High **A**ssurance **C**yber **M**ilitary **S**ystems **(HACMS)**

Making sure *you* are in control of your vehicle

PROPOSERS' DAY

Arlington, VA

February 21, 2012

Images of specific products throughout this presentation are used for illustrative purposes only.
Use of these images is not meant to imply inherent vulnerability of a product or company.

Agenda

0900 – 1000	Check-In/Registration	
1000 – 1005	Welcoming Remarks	Dr. Kathleen Fisher, DARPA
1005 – 1020	Contracts	Mr. Mark Jones, DARPA
1020 – 1030	Security	Ms. Angela Ivey, DARPA
1030 – 1130	HACMS Program	Dr. Kathleen Fisher, DARPA
1130 – 1200	Platform Demo	Mr. Brian Hart, Black-I Robotics
1200 – 1300	LUNCH BREAK (Submit questions)	
1300 – 1430	Individual Company Presentations	
1430 – 1530	Government Response to Questions	Dr. Kathleen Fisher, DARPA

Logistics

- Anticipated BAA
  - Posted on FedBizOpps website (http://www.fedbizopps.gov) and Grants.gov website (http://www.grants.gov)
  - Posting Date: TBD
  - Proposal Due Date: TBD
  - BAA Closing Day: TBD

- Procedure for Questions/Answer
  - Questions can be submitted at anytime at the registration desk until 12:30 pm
  - Questions will be answered during Q&A session in the afternoon

- Websites
  - Proposers' Day website (www.solers.com/BAAinfo-reg/hacms)
  - HACMS program website (http://www.darpa.mil/Our_Work/I2O/Programs/High-Assurance_Cyber_Military_Systems_(HACMS).aspx)
  - Copy of presentations
  - Video recording
  - Frequently Asked Questions (FAQ)

Contracts Briefing

Mr. Mark Jones

BAA PROCESS OVERVIEW

- Solicitation will be released utilizing BAA procedures in accordance with FAR 35.016
- The BAA (and any amendments) will be posted in FEDBIZOPPS at www.fbo.gov and Grants.gov at www.grants.gov
- BAA allows for a variety of technical solutions
- Proposal evaluations will be accomplished through a scientific review using the evaluation criteria stated in the BAA.
- The BAA will contain an initial closing time/date and a final closing time/date and these times/dates will be annotated in the BAA. The initial closing time/date is THE timeframe to submit proposals.
- BAA will cover all info needed to propose.
- Following the proposal preparation instructions assists the evaluation team to clearly understand what is being proposed and supports a timely negotiation

ELIGIBILITY

- All interested/qualified sources may respond subject to the parameters outlined in BAA
- Foreign participants/resources may participate to the extent allowed by applicable Security Regulations, Export Control Laws, Non-Disclosure Agreements, etc.
- FFRDCs and Government entities are subject to applicable direct competition limitations and cannot propose to this BAA in any capacity, unless they clearly demonstrate the work is NOT otherwise available from the private sector AND provide written documentation citing the specific statutory authority establishing eligibility to propose to Government solicitations and (for FFRDCs) written authorization from the sponsoring agency.
- Procurement Integrity: Potential Conflicts of Interest – Identify and discuss mitigation – failure to do so will result in proposal rejection without technical evaluation or further consideration for award

POTENTIAL AWARD INSTRUMENTS

- FAR Based Procurement Contracts
- Cooperative Agreements – NO GRANTS
- Other Transaction Agreements (TIA and 845 Prototypes)

The contracting officer shall have sole discretion to select award instrument type and to negotiate all instrument provisions with selectees.

PROPOSAL PREPARATION INFORMATION

- Consists of two volumes – Technical (with required Appendix A and optional Appendix B) and Cost
- Volume I - Technical and Management
  - Volume I will have a page limitation as indicated in the BAA. The evaluation team will not review any submitted pages that exceed the Volume I limit.
  - Volume I includes a mandatory Appendix A and optional Appendix B (appendixes have no page limits). The Appendixes do not count towards Volume I's page limit total(s).
- Volume II – Cost – No page limitation
- BAA describes the necessary information to address is each volume –
    - Make sure to include every section identified
    - If section does not apply – put "None" (e.g. Animal Use – None, OCI - None)
    - Include a working spreadsheet as part of your Cost Volume submission
    - Remember: Appendix A is mandatory

PROPOSAL PREP – TECHNICAL DATA RIGHTS

- Government desires, at a minimum, **Government Purpose Rights** for any proposed noncommercial software (including source code), software documentation, hardware designs and documentation, and technical data.

