DISTRIBUTION A. APPROVED FOR PUBLIC RELEASE; DISTRIBUTION UNLIMITED

U.S. ARMY RESEARCH, DEVELOPMENT AND ENGINEERING COMMAND

U.S. Army Ground Vehicle Applications for the seL4 Microkernel

Leonard Elliott

Electrical Engineer

Tank and Automotive Research, Development and Engineering Center

DISTRIBUTION A. APPROVED FOR PUBLIC RELEASE; DISTRIBUTION UNLIMITED
OPSEC #: 1721

CURRENT DOD WEAPON SYSTEM SECURITY

- Recent GAO report cites the need for improved cyber resilience across DoD weapon systems [1]
- Report does not mention specific platforms but refers to “combat vehicles”

United States Government Accountability Office

GAO

Report to the Committee on Armed Services, U.S. Senate

October 2018

WEAPON SYSTEMS CYBERSECURITY

DOD Just Beginning to Grapple with Scale of Vulnerabilities

GAO-19-128

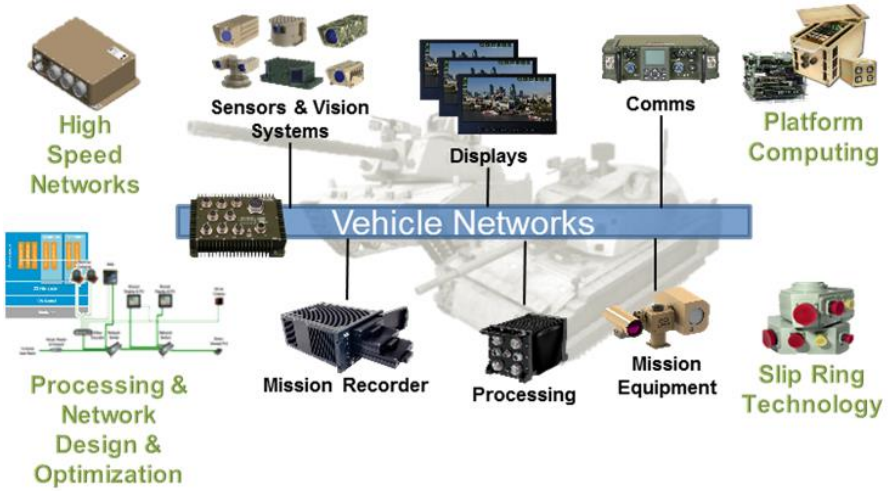
EMERGING CAPABILITIES NEED EVEN MORE SAFETY AND SECURITY

- Active Protection Systems

