Approaches to Safety Assurance

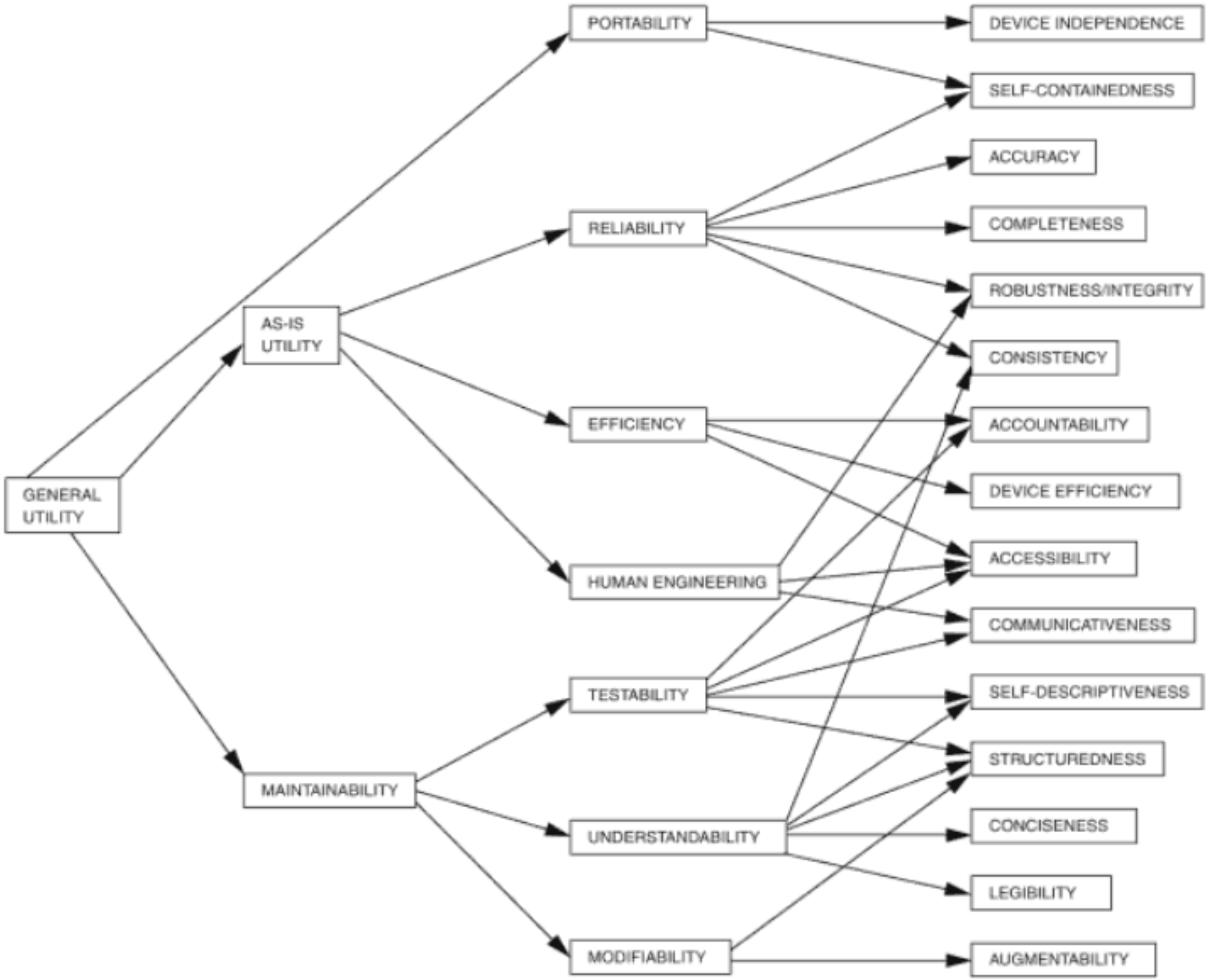
- Three main approaches
  - Process-oriented – looking at processes and people expertise
  - (Using quality models)
  - Using safety cases
- These complement each other, but their different character, if misunderstood, could lead to making unjustified assertions

An Example of Fallacious Reasoning

- If I have all necessary processes in place, and the right people on the job, that guarantees safety
  - Consider following a cake recipe – does that guarantee a perfect cake?
  - Leads to increased level of confidence, human expertise could further improve that (consider a master chef following the recipe, versus a regular person)
  - A product perspective is necessary to establish safety (see papers from Tom, Mark and Alan☺, etc.)

