BIRD - ICRDE Project Extension:

RumRaisin on Chip

J. Sukarno Mertoguno

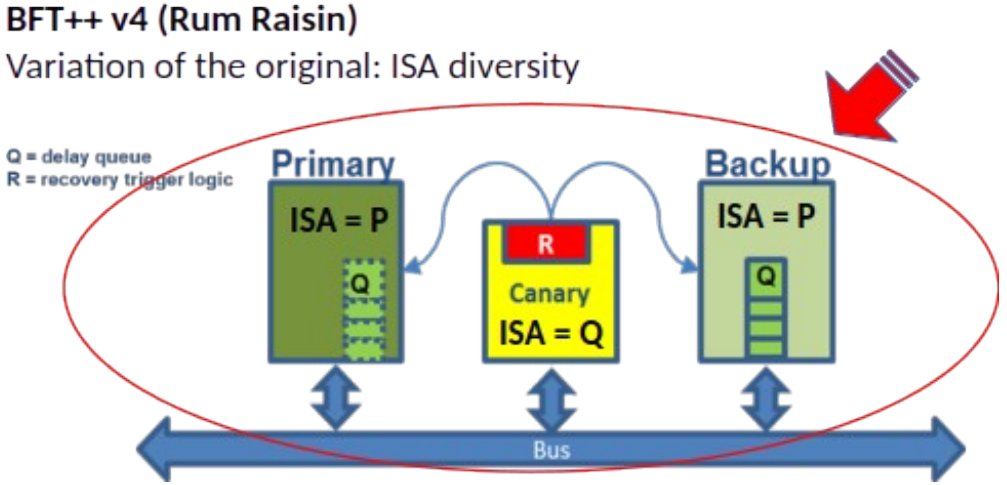
Georgia Tech College of Computing
School of Cybersecurity and Privacy

Problem Statement (motivation)

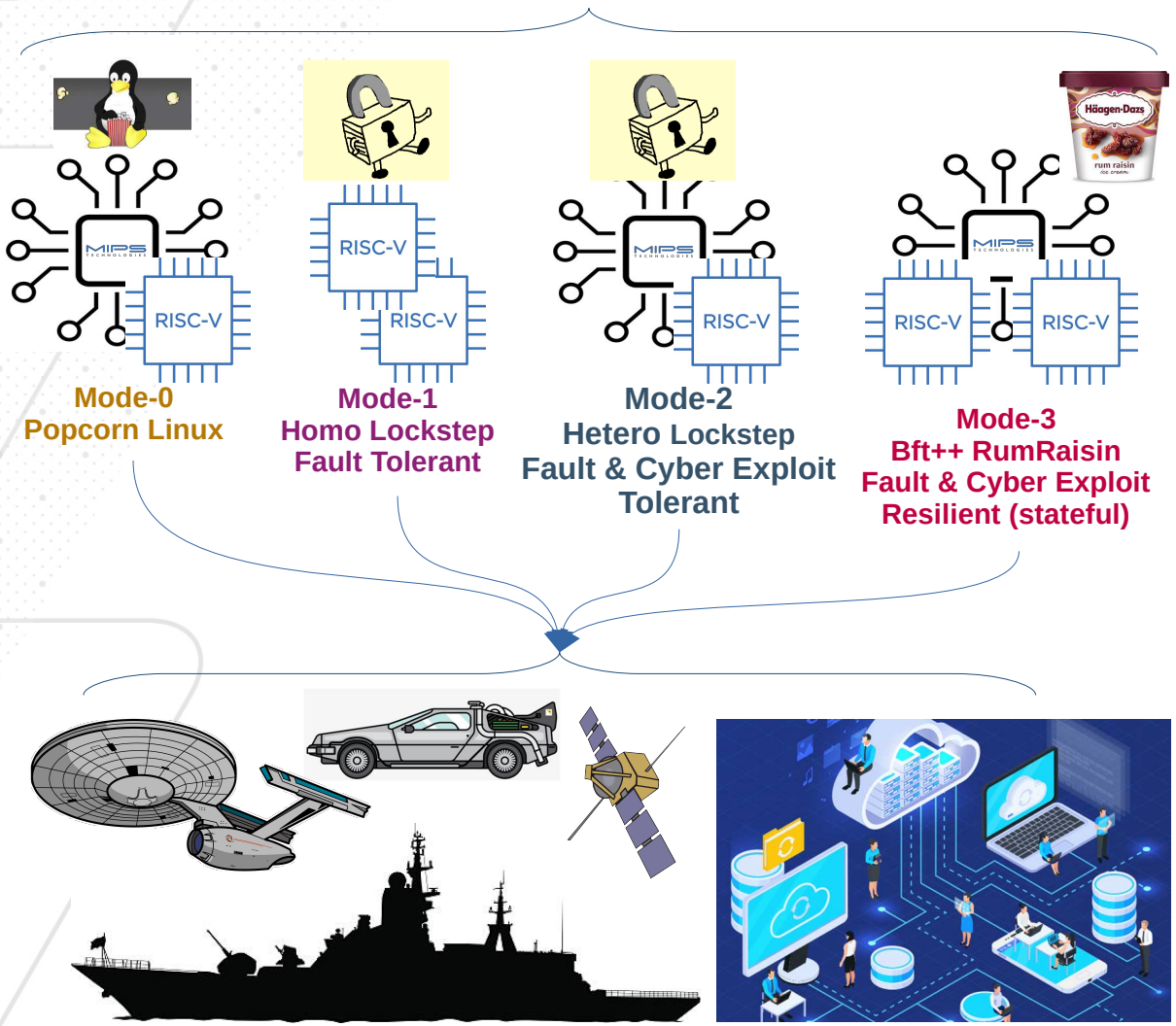
- Dual (homogeneous) Core Lockstep:
  - Highest security ASIL-D in automotive application standard ISO-26262
  - Resilient against Random failure → Fault Tolerant
- However, Dual Homogeneous Cores Lockstep:
  - Susceptible to Cyber-Exploits → Common mode failure
- What is needed is Dual Heterogeneous Cores Lockstep
  - Following the footstep of BFT++ family methods for cyber-attack tolerant
  - Dual Heterogeneous Cores Lockstep is both fault tolerant & cyber-exploit tolerant