- Mobile Robotic Systems

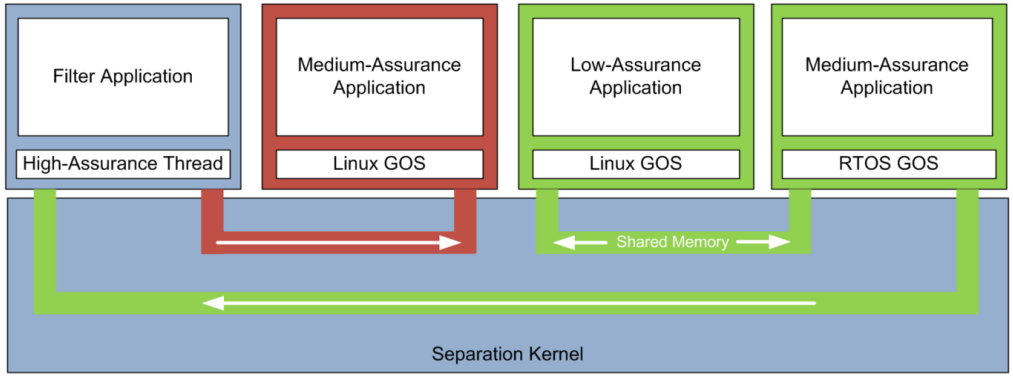
TARDEC VEA'S ROLE IN TECH INSERTION

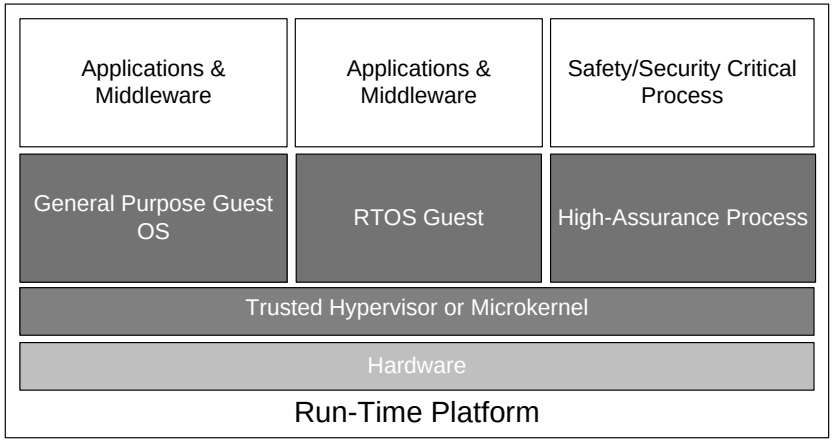
- Enable vehicle modernization and new capabilities via reference implementations, specifications, and guidance for Vehicle Programs
  1. Secure the initialization/boot process
  2. Enable secure software downloads/updates
  3. **Digital containerization**



SEPARATION KERNELS: NOT JUST FOR AVIONICS ANYMORE?

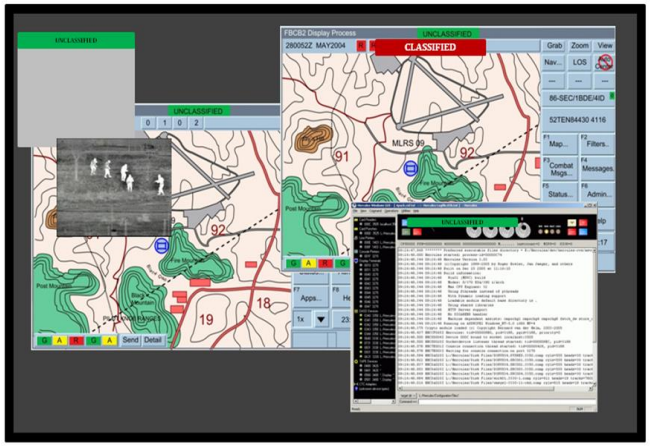
- Separation Kernels may support new capabilities and improve security and resilience for Army ground vehicles
- Supported architectural patterns and benefits include:
  1. Secure integration of mixed-criticality networks and processes
  2. Hardware consolidation for decreased Size, Weight, and Power
  3. Same-level partitioning of domains for Principle of Least Privilege

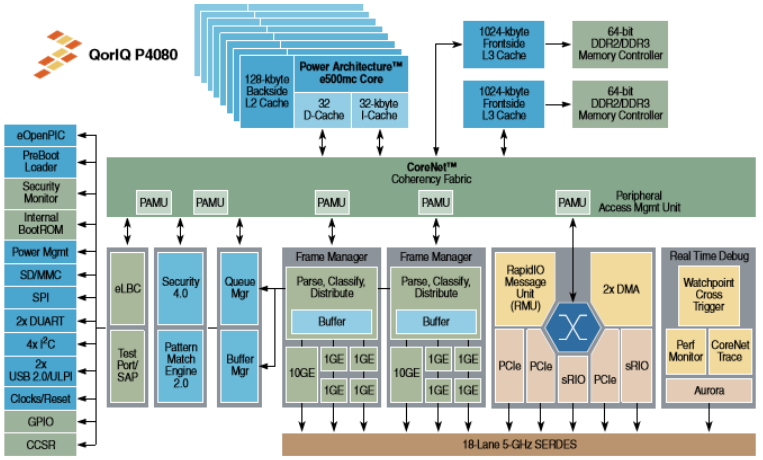




TARDEC VEA MILS EFFORT (2012 – 2014)