Quality Models

- Hierarchy linking product quality to its influencing product characteristics
- Further broken down into sub-characteristics, until measurable
- Some models are customizable (consider ISO/IEC 9126), in order to best fit the product domain and specific user expectations
- Customization is in terms of both structure and parameters
- Any customization needs to be recorded and justified in the accompanying product documentation



Metrics

Quality model: Boehm (Selby, 2007)

Quality Standards and Safety

- What is the relationship between quality models, quality standards (like SQuaRE) and assurance cases?
- Answer:
  - A quality model "is" a measurement framework, like IS for physical sciences
  - Existing quality models are very poor substitutes for proper measurement frameworks (so standards are commensurately bad)
  - Intuition is not a proper basis for engineering
  - Even a "proper" quality model (or corresponding standard) is *absolutely not* an assurance case for anything, including quality!

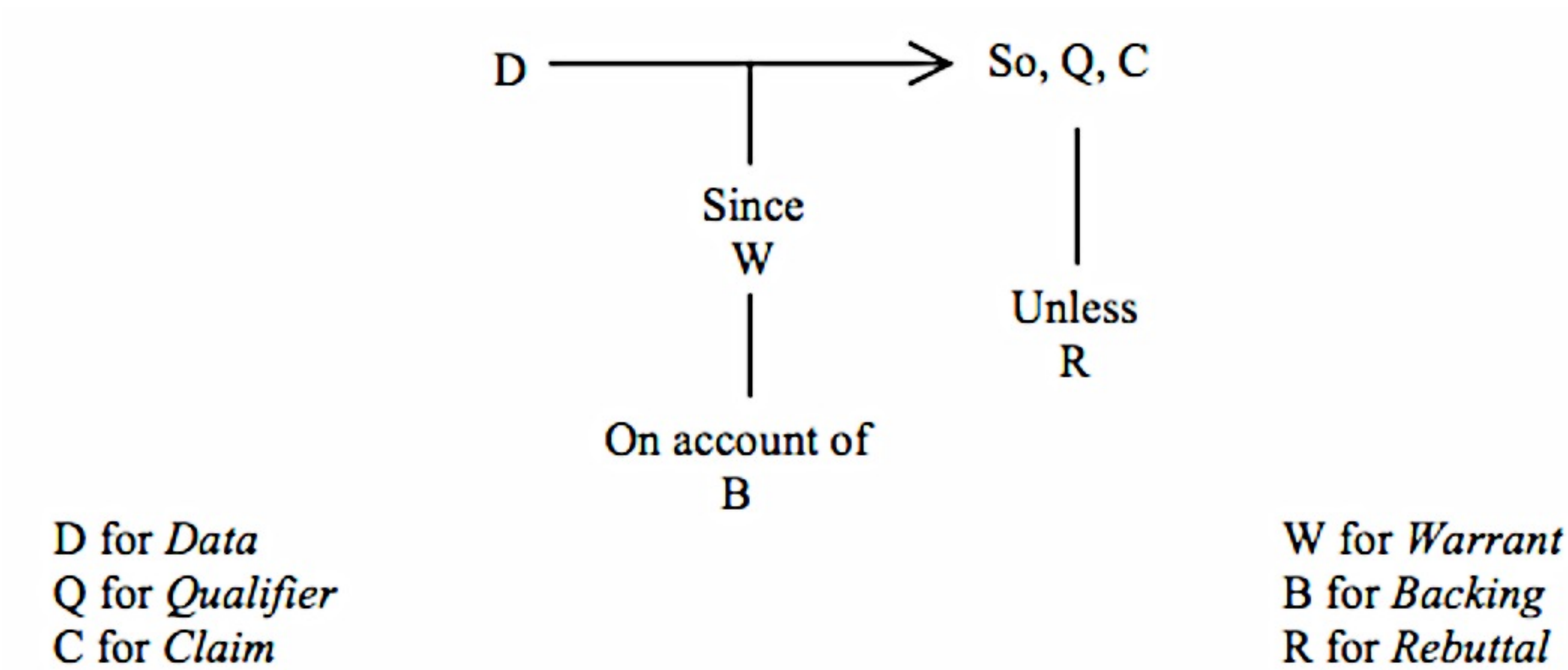
Quality Model Customization

- Solving managerial, technological, scientific problems in modern society almost always requires *explicit justification*
- What is the best way to document customization decisions related to quality assurance? Answer: as arguments
  - The justification of the quality model customization represents part of the reasoning, which needs to be included in the associated documentation
  - Proper encoding facilitates the identification of the premises and inferences underlying the decisions made
  - This further helps to uncover potential rebuttals/ defeaters, and to address them accordingly

How Best to Encode an Argument?

- Quality arguments are defeasible in nature
  - New evidence could potentially invalidate previously true assumptions and claims
- The argument scheme suggested by Toulmin could serve to model this
- This would make it possible to challenge the assumptions and inferences underlying the customization of the model in a more systematic way
- Therefore, supplementing the quality model with an explicit argument makes the task of demonstrating product quality more amenable to review, and provides a more comprehensive demonstration of product quality

