptability:** "The product does not cause harm", including undefined intended behavior

MÄLARDALEN UNIVERSITY
SWEDEN

Six Sub-Claims cont.



InitAirw

COTS component is demonstrably initial airworthy

ArgOverIsoCompInteComp

Argument over isolated COTS component and integrated COTS component

IsoCompExhiBehav

The isolated COTS component exhibits the desired behavior

DesCOTSBehav

Desired COTS behavior

InteCompExhiBehav

The integrated COTS component exhibits the desired behavior on LRU/board-level

DesLBLBehav

Desired LRU/board-Level Behavior

1 **IsoCompIntent**

COTS component defined intended behavior is correct and complete with respect to the desired behavior

2 **IsoCompCorrectness**

The configured and installed COTS component is correct with respect to its defined intended behavior, under foreseeable operating conditions

3 **IsoCompAcceptibility**

Any part of the configured and installed COTS component that is not required by the defined intended behavior has no unacceptable safety impact

4 **InteCompIntent**

The integrated COTS component defined intended behavior on LRU/board-level is correct and complete with respect to the desired behavior

5 **InteCompCorrectness**

The integrated COTS component on LRU/board-level is correct with respect to its defined intended behavior, under foreseeable operating conditions

6 **InteCompAcceptibility**

Any part of the integrated COTS component on LRU/board-level that is not required by the defined intended behavior has no unacceptable safety impact

If 6 Sub-Claims are Enough …

- Then the objectives in the latest guidance from the authorities should cover all six areas

COTS objective	Relevant level and Overarching Property
COTS-1 – assessment of complexity	Isolated - Intent
COTS-2 – electronic component management process	Isolated - Correctness
COTS-3 – usage outside manufacturer's specification	Isolated - Correctness
COTS-4 – non-qualified microcode	Integrated - Correctness
COTS-5 – assessment of errata	Isolated - Acceptability
COTS-6 – failure modes and common modes	Isolated - Acceptability & Integrated - Acceptability
COTS-7 -intended function of COTS device including interfaces	Integrated - Intent
COTS-8 – inadvertent alteration of critical configurations settings	Isolated - Intent

Our Framework to Integrate COTS Assurance Objectives

- Is a five step process
  1. Choose the level on which the assurance objective has to be demonstrated
  2. Assign the assurance objective to the relevant OP
  3. Reformulate it to a conclusion
  4. Demonstrate its satisfaction in the primary argument
  5. Explain in the confidence argument how you reduce the uncertainty in the primary argument

We split Each Sub-Claim into a **Primary** and a **Confidence** Argument

Example from COTS Based Machine Learning

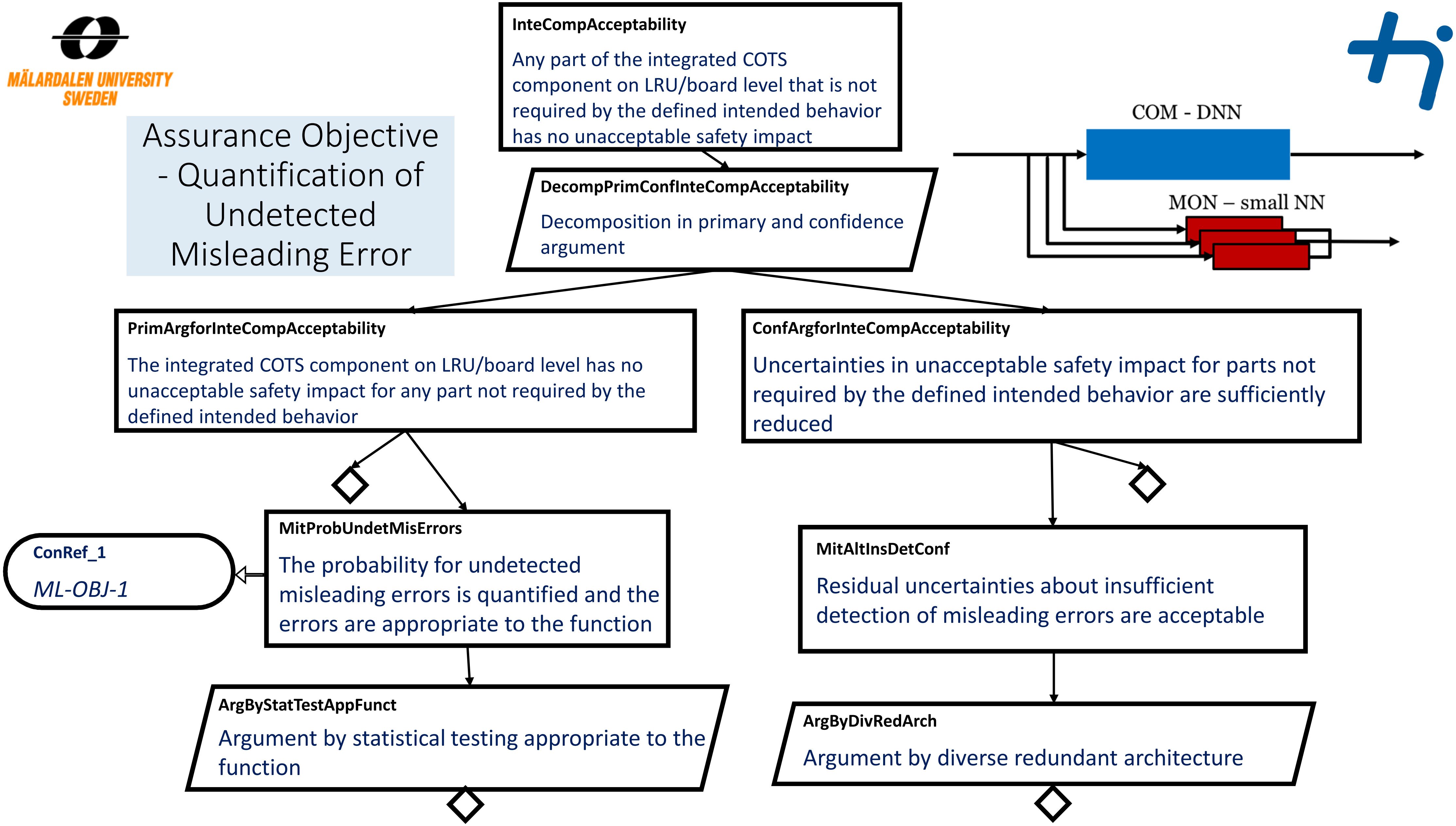
- Assume that at least the following four objectives are necessary for a COTS based Machine Learning system