- Data Rights Assertions – Assert rights to all technical data & computer software generated, developed, and/or delivered to which the Government will receive **less than Unlimited Rights**. This information may be assessed during evaluations.
  - Provide and justify basis of assertions that apply to the Prime and any Subs in the prescribed format (See DARPA-BAA-11-63 Section VI (B) 2). Break out these assertions in a separate table (if possible) to be included as an attachment to a resultant contract or agreement.
  - Explain how the Government will be able to reach its program goals (including transition) within the proprietary model offered; and
  - Provide possible nonproprietary alternatives in any areas that might present transition difficulties or increased risk or cost to the Government under the proposed proprietary solution. NOTE: Offerors expecting to use, but not to deliver, open source tools or other materials in implementing their approach may be required to indemnify the Government against any legal liability arising from such use.

ITEMS TO NOTE

- Understand and be compliant with Central Contractor Registration (CCR), Online Representations and Certifications Application (ORCA), Electronic and Information Technology compliance, Employment Eligibility Verification (E-verify), Reporting Executive Compensation and First-Tier Subcontract Awards and Updates of Information Regarding Responsibility Matters (FAPIIS)

- Awardees will be required to use i-Edison, T-FIMS and Wide Area Workflow (WAWF)

- Subcontracting Issues
  - NON SMALL BUSINESSES: Subcontracting Plans required for FAR based contracts with subcontracting possibilities expected to exceed $650,000
  - Subcontractor cost - Proposals must include, at a minimum, a non-proprietary, subcontractor proposal for EACH subcontractor
  - If utilizing FFRDC, Government entity, or a foreign owned firm as a subcontractor, submit their required eligibility information

HACMS Proposers' Day

- Proposals must be valid for a minimum of 120 days
- If a prospective proposer believes a conflict of interest exists or may exist (whether organizational or otherwise) or has a question on what constitutes a conflict, the proposer should promptly raise the issue with DARPA by sending the proposer's contact information and a summary of the potential conflict to the BAA mailbox before preparing a proposal and mitigation plan.
- Document files must be in Portable Document Format (.pdf, ISO 32000-1), OpenDocument (.odx, ISO/IEC 26300:2006), .doc, .docx, .xls, or .xlsx formats.
- Submissions must be written in English.

ITEMS TO NOTE – NEW ITEMS

- 2 new certification requirements:
  1. Representation by Corporations Regarding Unpaid Delinquent Tax Liability or a Felony Conviction Under Any Federal Law – Applies to ALL
  2. Cost Accounting Standards Notices and Certification (Deviation 2012-00003 (JAN 2012) – Applies to ALL proposed FAR base procurement contracts over $700K

- New DARPA Mailing Address as of April 2, 2012

675 North Randolph Street

Arlington, VA 22203-2114

PROPOSAL SUBMISSION

- The BAA outlines proposal submission procedures for both unclassified and classified proposals:
  - Follow procedures detailed in BAA - Failure to comply with the submission procedures may result in the submission not being evaluated
  - Proposers must submit their entire proposal via the same method; applications cannot be submitted in part via one method and in part via another method nor should duplicate submissions be sent via multiple methods.
- DO NOT email or fax proposals
- DO NOT wait until the last minute to submit proposals – submission deadlines are strictly enforced and late submissions may not be evaluated

EVALUATION / AWARD

- No common Statement of Work - Proposal evaluated on individual merit and relevance as it relates to the stated research goals/objectives rather than against each other.
- Evaluation Criteria will be identified in the BAA.
- Evaluation Process is a scientific/technical review - Reviews conducted by panels of experts that may include contracted Government SETAs bound by strict non disclosure agreements.
- Government reserves the right to select for award all, some, or none of the proposals received, to award portions of a proposal, and to award with or without discussions.
- No portion of this announcement will be set aside for Historically Black Colleges and Universities (HBCUs), Small Businesses, Small Disadvantaged Businesses and Minority Institutions (MIs) and no preferences apply.

COMMUNICATION

- Prior to Receipt of Proposals – No restrictions, however Gov't (PM/PCO) shall not dictate solutions or transfer technology. FAQs will be periodically posted to this BAA's DARPA Web page.

- After Receipt of Proposals – Prior to Selection: Government (PM/PCO) may communicate with offerors in order to understand the meaning of some aspect of the proposal that is not clear or to obtain confirmation or substantiation of a proposed approach, solution, or cost estimate. After Selection/Prior to Award: Government (PCO) may clarify aspects of the proposal and/or may conduct negotiations. Government (PM/COR/PCO) may clarify the Statement of Work or, in cases where only portions of the proposal are accepted, may discuss reductions to the scope to match the selected effort.