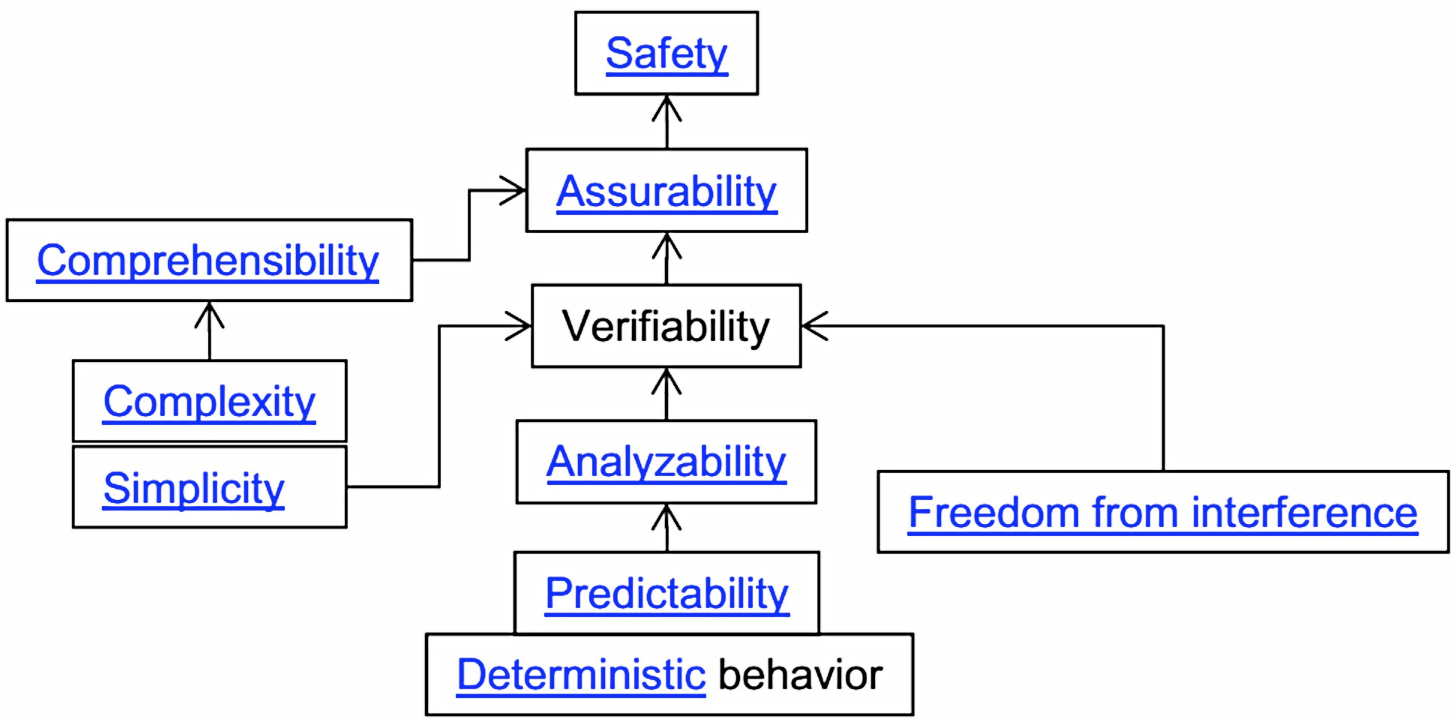
Toulmin's Argument Scheme



Quality Models and Assurance Cases

- Quality models do not provide an explicit argument for their validity (while assurance cases are meant to do so)
- Adding an explicit argument, justifying the structure and parameters of the quality model would effectively transform it into a quality case
- The task is not straightforward, but as with quality model structure, templates for argument patterns could be identified and reused
- Explicitly encoding the argument and reasoning accompanying the quality assurance process makes it possible to associate a more rigorous measure of confidence with the conclusions
- This facilitates the review of the quality case and the identification of the areas characterized by greatest uncertainty

Quality Characteristics to Support Safety (RIL 1101)



Another Example of Fallacious Reasoning

- These characteristics indeed support safety, but do not ensure it
- Being able to assure safety is different from actually assuring safety