  - The computing algorithm used is static when deployed, i.e. no dynamic (self-adaptive) algorithms should be used
  - The computation should maintain integrity, i.e. using the same input data twice should show identical results (unless altered by physical phenomena, which must be detected);
  - It should be possible to demonstrate success via statistical simulation to some percent at a system level; and
  - It should be possible to quantify the probability of an undetected, misleading error and show that the error is appropriate to the function

Put the Objective into our Framework

- The five steps
  1. The objective has to be treated on integrated COTS level since undetected misleading errors cannot be captured on isolated COTS level
  2. The assigned OP is acceptability since it deals with undetected misleading errors
  3. Reformulate to a conclusion: *The probability for undetected misleading errors is quantified and the errors are appropriate to the function*
  4. Demonstrate its satisfaction in the primary argument – see next slide ->
  5. Explain in the confidence argument how you reduce the uncertainty in the primary argument – see next slide ->

Assurance Objective - Quantification of Undetected Misleading Error



InteCompAcceptability

Any part of the integrated COTS component on LRU/board level that is not required by the defined intended behavior has no unacceptable safety impact

DecompPrimConfInteCompAcceptability

Decomposition in primary and confidence argument

PrimArgforInteCompAcceptability

The integrated COTS component on LRU/board level has no unacceptable safety impact for any part not required by the defined intended behavior

ConfArgforInteCompAcceptability

Uncertainties in unacceptable safety impact for parts not required by the defined intended behavior are sufficiently reduced

ConRef_1

ML-OBJ-1

MitProbUndetMisErrors

The probability for undetected misleading errors is quantified and the errors are appropriate to the function

MitAltInsDetConf

Residual uncertainties about insufficient detection of misleading errors are acceptable

ArgByStatTestAppFunct

Argument by statistical testing appropriate to the function

ArgByDivRedArch

Argument by diverse redundant architecture

MÄLARDALEN UNIVERSITY SWEDEN

Discussions

- Why is not the new certification guidance* sufficient for new technology?
  - Because new COTS technology may implement behavior which cannot be assured using existing guidance

- Why didn’t you modulate objectives with design assurance levels (DALs)?
  - That would be great!
  - But the association of DALs to certain assurance activities is often debatable and a very subjective task that should be agreed with the certification authority

*EASA, Notice of Proposed Amendment 2018-09, “Regular update of AMC-20:AMC 20-152 on Airborne Electronic Hardware and AMC 20-189 on Management of Open Problem Reports,” TE.RPRO.00034-006.

Conclusions

- We have via examples shown that COTS specific assurance objectives can be dealt with through assurance cases using Overarching Properties
- Through our framework consisting of five process steps, the applicant will have flexibility to adapt the assurance
- We believe that our results are a way forward to address the assurance of future COTS-based computer platforms