# Properties of evidence and of evidence generation

**Odd Ivar Haugen**

09 October 2018

# Disclaimer

- The content of the paper and this presentation is my personal view, as seen from a scientific perspective, it does not necessarily represent the views held or expressed by DNV GL as a company or as a classification society.

# Inspiration/Background

- During a discussing concerning failure of thruster in a simulated test environment, someone may states that:
  - "There is no need to test thrusters, we have already done it in the FMEA proving trial."

- When discussing the possible consequence of a single failure, someone may state that:
  - "We need to increase the verification"

- Questions:
  - Is it always a valid statement that something has been **tested** (and therefore implicitly state that we don't have to do it again, because it is redundant)?
  - What do we really mean by **increased** verification?

# Aspects of verification

# The objective of verification and assurance

- One definition verification: “The process of providing **objective evidence**…”
- Assurance: “… ground for **justified confidence**…”
- We generate evidence through **reviews, analysis, inspections, testing**…

# Different kinds of verification (and evidence)

- Product verification
  - Generates **primary** evidence
- Process verification
  - Generates **circumstantial** evidence
- Both types of evidence contributes in creating confidence in the system

# Primary evidence (product verification)

- Directly linked to the **behaviour of the system**
- Test items:
  - actual system
  - some representation of it, such as
    - design documents
    - source code
    - digital models (virtual system)

# Types of testing generating primary evidence

- White-box testing (or glass-box)
  - Tester **have access** to the internal workings of the test item
- Black-box
  - Tester do **not have access** to the internal workings of the test item

- Static testing
  - document reviews
  - source code review
- Dynamic testing (testing the running system)
  - FAT
  - seatrial
  - simulator-based testing

# Circumstantial evidence (process verification)

- Needs inference to draw conclusion about facts
- Reviews of development processes
- Reviews of artefacts showing details about how the process was conducted
- Artefacts showing conformance to standards or procedures

# Roles within the verification effort

- Verification Organization (VO)
  - Generates primary evidence
  - To quality as a VO:
    - conduct own analysis
    - specify and create test products (e.g. test plans)
    - perform the test activity
    - preferably own tools
    - follow up findings
- Assessor
  - Asses primary evidence
  - Generates circumstantial evidence
- Test Witness
  - Often part of an assessor's role
  - Assess the test activity
- Stakeholders tend to change roles during a project
- Class are
  - VO early in the project (static testing)
  - Assessor and Test witness later (FAT, seatrial)
- Supplier
  - VO during FAT and seatrial
- FMEA company
  - VO

# Aspects of the verification effort

- Intensity
  - Scope across normal and abnormal system condition
  - Number of
    - test data dimensions
    - test items
    - development phases where verification is performed
- Rigour
  - Level of **formalism** of the methods, techniques, and documentation used in the testing
- Detachment
  - Level of independence of the VO (from the developer)
  - Goal: Increase the "distance" in terms of:
    - mental
    - organizational
    - financial
    - procedural
    - technological

  between the VO and the developer.

  Why?

  to **minimize** the possibility of **cognitive and societal biases** that may **mask defects**

## The position of algorithms in the verification effort:

# Algorithm-based Verification Agent (AVA)

# What is an Algorithm-based Verification Agent (AVA)?

- Have the position of a verification practitioner
- Generates evidence, or being instrumental in this process
  - Condition Monitoring system
  - Automatic test case generation
  - Generating artificial test data for machine learning algorithms
- May be based on AI
- Enabled through the use of sensors and data science

# Why Algorithm-based Verification Agent (AVA)

- (DP) Systems is a complex software-intensive system
- A lot of interconnections and dependencies between components and other sub-systems
- Vast number of possible scenarios that may lead to loss of position
- Autonomous navigation based on AI
- Remote controlled vessel
- Cost of man-hours
- Access to asset
- Assurance is moving from date-based towards condition-based

# What is challenging?

- Is the evidence generated by the AVA trustworthy?
- Can the same biases in the DP system also be implemented in the e.g. condition monitoring system, masking defects?
- They may be based on machine learning
  - Given the test results (evidence), the conclusion may not be human comprehendible – just have to "trust" it
- May lead to unclear authority between operator and the algorithm
  - "I don't know, but the algorithm say so"
- May lead to unclear authority between human tester and algorithm
- May disguise lack of independence in the generating of evidence

# New type of evidence

- Current:
  - **Primary** evidence from system verification
  - **Circumstantial** evidence from development/change process verification
- New
  - **Indirect primary** evidence from verifying AVA

- What can we infer about the system from **Indirect** primary evidence?