- "Bleeding Edge" commercial Multiple Independent Levels of Security (MILS) product evaluated for military ground vehicles applications [2]
- Secure integration of applications on Freescale P4080 multicore platform (e500mc PowerPC core x 8)
- Effort highlighted challenges associated with configuring and debugging applications in MILS environment
- AFRL report indicates P4080 unsuitable for MILS [3]



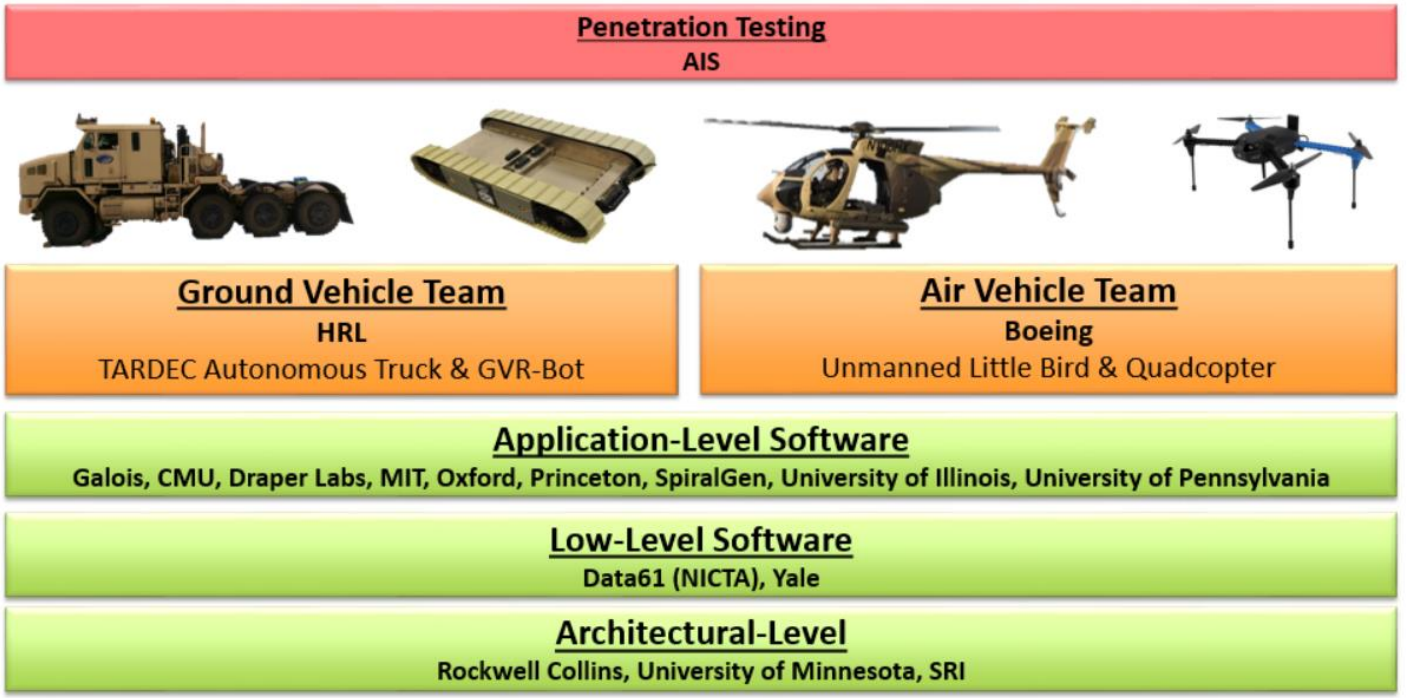


WHY SEL4?

- Commercial offerings traditionally not within budget for ground-vehicles (Abrams Tank ~$5M; Boeing 777 ~$320M)
- Army Ground Vehicle PM's reluctant to commit to expensive service contracts
- Few commercial offerings provide artifacts to support Evaluation of Assurance Level 7 (Formally Verified Design and Tested)
- Commercial products need to protect IP but seem to tend towards security through obscurity
- Contribute to seL4 ecosystem while leveraging open-source benefits to decrease costs

