{

"DARPA Program": "HACMS",

"Program Teams": ["Rockwell Collins"],

"Software": "FM Workbench",

"Internal Link": "",

"External Link": "http://crisys.cs.umn.edu/Tools.shtml",

"Public Code Repo": "",

"Description": "This software package contains the AADL model and some verification properties for the unmanned aerial system used as part of the Secure Mathematically-Assured Composition of Control Models (SMACCM) research project under the HACMS program. This package also contains the Lute plug-in for OSATE in which the properties are encoded",

"Internal Code Repo": "",

"License": "3-clause BSD license",

"Languages": [""],

"Categories": ["Research Integration"]

}

{

"DARPA Program": "HACMS",

"Program Teams": ["Rockwell Collins"],

"Software": "JKind model checker",

"Internal Link": "",

"External Link": "https://github.com/agacek/jkind",

"Public Code Repo": "https://github.com/agacek/jkind",

"Description": "JKind is a Java implementation of the KIND model checker. KIND is a parallel multi-property k-induction based model checker for Lustre programs",

"Internal Code Repo": "",

"License": "3-clause BSD license",

"Languages": [""],

"Categories": ["Research Integration"]

}

{

"DARPA Program": "HACMS",

"Program Teams": ["Galois"],

"Software": "SMACCMPilot",

"Internal Link": "",

"External Link": "http://smaccmpilot.org/",

"Public Code Repo": "https://github.com/galoisinc/smaccmpilot-build",

"Description": "SMACCMPilot is an open source autopilot software for small unmanned aerial vehicles (UAVs) using new high-assurance software methods.",

"Internal Code Repo": "",

"License": "BSD3",

"Languages": [""],

"Categories": ["Control Systems"]

}

{

"DARPA Program": "HACMS",

"Program Teams": ["Galois"],

"Software": "cbmc-reporter",

"Internal Link": "",

"External Link": "https://github.com/GaloisInc/cbmc-reporter",

"Public Code Repo": "https://github.com/GaloisInc/cbmc-reporter",

"Description": "cbmc-reporter is a driver for the CBMC model-checker for use in verifying C library code. cbmc-reporter helps (1) utilize multi-threading when verifying a large number of claims, (2) generates summary tables of resulting proofs, and (3) aids in build-system integration for library code (e.g., parsing function definitions from sources).",

"Internal Code Repo": "",

"License": "BSD3",

"Languages": [""],

"Categories": ["Control Systems"]

}

{

"DARPA Program": "HACMS",

"Program Teams": ["Ivory"],

"Software": "Galois",

"Internal Link": "",

"External Link": "http://smaccmpilot.org/",

"Public Code Repo": "",

"Description": "Ivory is an embedded domain-specific language for safer systems programming. Ivory is implemented as a library of the Haskell programming language. Ivory programs are written using Haskell syntax and types. Ivory is not a general purpose programming language. It aims to be a good language for writing a restricted subset of programs. Ivory gives strong guarantees of type and memory safety, and has features which allow the programmer to specify other safety properties. Ivory is well suited for writing programs which interact directly with hardware and do not require dynamic memory allocation. Ivory can be considered to be a lot like a restricted version of the C programming language, embedded in Haskell.",

"Internal Code Repo": "",

"License": "BSD3",

"Languages": [""],

"Categories": ["Control Systems"]

}

{

"DARPA Program": "HACMS",

"Program Teams": ["Galois"],

"Software": "Tower",

"Internal Link": "",

"External Link": "http://smaccmpilot.org/",

"Public Code Repo": "",

"Description": "Tower is a language for composing Ivory programs into real-time tasks. Tower is both a specification language and a code generator. A Tower program describes communication channels and tasks, and provides an Ivory implementation of each task. Tower compiles the specification for the program and delegates code generation to an operating-system specific backend",

"Internal Code Repo": "",

"License": "BDS3",

"Languages": [""],

"Categories": ["Control Systems"]

}

{

"DARPA Program": "HACMS",

"Program Teams": ["NICTA"],

"Software": "CAmkES: Component Architectures for microkernel-based Embedded System",

"Internal Link": "",

"External Link": "http://www.ertos.nicta.com.au/research/camkes/",

"Public Code Repo": "",

"Description": "The CAmkES project provides a solution for quickly and reliably building complex microkernel-based embedded systems software",

"Internal Code Repo": "",

"License": "BSD",

"Languages": [""],

"Categories": ["Operating Systems"]

}

{

"DARPA Program": "HACMS",

"Program Teams": ["NICTA"],

"Software": "WCET: Worst-case execution time computations tools",

"Internal Link": "",

"External Link": "http://www.ssrg.nicta.com.au/software/TS/wcet-tools/",

"Public Code Repo": "http://www.ssrg.nicta.com.au/software/TS/wcet-tools/",

"Description": "The WCET computation is based on Chronos 4.2 and is augmented with additional code to perform control flow graph extraction, loop bound computation and infeasible path detection. The default modelled hardware is the ARM1136 i.MX31 processor on the KZM evaluation board. This software was developed as part of research into mixed-criticality real-time systems, and has been used to compute execution time bounds for seL4",