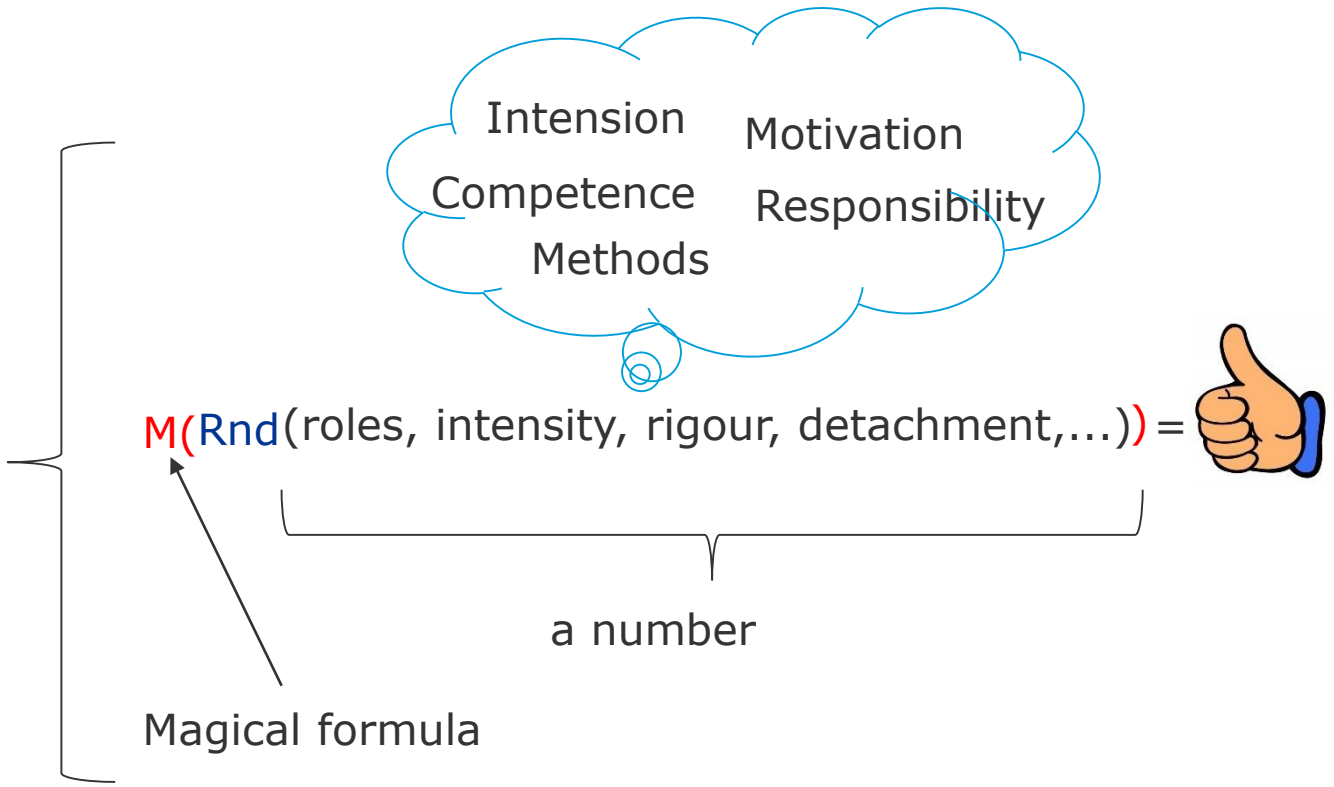
# Properties of evidence and of evidence generation