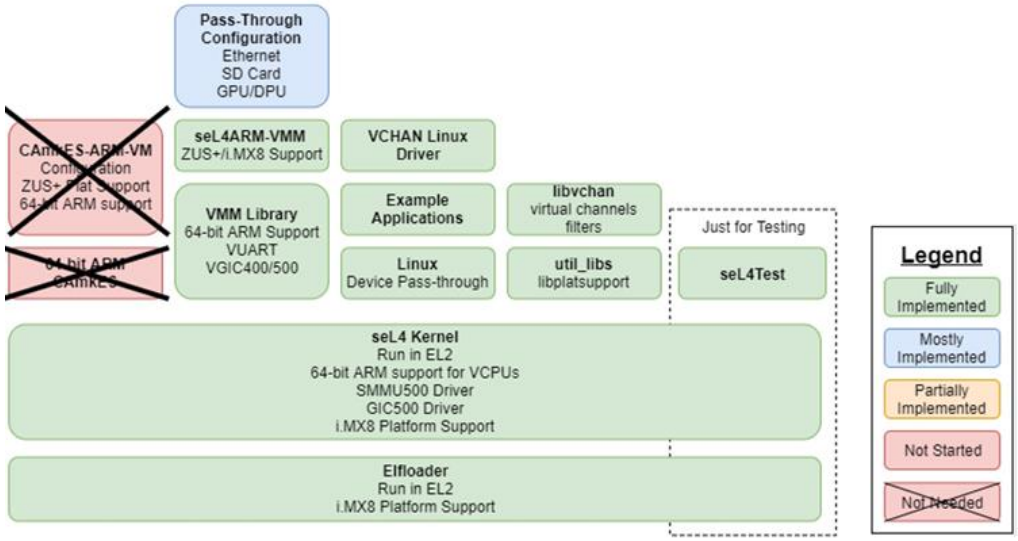
TARDEC HISTORICAL SEL4 EFFORTS

- TARDEC Ground Vehicle Robotics involved in DARPA High-Assurance Cyber Military System (HACMS) project (~2012-2017) [5]
- HACMS performers significantly hardened the TARDEC Autonomous Truck platform



