AI and Dependability in Computing Systems: Friend or Foe?

Saurabh Bagchi
Purdue University
School of Electrical and Computer Engineering
Department of Computer Science
Director, NSF Center CHORUS
Director, ARL Assured Autonomy Innovation Institute (A2I2)

1

Roadmap

- **Dependability across the stack**
  - Definition
  - Trends
  - Conceptualization
- AI in Reliability
  - Foe
  - Friend
  - Our Work
- AI in Security
  - Foe
  - Friend
  - Our Work
- Takeaways and the Road Forward

5

Key Takeaways and Future Directions

AI should become a friend for reliability and security, if

- Understand it **well enough** to identify weak spots and attack surfaces
- Design it to aid human cognition **for experts**
- Built a **fail-safe mentality** into models and their execution

Therefore, we should roll up our sleeves for