"Internal Code Repo": "",

"License": "GPL",

"Languages": [""],

"Categories": ["Operating Systems"]

}

{

"DARPA Program": "HACMS",

"Program Teams": ["NICTA"],

"Software": "Trustworthy File Systems",

"Internal Link": "",

"External Link": "http://www.ssrg.nicta.com.au/projects/TS/filesystems.pml",

"Public Code Repo": "",

"Description": "The aim of Trustworthy File Systems is to develop a methodology for the creation of correct-by-construction file systems.",

"Internal Code Repo": "",

"License": "Open Source License TBD",

"Languages": [""],

"Categories": ["Operating Systems"]

}

{

"DARPA Program": "HACMS",

"Program Teams": ["Princeton University"],

"Software": "Verified Software Toolchain",

"Internal Link": "",

"External Link": "http://vst.cs.princeton.edu/",

"Public Code Repo": "http://vst.cs.princeton.edu/",

"Description": "The software toolchain includes static analyzers to check assertions about your program; optimizing compilers to translate your program to machine language; operating systems and libraries to supply context for your program. The Verified Software Toolchain project assures with machine-checked proofs that the assertions claimed at the top of the toolchain really hold in the machine-language program, running in the operating-system context. ",

"Internal Code Repo": "",

"License": "Most falls under BSD license, but some of CompCert portion is GPL",

"Languages": [""],

"Categories": ["Operating Systems"]

}

{

"DARPA Program": "HACMS",

"Program Teams": ["Princeton University"],

"Software": "Message-authentication enhancements to the ROS operating system",

"Internal Link": "",

"External Link": "",

"Public Code Repo": "",

"Description": "Message-authentication enhancements to the ROS operating system ",

"Internal Code Repo": "",

"License": "Open source license TBD",

"Languages": [""],

"Categories": ["Operating Systems"]

}

{

"DARPA Program": "HACMS",

"Program Teams": ["Yale University"],

"Software": "CertiKOS kernel",

"Internal Link": "",

"External Link": "http://flint.cs.yale.edu/certikos/",

"Public Code Repo": "",

"Description": "CertiKOS is a new hypervisor kernel that leverages formal certification to ensure correctness and isolate critical services from noncritical components.",

"Internal Code Repo": "",

"License": "Open source license TBD",

"Languages": [""],

"Categories": ["Operating Systems"]

}

{

"DARPA Program": "HACMS",

"Program Teams": ["MIT"],

"Software": "Bedrock Coq library",

"Internal Link": "",

"External Link": "http://plv.csail.mit.edu/bedrock/",

"Public Code Repo": "http://plv.csail.mit.edu/bedrock/",

"Description": " Bedrock is a library that turns Coq into a tool much like classical verification systems (e.g., ESC, Boogie), but niftier. In particular, Bedrock is: (1) Low-level: You can verify programs that, for performance reasons or otherwise, can't tolerate any abstraction beyond that associated with assembly language. (2) Foundational: The output of a Bedrock verification is a theorem whose statement depends only on the predicates you choose to use in the key specifications and on the operational semantics of a simple cross-platform machine language. That is, you don't need to trust that the verification framework is bug-free; rather, you need to trust the usual Coq proof-checker and the formalization of the machine language semantics. Higher-order: Bedrock facilitates quite pleasant reasoning about code pointers as data. (3) Computational: Many useful functions are specified most effectively by comparing with "reference implementations" in a pure functional language. Bedrock supports that model, backed by the full expressive power of Coq's usual programming language. (4) Structured: Bedrock is an extensible programming language: any client program may add new control flow constructs by providing their proof rules. For example, adding high-level syntax for your own calling convention or exception handling construct is relatively straightforward and does not require tweaking the core library code. (5) Mostly automated: Tactics automate verification condition generation (in a form inspired by separation logic) and most of the process of discharging those conditions. Many interesting programs can be verified with zero manual proof effort, in stark contrast to most Coq developments.",

"Internal Code Repo": "",

"License": "BSD",

"Languages": [""],

"Categories": ["Operating Systems"]

}

{

"DARPA Program": "HACMS",

"Program Teams": ["The Charles Stark Draper Laboratory, Inc."],

"Software": "LLVM decompiler",

"Internal Link": "",

"External Link": "",

"Public Code Repo": "",

"Description": "Draper's HACMS Decompiler is a software tool based on the LLVM open source compiler project. The HACMS Decompiler is a set of modifications to the LLVM compiler that make it run backwards. The HACMS Decompiler converts computer program instructions for a specific machine (binary software program) into generic machine instructions (machine-independent assembly program) called LLVM intermediate representation (IR). The HACMS Decompiler enables a user to directly analyze and modify the resulting LLVM IR. Near term additions to the HAMCS Decompiler include the ability to emit a C program representation from the IR. The HACMS Decompiler currently supports ARM architectures, however it will be extended to include X86, PowerPC, MIPS, and other ISAs as required by the program.",