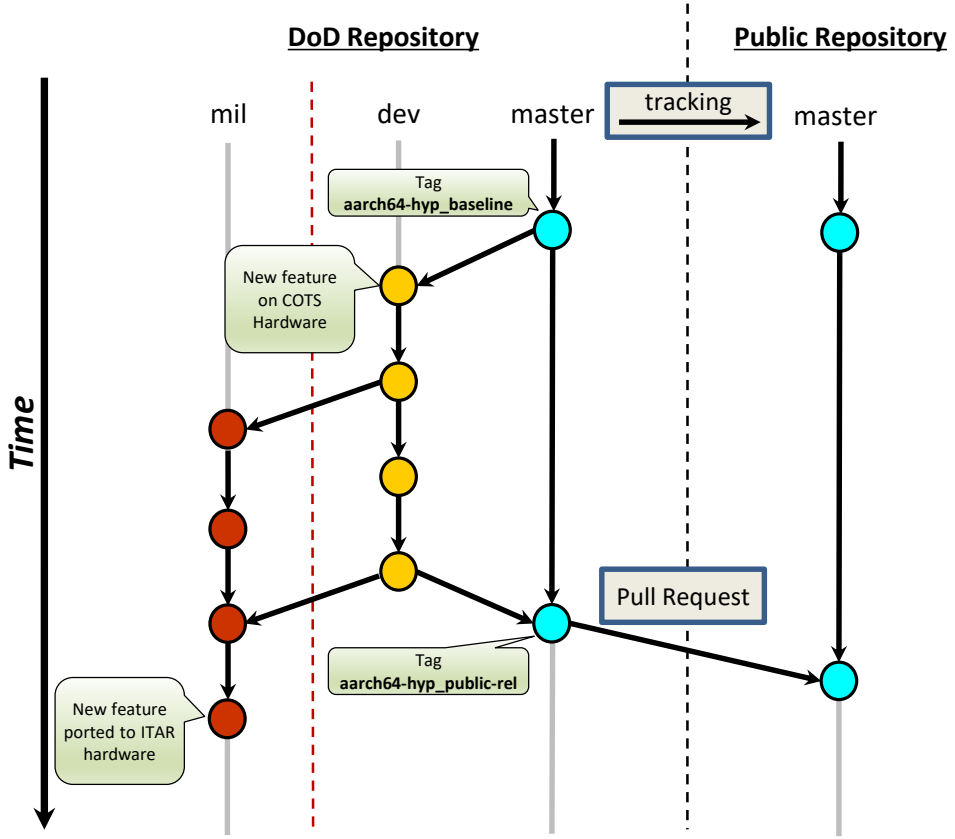
TARDEC SEL4 ONGOING WORK

- TARDEC OTA effort with DornerWorks to port seL4 to i.MX8 with enhanced virtualization and guest support
- Portions of this code has been approved for public-release, however a large portion is undergoing OPSEC review
- Effort is now looking at expanding to Intel Xeon and extending multicore to VMM mode



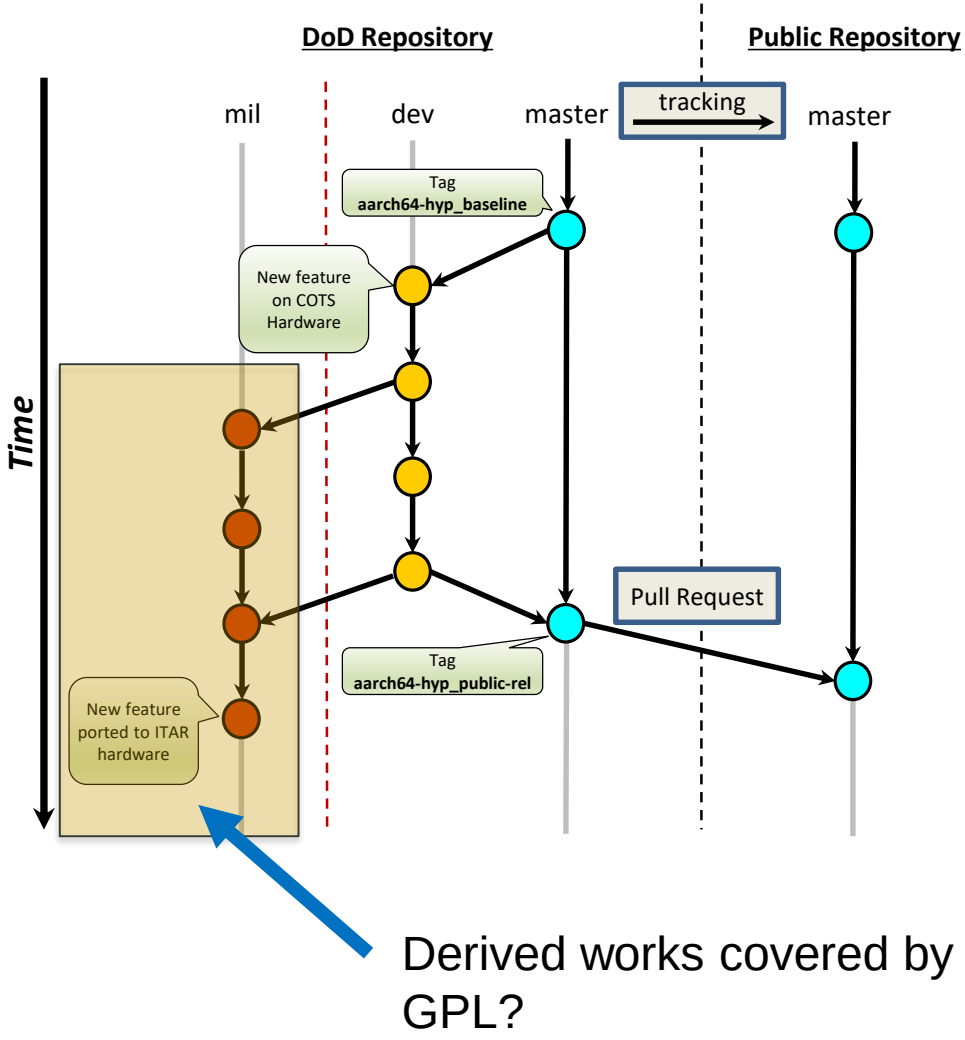
POTENTIAL CHALLENGES: OPEN-SOURCING

- TARDEC public-release process intended for journal articles and presentations
- Pending seL4 open-source submission package (~236 files; ~54,000 SLOC; Git metadata)
- Increased caution/scrutiny required once development targets military hardware



