Dependability Assurance Challenges Posed by 21st Century Trends

John F. Meyer
jfm@umich.edu

84th Meeting of IFIP WG 10.4
Arcos de Valdevez, Portugal
June 23-26, 2023

IFIP WG 10.4

Computer Science and Engineering
The University of Michigan

Dependability Assurance

Dependability Assurance

- Any methodical process of determining whether a system meets specified dependability requirements
  - for a given application and operating environment
  - under assumed fault assumptions

Dependability Assurance

- Any methodical process of determining whether a system meets specified dependability requirements
  - for a given application and operating environment
  - under assumed fault assumptions
- Can take place at various phases and levels of system development

Dependability Assurance

- Any methodical process of determining whether a system meets specified dependability requirements
  - for a given application and operating environment
  - under assumed fault assumptions
- Can take place at various phases and levels of system development
- Dependability requirements can be expressed
  - qualitatively or quantitatively
  - in terms of various measures depending on phase and level

Dependability Assurance

- Any methodical process of determining whether a system meets specified dependability requirements
  - for a given application and operating environment
  - under assumed fault assumptions
- Can take place at various phases and levels of system development
- Dependability requirements can be expressed
  - qualitatively or quantitatively
  - in terms of various measures depending on phase and level
- Can employ a variety of techniques
  - model-based (formal methods, analysis, simulation)
  - testing (I/O, fault injection, field testing, etc.)
  - reasoning (e.g., safety cases)

21st Century Trends

21st Century Trends

- There are a number of trends that pose serious challenges wrt certain aspects of dependability assurance

21st Century Trends

- There are a number of trends that pose serious challenges wrt certain aspects of dependability assurance
- Would like to focus on two trends which relate closely to
  - longtime interests in model-based evaluation of system dependability/performability
  - recent involvement in WG 10.4's IVDS Project

21st Century Trends

- There are a number of trends that pose serious challenges wrt certain aspects of dependability assurance
- Would like to focus on two trends which relate closely to
  - longtime interests in model-based evaluation of system dependability/performability
  - recent involvement in WG 10.4's IVDS Project

1) System applications with increasingly large and complex operating environments

21st Century Trends

- There are a number of trends that pose serious challenges wrt certain aspects of dependability assurance
- Would like to focus on two trends which relate closely to
  - longtime interests in model-based evaluation of system dependability/performability
  - recent involvement in WG 10.4's IVDS Project

1) System applications with increasingly large and complex operating environments
2) Employment of AI (e.g., ML, DL) algorithms for which the key dependability concepts of *correct service* and *failure* (deviation from correct) are elusive if not nonexistent

Assurance Challenges Posed by Large, Complex Environments

Assurance Challenges Posed by Large, Complex Environments

- Consider the operating environment of an intelligent autonomous vehicle
  - road type, time of day, other vehicles, pedestrians, road signs, traffic volumes, weather and visibility conditions, etc.

Assurance Challenges Posed by Large, Complex Environments

- Consider the operating environment of an intelligent autonomous vehicle
  - road type, time of day, other vehicles, pedestrians, road signs, traffic volumes, weather and visibility conditions, etc.
- Test driving in actual environments not sufficient
  - assuming an average vehicle speed of 40 mph, to satisfy a safety requirement of $\leq 5 \times 10^{-8}$ fatalities/hr with 90% confidence requires ~1.842 billion miles of fatality-free driving [Kleyner 2014; Karla, Paddock 2016]

Assurance Challenges Posed by Large, Complex Environments

- Consider the operating environment of an intelligent autonomous vehicle
  - road type, time of day, other vehicles, pedestrians, road signs, traffic volumes, weather and visibility conditions, etc.
- Test driving in actual environments not sufficient
  - assuming an average vehicle speed of 40 mph, to satisfy a safety requirement of $\leq 5 \times 10^{-8}$ fatalities/hr with 90% confidence requires ~1.842 billion miles of fatality-free driving [Kleyner 2014; Karla, Paddock 2016]
- **Challenges**
  - Construct comprehensive environment models (EMs) that combine analytical, simulation and AI models to conservatively represent reality
  - Devise means of determining an EM's approximation to the real world
  - Incorporate such EMs in integrated methodologies for assuring that specified dependability requirements are satisfied for the target system

Assurance Challenges Posed by AI

Assurance Challenges Posed by AI

- Dependability issues associated with AI, per se, and AI-enabled systems have been a concern of our community for the past decade, as evidenced by
  - several DSN and 10.4 workshops
  - a recent lengthy 10.4 email thread, chronicled by Brian last March

Assurance Challenges Posed by AI

- Dependability issues associated with AI, per se, and AI-enabled systems have been a concern of our community for the past decade, as evidenced by
  - several DSN and 10.4 workshops
  - a recent lengthy 10.4 email thread, chronicled by Brian last March
- **Conundrum:** Without a specification of correct service, how to decide whether an AI system has failed

Assurance Challenges Posed by AI

- Dependability issues associated with AI, per se, and AI-enabled systems have been a concern of our community for the past decade, as evidenced by
  - several DSN and 10.4 workshops
  - a recent lengthy 10.4 email thread, chronicled by Brian last March
- **Conundrum:** Without a specification of correct service, how to decide whether an AI system has failed
- **Challenges**
  - For AI-enabled systems with usual application-oriented service requirements, determine means of inferring possible AI contributions to system failures
  - For AI systems in isolation, investigate use of evaluation measures that do not require a notion of failure and yet can quantify the extent of errant AI behavior (performability, uncertainty,?)