- Informal feedback for non selected proposals may be provided once the selection(s) are made.

Only a duly authorized Contracting Officer may obligate the Government

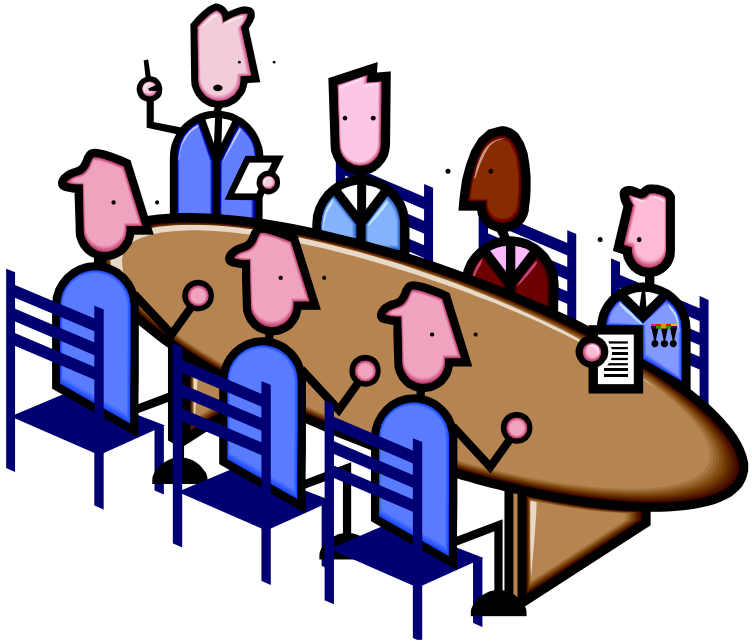
Security Briefing

Ms. Angela Ivey

MEETING LEVEL

- THIS MEETING IS SET AT THE UNCLASSIFIED LEVEL. THERE WILL BE PUBLIC RELEASE INFORMATION ONLY WITH NO CLASSIFIED DISCUSSIONS.

- PARTICIPANTS
  - U.S. INDUSTRY
  - U.S. DOD AGENCIES
  - UNIVERSITIES
  - FOREIGN NATIONALS



PROGRAM OVERVIEW

- DARPA security is governed by:

  -- Executive Order 13526, "Classified National Security Information"

  -- DoD 5220.22-M, National Industrial Security Program Operating Manual, (NISPOM)

- It is anticipated that there will be not be a DARPA Security Classification Guide (SCG) for this Program. However guidance will be provided.

  --Guidance will assist with identifying what aspects are classified (if any).

  (ie. Vulnerabilities, capabilities, testing, countermeasures)

Facilities/Personnel Clearance Requirements

Documentation of your Ability to Support Classified Development:

- Proposers submitting a proposal for Technical Areas 1, 4, and 5 must include what level of classified support (e.g., Secret, Top Secret, SCI) they can provide, their CAGE code, and security point(s) of contact in their proposals.

- Technical Areas 2 and 3 - No clearance requirements.

Note: While it is not necessary for all members of a prime proposer's team (including subcontractors) to hold clearances, all primes are responsible for ensuring that un-cleared personnel are properly firewalled from access to classified data.

Proposal Submissions

- The Government anticipates that proposals submitted under this BAA will be unclassified.

  HOWEVER,

  - IF proposals are classified, the proposals must indicate the classification level and marked at the appropriate level and then submitted to DARPA for a final classification determination.

  - Offerors choosing to submit classified information must follow the procedures outlined in **Section IV B. of the BAA**

  - Offerors submitting classified proposal from other classified sources must first obtain written permission from the Original Classification Authority (OCA) to use their information in the proposal submissions.

  - Also the applicable security classification guide must be provided to ensure proper protection of the proposal (if applicable).

PROPOSAL CREATION

- PROPOSAL SUBMISSIONS

  -- UNCLASSIFIED - Preferred

  -- CLASSIFIED Annexes Allowed

  Submit classified material per instructions in Section IV..

- PERFORMER RESPONSIBILITIES

  -- PROTECTING THE INFORMATION

  -- CUI (Controlled Unclassified Information)

  -- ITAR (*International Traffic and Arms Regulation*)

  -- FOUO (For Official Use Only)

  etc.