- Furthermore, as a global property, safety is concerned with system-level context and assumptions, which are not necessarily reflected in the quality model
- Our suggestion - have at the top of the hierarchy "Safety demonstrability" to avoid misunderstanding
- **!!!** "…beware of -ilities" – Carnap **!!!**

Measurement

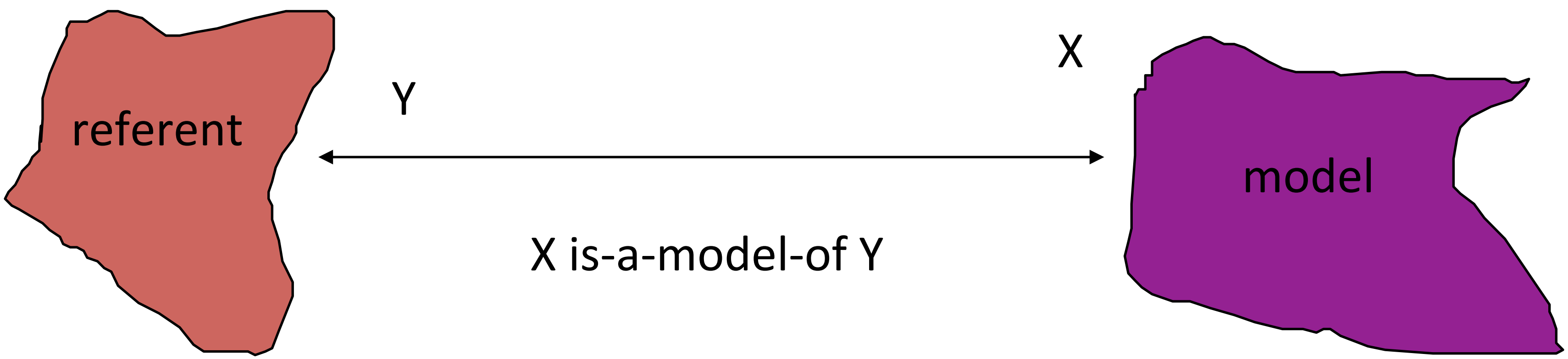
- Both quality models and assurance cases are hierarchies, with measurable system "attributes" at the leaves
- A proper measurement framework is needed for any rigorous analysis
  - Scientific results and engineering achievements can only be judged on the basis of evidence
  - Convincing evidence can only be provided by *measurement*
  - "Measurement is the key to all disciplines of science and technology, and the maturity of the discipline is marked by the extent to which it is supported by a sound and comprehensive system of *measures*, *measurement standards*, *measurement tools* and *measuring procedures*."
- Measurement is the basis of expressing values and forming judgements

What is Measurement?