# Properties of evidence and of evidence generation

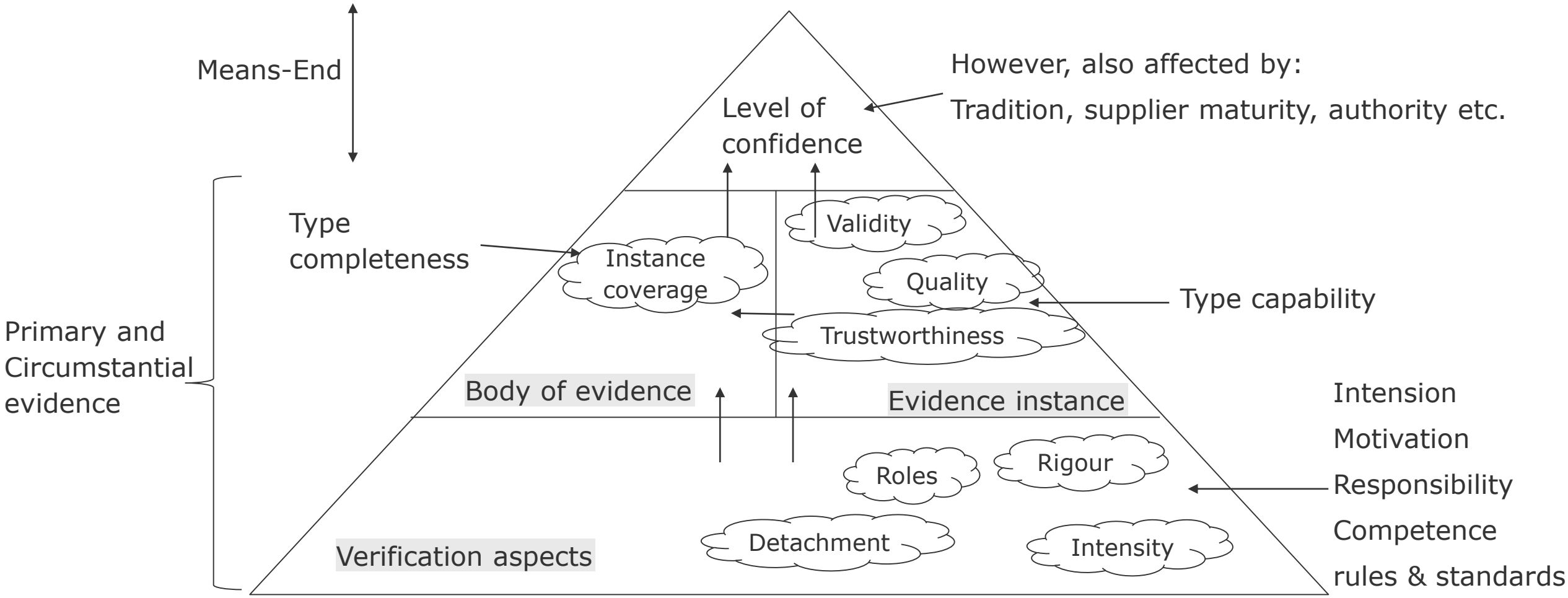
- evidence **type capability**
  - document review will identify design defects early so that they can be fixed before the vessel is built at a lowest possible cost, however, it cannot show implementation errors
- evidence **instance quality**
  - test cases may lack necessary descriptions to make the test result *repeatable*
  - document review may not follow a prescribed procedure, resulting in some aspects not being assessed
- evidence **instance trustworthiness**
  - Lack of *objectivity* in the verification effort
- evidence **instance validity**
  - test activity may not be conducted on the correct version of the software, or hardware
  - data of which the evidence is based upon, perhaps in the context of an AVA, may be corrupted
- **body** of evidence **type completeness**
  - identify the needed verification intensity, and dedicate evidence types, with adequate capability, to the different parts of the scope
- **body** of evidence **instance coverage (and depth)**
  - evidence *instance* is not completely determined by the evidence *type*
  - depends on the *quality and needed depth*

# Applying the "magical" formula

- evidence **type capability**
- evidence **instance quality**
- evidence **instance trustworthiness**
- evidence **instance validity**
- **body** of evidence **type completeness**
- **body** of evidence **instance coverage (and depth)**



# (Mental) model of the "Miracle formula"



# Inspiration/Background

- Questions:
  - Is it always a valid statement that something has been **tested** (and therefore implicitly state that we don't have to do it again, because it is redundant)?
  - What do we really mean by **increased** verification?

**Odd Ivar Haugen**
odd.ivar.Haugen@dnvgl.com
+4791715040

**www.dnvgl.com**

**SAFER, SMARTER, GREENER**