"Internal Code Repo": "",

"License": "Open Source License TBD",

"Languages": [""],

"Categories": ["Red Team"]

}

{

"DARPA Program": "HACMS",

"Program Teams": ["The Charles Stark Draper Laboratory, Inc."],

"Software": "CSPM parser/type-checker/evaluator included in FDR3",

"Internal Link": "",

"External Link": "https://github.com/tomgr/libcspm",

"Public Code Repo": "https://github.com/tomgr/libcspm",

"Description": "This library provides a FDR-compliant parser, type checker and (experimental) evaluator for machine CSP files. There is also a program, cspmchecker, that makes use of this library to provide command line type checking.",

"Internal Code Repo": "",

"License": "Open Source License TBD",

"Languages": [""],

"Categories": ["Red Team"]

}

{

"DARPA Program": "HACMS",

"Program Teams": ["SRI"],

"Software": "Evidential Tool Bus",

"Internal Link": "",

"External Link": "",

"Public Code Repo": "",

"Description": "The evidential tool bus(ETB) allows for low-cost integration of diverse tools and components into customized tool chains, and the combination of evidence from different sources into a credible assurance case.",

"Internal Code Repo": "",

"License": "GPL license",

"Languages": [""],

"Categories": ["Research Integration"]

}

{

"DARPA Program": "HACMS",

"Program Teams": ["SRI"],

"Software": "New high-assurance ROS modules that will provide security services such as authentication and integrity",

"Internal Link": "",

"External Link": "",

"Public Code Repo": "",

"Description": "New high-assurance ROS modules that will provide security services such as authentication and integrity ",

"Internal Code Repo": "",

"License": "BSD license TBD",

"Languages": [""],

"Categories": ["Research Integration"]

}

{

"DARPA Program": "HACMS",

"Program Teams": ["Kestrel"],

"Software": "Specware System",

"Internal Link": "",

"External Link": "http://www.specware.org/ ",

"Public Code Repo": "http://www.specware.org/news.html",

"Description": "Specware is a software engineering tool that automatically generates high-assurance software. Specware is a leading-edge automated software development system that allows users to precisely specify the desired functionality of their applications and to generate provably correct code based on these requirements. At the core of the design process in Specware lies stepwise refinement, in which users begin with a simple, abstract model of their problem and iteratively refine this model until it uniquely and concretely describes their application.",

"Internal Code Repo": "",

"License": "Open Source License TBD",

"Languages": [""],

"Categories": ["Operating Systems"]

}

{

"DARPA Program": "HACMS",

"Program Teams": ["University of Pennsylvania"],

"Software": "ROS based cruise controller simulator ",

"Internal Link": "",

"External Link": "",

"Public Code Repo": "",

"Description": "ROS based cruise controller simulator",

"Internal Code Repo": "",

"License": "GNU GPL",

"Languages": [""],

"Categories": ["Control Systems"]

}

{

"DARPA Program": "HACMS",

"Program Teams": ["University of Pennsylvania "],

"Software": "Attack-resilient implementation of cruise controllers",

"Internal Link": "",

"External Link": "",

"Public Code Repo": "",

"Description": "A constant-speed cruise control for LandShark that ensures vehicle maintains speed when some sensors are attacked (e.g., attack on encoders & GPS spoofing). Also includes adaptive cruise control for an American Built Car based on the CarSim simulator",

"Internal Code Repo": "",

"License": "GNU GPL",

"Languages": [""],

"Categories": ["Control Systems"]

}

{

"DARPA Program": "HACMS",

"Program Teams": ["University of Pennsylvania "],

"Software": "Attack-resilient sensor fusion module",

"Internal Link": "",

"External Link": "",

"Public Code Repo": "",

"Description": "Ubiquitous/redundant sensors can provide additional information about system state. Low-precision sensors can be used to improve attack detection and identification. ",

"Internal Code Repo": "",

"License": "GNU GPL",

"Languages": [""],

"Categories": ["Control Systems"]

}

{

"DARPA Program": "HACMS",

"Program Teams": ["Carnegie Mellon University"],

"Software": "HACMS Spiral package",

"Internal Link": "",

"External Link": "",

"Public Code Repo": "",

"Description": "Open source package that runs on top of the core Spiral Engine and does everything HACMS-specific",

"Internal Code Repo": "",

"License": "Open Source License TBD",

"Languages": [""],

"Categories": ["Control Systems"]

}