- Purpose of measurement is to provide a valid, trustworthy, traceable representation of some chosen *entity* whose selected *attributes* are of interest
- Measures *may be* (obviously!) quantitative (but data gathering and casual assignment of numbers to things do not constitute measurement)
- Some very important measures may be non-numerical
  - blood types
  - correctness of SW
  - alarm conditions
  - quality level

Referents, Attributes and Properties

- The basis of science and engineering is the construction of *models*.
- *Modelling* is essential for measurement: the purpose of modelling is to delimit the aspects (or parts) of the *referent* considered to be of interest.
- For our purposes, a model is a kind of *representation*:



Measures

- A *measure* is a particular value of a *property variable* (used to model an *attribute*).
- **To characterise a referent, a measure must be assigned to each property which corresponds to its (objective or subjective) attributes.**
- Measures may be:
  - QUANTITATIVE: use *symbol systems* which are complex
  - QUALITATIVE: use *symbol systems* which are small discrete domains
- A *direct* measure is one which may be determined by direct observation (e.g., number of lines of code).
- An *indirect* measure is one which is derived in some formal manner from other measures (e.g., fault density).

Measures cont.

UTILITY MEASURES

- The ultimate aim of measurement is to assist choice and to support decision making.
- Choice is always subjective.
- Rational, *informed* choice in science, technology or business relies on fact (and should not be random or capricious).

PROFESSIONAL ACCOUNTABILITY requires that the factual basis of the choice should be defined, the value system be explicit and the decision repeatable.

Utility Measures

- One must construct an explicit model of the subjective attribute on which the judgement is made.
- The *utility property* is given as a function of the directly or indirectly measurable objective properties of the referent.
- The *arguments* of the function are measures of objective attributes, reflecting 'facts'.
- The *form* of the function is subjectively determined by the problem solver, reflecting judgement.
- The *value* of the function, the *utility measure*, is subjective, but is explicitly defined, its further use objective.

Some Laws of Measurement Theory

- REPRESENTATION CONDITION

  A set of measures is a valid *representation* of a referent with respect to a given attribute if the mapping from the empirical domain of attributes to the formal domain of measures is a homomorphism.

- UNIQUENESS AND SCALING:

  The scale (i.e., symbol system) chosen must either be unique or the truth value of a statement must remain invariant under all admissible transformations. (So the measurement scale adopted is in general not unique for the purpose at hand.)

Characterising Measures

- A measurement statement is said to be *meaningful* if its truth value is invariant under all admissible transformations.
  - So, is the following meaningful: The temperature in Washington today is twice the temperature in Toronto.
- Classical scales: nominal, ordinal, interval, ratio, absolute
  - There are multiple scales appropriate for the measurement of quality and safety attributes
  - It might be beneficial to associate tuples (of potentially heterogeneous values) with quality or safety, instead of single values, based on the modeling approach

How to Approach Measuring Safety?

- Define a model of safety suitable for your purposes
- Define a measurement framework for it
  - Consider all potential sources of evidence and their comparative relevance
  - Establish all relevant base measures and derived measures (some using utility functions), and assign appropriate measurement scales
  - Define appropriate measurement procedures for base attributes, utility functions for (some) derived attributes
  - Validate model empirically, checking satisfaction of measurement laws
  - Adjust in light of experience with framework, identification of new sources of evidence
- Train engineers in use of measurement framework

Conclusion

- To wrap things up - the best way to assure safety is a combination of the approaches:
  - Ensure that the processes are in place and implemented by experienced personnel
  - Safety assurability should be built into the system
  - Most importantly, use an explicit safety case to document all safety practices and reasoning, thus making it easier to conduct reviews and uncover problematic areas
- Applying a proper measurement framework is vital for associating values with system safety, as well as for establishing the level of confidence to be associated with these values
- Questions and comments are welcome!

References

- ISO/IEC. (2001). ISO/IEC 9126-1: Software Engineering-Product quality-Part 1: Quality model. Geneva, Switzerland: International Organization for Standardization.
- Selby, R. W. (Ed.). (2007). *Software Engineering: Barry W. Boehm's Lifetime Contributions to Software Development, Management, and Research*, IEEE CS Press-John Wiley &Sons.
- ISO/IEC. (2011). ISO/IEC 25010: Systems and software engineering-Systems and software Quality Requirements and Evaluation (SQuaRE)-System and software quality models. Geneva, Switzerland: International Organization for Standardization.
- Toulmin, S. E.. (1958). *The Uses of Argument*, Cambridge University Press.
- The Office of Nuclear Regulatory Research. (2014). Research Information Letter (RIL) 1101: Technical Basis to Review Hazard Analysis of Digital Safety Systems.