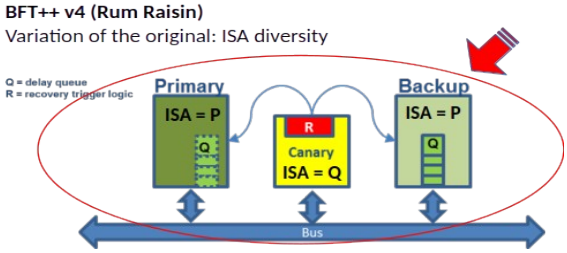
RumRaisin on Chip (RRoC)

J. S. Mertoguno, Georgia Institute of Technology

With the increasing prevalence of ``drive by wire", electronic systems like advanced driver-assistance systems (ADAS) and electronic control units (ECUs) are taking over more and more critical roles in the functionality and safety of modern day vehicles. Unfortunately, as highlighted in many real life events [1][2]. This trend also means increased safety risk from any malfunction in these components. In response, the ISO 26262 was proposed as a systematic approach for managing functional safety throughout the development lifecycle of automotive electrical and electronic systems. In particular, ISO 26262 defines the Automotive Safety Integrity Levels (ASIL) to combine the probability of exposure to hazard, the extent to which it is controllable by a driver, and the severity of failure to control such hazard. ASIL-D is the highest level of integrity defined under ISO 26262. In order to attain ASA standard approach for achieving ASIL-D is to have redundant hardware components operating on the same inputs and flag any discrepancy in their output as an error condition. A popular implementation of this idea is the dual-core lockstep configuration (DCLS), a system needs to satisfy a system requirement of having fewer than 1% single point of failure. Unfortunately, since ISO 26262 (and thus ASIL) only focuses on random, unintentional faults, existing ASIL-D compliant systems are unlikely to provide any defense against the much more dire threat from cyberattacks. This is because in the face of a cyberattack, all the redundant components will be processing the same malicious input, and thus reaching the same compromised state, which will be passed as normal by any fault tolerance mechanism (common ode failure).

In order to extend ASIL-D compliant systems to achieve any safety guarantee against cyberattacks, we need an approach that is i) scalable in both the class of attacks and the size of software that can be covered, ii) cheap to deploy in both hardware and performance cost, and iii) provides high safety, security and compatibility guarantee. The scalability requirement precludes fault avoidance methods that use formal methods to identify and remove all security problems in software. The stringent performance requirement precludes many software based security monitoring solutions (which can have >5% performance overhead).



BFT++ family of methods [3,4] can easily provides cyber-attack tolerance as well as fault tolerance. A variant of BFT++, called RumRaisin uses ISA diversity to defends against cyber-attack while providing fault tolerant. It will surpass ASIL-D requirement and provide additional safety of cyber-attack resilience with stateful program execution recovery (warm recovery). Rum Raisin uses 2 different processor instruction set architectures (ISAs), and configure them in BFT++ fashion, as such if one of the particular ISA core is attack, the other ISA core will crash, hence an attack is detected, and stateful recovery can immediately be initiated, using the delayed state of the backup core.

GaTech is proposing to develop a prototype of RRoC and evaluate its efficacy against faults and cyber-attacks. We will develop RRoC with three cores using two distinct instruction set architectures RISC-V and MIPS, on an FPGA. We will evaluate and demonstrate that RRoC is resilient against farious cyber-attacks as well as faults. While the development of RRoC was initially motivated by automotive safety & security, RRoC is largely applicable to general CPS applications with high safety and security requirements, including that of energy infrastructure.

References:

1. 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
2. Part 573 Safety Recall Report 22V-648, https://static.nhtsa.gov/odi/rcl/2022/RCLRPT-22V648-1386.PDF
3. 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.
4. 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)