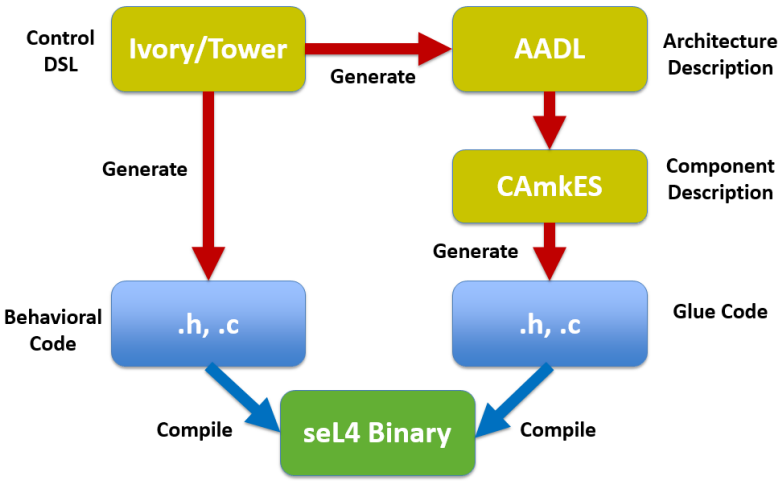
POTENTIAL CHALLENGES: LICENSING

- seL4 Kernel is licensed under GPL version 2
- seL4 tools and libraries are licensed primarily under BSD
- Defense contractors and integrators are wary of “copyleft” licensing
- Potential impact on projects seeking to create derived works from ***mil*** branch



POTENTIAL CHALLENGES: TOOLS & IMPLEMENTATION

- Building trustworthy user-level code involves specialized tools [5]
- Complicated configuration, particularly for multicore architectures with complex switch fabrics



- Limited number of subject matter experts and "formal methods people" available for vehicle programs
- Policy development and implementation:

"However, it is difficult to hire and maintain a workforce with the needed knowledge due to its highly specialized nature. Without this expertise, it will be difficult for programs to effectively implement cybersecurity policies and guidance." [1]

TAKEAWAYS

- DoD weapon systems need improved cyber resilience
- Emerging capabilities substantially increase the need for security
- Commercial separation kernel products have been evaluated and will continue to be monitored
- Several groups in TARDEC working to leverage and contribute to seL4 ecosystem to support high-assurance ground vehicle applications
- DoD Community Source is becoming more common for DoD agencies, but contributing to open-source still a challenge

QUESTIONS?

REFERENCES

1. “Weapon Systems Cybersecurity: DOD Just Beginning to Grapple with Scale of Vulnerability.” U.S. Government Accountability Office. 08 October 2018, https://www.gao.gov/assets/700/694913.pdf
2. Elliott, Leonard, et al. “Separation Kernel Technology for Multiple Independent Levels of Security (MILS) in Military Ground Vehicles.” March 2014, https://www.dtic.mil/DTICOnline/citation.search?docId=ADB398396&collectionId=tr&index=1&format=1f&contentType=HTML
3. “Implications of Multi-Core Architectures on the Development of Multiple Independent Levels of Security (MILS) Compliant Systems.” Air Force Research Lab, October 2012, www.dtic.mil/cgi-bin/GetTRDoc?AD=ADA568860
4. “QorIQ P4080 Communications Processor Product Brief.” Freescale Semiconductor, September 2008, http://cache.freescale.com/files/32bit/doc/prod_brief/P4080PB.pdf?fsrch=1&sr=1
5. Mikulski, Dariusz. “Using Formal Methods Tools to Improve Security in an Autonomous Military Truck.” SANS Automotive Cybersecurity Summit, 01 May 2017, Detroit, MI. https://www.sans.org/cyber-security-summit/archives/file/summit_archive_1493690240.pdf