Project Proposal (Solution to the problem)

- Develop a proof of concept for Hecocefta, supporting BFT++ v4 (Rum Raisin) on chip
- Employing 3 cores with 2 different instruction set architectures (ISAs); RISC-V and Xilinx's MicroBlaze (or opensource MIPS), 2 RISC-V and 1 MicroBlaze/MIPS
- Provides 4 software configurable modes:
  - Mode-0: simple 3 cores Multi-ISA (2 RISC-V & 1 MicroBlaze), for Popcorn Linux
  - Mode-1: 2 homogeneous core lockstep for ASIL-D (RISC-V)
  - Mode-2: 2 heterogeneous core lockstep for fault & cyber-exploit tolerant version of ASIL-D (RISC-V & MicroBlaze)
  - Mode-3: 3 cores Rum Raisin (BFT++ v4) fault & cyber-exploit tolerant with efficient stateful recovery (2 RISC-V & 1 MicroBlaze) .
  - More ?



Potential Application Areas

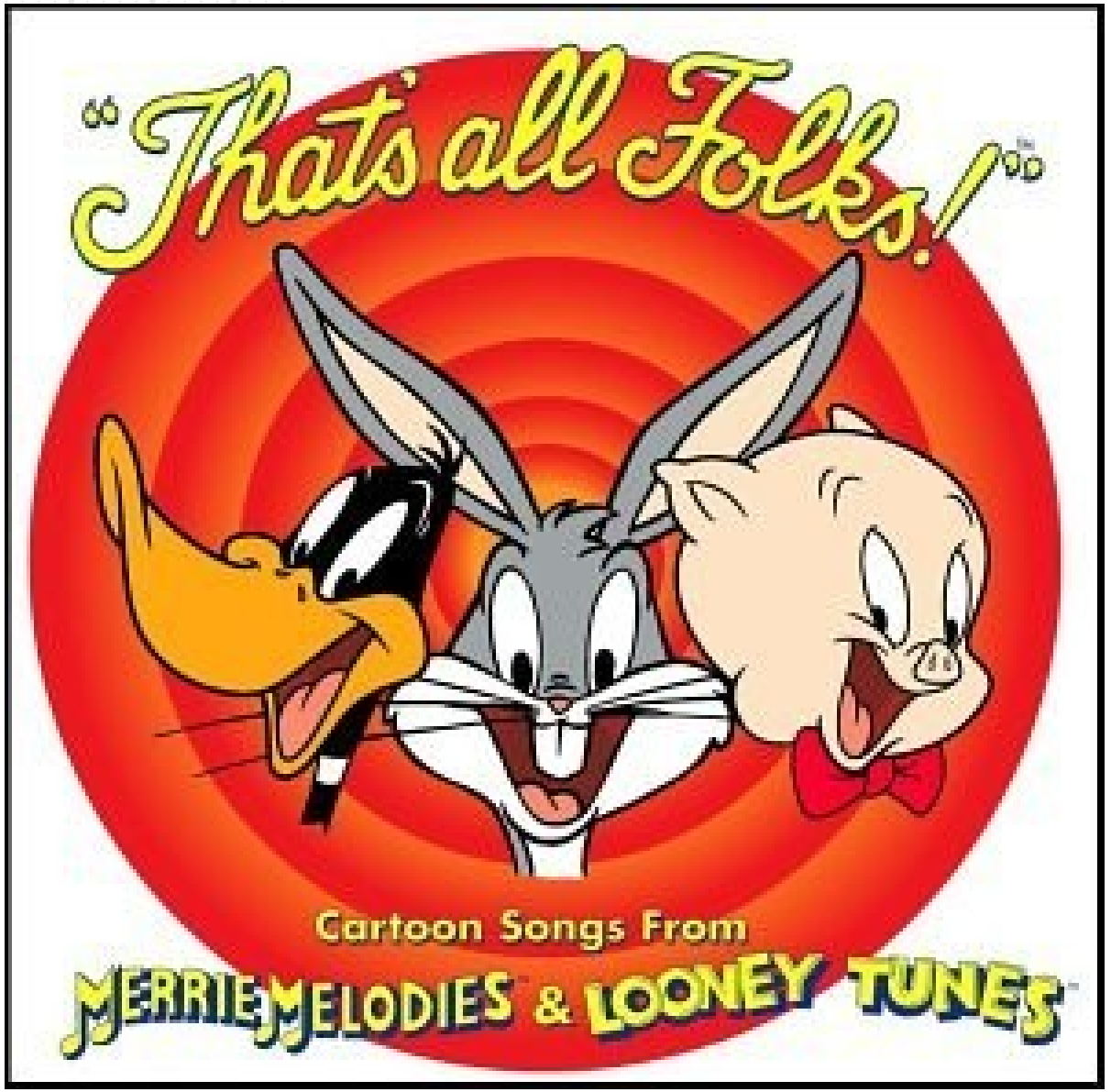


- Safety & security critical application and infrastructure where cyber-exploit is a concern
- Applicable to:
- Automotive & Vehicular
- Satellite & Space technologies
- Naval automation & Infrastructure
- Weapon systems
- General IT
- CPS & critical infrastructure
- Etc.

Georgia Tech College of Computing
School of Cybersecurity and Privacy

References

- 22V-xyz Model Year 2007-2014 MINI – (Hardtop 2 Door, Clubman) Footwell Control Module (FRM) Chronology 11 May 2023, https : / / static . nhtsa . gov / odi / rcl / 2023 / RMISC - 23V337 - 8958 . pdf
- Part 573 Safety Recall Report 22V-648, https://static.nhtsa.gov/odi/rcl/2022/RCLRPT- 22V648-1386.PDF
- J. S. Mertoguno, R. M. Craven, M. S. Mickelson, and D. P. Koller, “A physics-based strategy for cyber resilience of CPS,” in Autonomous Systems: Sensors, Processing, and Security for Vehicles and
- Infrastructure 2019, M. C. Dudzik and J. C. Ricklin, Eds., International Society for Optics and Photonics, vol. 11009, SPIE, 2019, 110090E. DOI: 10.1117/12.2517604. [Online]. Available: https://doi.org/10.1117/12.2517604.
- A. AlMaruf, L. Niu, A. Clark, J.S. Mertoguno, and R. Poovendran, 2023, A Timing-Based Framework for Designing Resilient Cyber-Physical Systems under Safety Constraint, J. ACM 37, 4, Article 111 (August 2023)



CPS → Physics Rules