DARPA Security Points Of Contact

- PROGRAM SECURITY REPRESENTATIVE

  Angela M. Ivey

  OFFICE : 703-526-4775

  EMAIL: Angela.Ivey.ctr@darpa.mil

- PROGRAM SECURITY OFFICER

  Brett A. Nelson

  OFFICE: 703-526-4738

  EMAIL: Brett.Nelson@darpa.mil

HACMS Program Briefing

Dr. Kathleen Fisher

Pervasive Vulnerability

SCADA Systems

Source: Laing O'Rourke

Source: Dept. of Energy

Medical Devices

Source: www.seekinglpha.com

Source: www.medtechbusiness.com

Computer Peripherals

Source: HP

Source: www.buy.com

Source: www.bagitech.com

Communication Devices

Source: NASA

Source: www.engadget.com

Source: GD C4S

Vehicles

Source: www.militaryaerospace.com

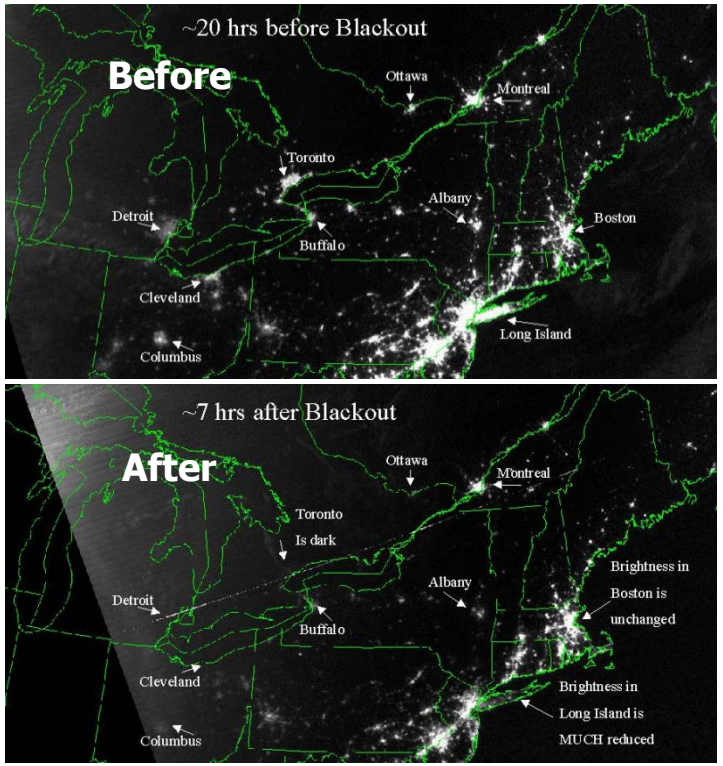
Source: www.naval-technology.com

Source: www.motortrend.com

Ubiquitous, Invisible, Networked, Computing Substrate

- In 2008, ~30 embedded processors per person in developed countries.
- In 2009, 98% of microprocessors were embedded [IEEE Computer `09]
- Trend: *Networked* embedded systems
- Vulnerabilities have economic and national security consequences. Extrapolating from *safety* failures:
  - June 10, 1999. Olympic Pipeline Company. 237K gallons of gasoline spilled. 3 deaths. >$45M damages. [NTSB report]
  - Aug 14 2003. Northeast Blackout cost $6B for 2 days of outage [DOE study]
  - April 26, 1986. Chernobyl Nuclear Disaster: >$300B. Belarus alone: $235B. [Chernobyl Forum]

August 14 2003
Northeast Blackout



Source: NOAA

The growing connectivity between information systems, the Internet, and other infrastructures creates opportunities for attackers to disrupt telecommunications, electrical power, energy pipelines, refineries, financial networks, and other critical infrastructures."
-- Dennis C. Blair, Director of National Intelligence, *Annual Threat Assessment of the Intelligence Community for the Senate Select Committee on Intelligence, Statement for the Record,* February 12, 2009

Many Remote Attack Vectors

Mechanic

Source: www.custom-build-computers.com

Source: CanOBD2

Short-range wireless

Bluetooth

Source: www.diytrade.com

Long-range wireless

Wi-Fi

Source: www.theunlockr.com

Source: www.autoblog.com

Source: christinayy.blogspot.com

Source: Koscher, K., et al. "Experimental Security Analysis of a Modern Automobile"

Source: www.wikipedia.org

Source: www.zedomax.com

Entertainment

Securing Cyber-Physical Systems: State of the Art

Control Systems

- Air gaps & obscurity

> Forget the myth of the air gap – the control system that is completely isolated is history.
> *-- Stefan Woronka, 2011*
> *Siemens Director of Industrial Security Services*

- Trying to adopt cyber approaches, but technology is not a good fit:
  - Resource constraints, real-time deadlines
  - Extreme cost pressures
  - Patches may have to go through lengthy verification & validation processes
  - Patches could require recalls

We need a *fundamentally different* approach

Cyber Systems

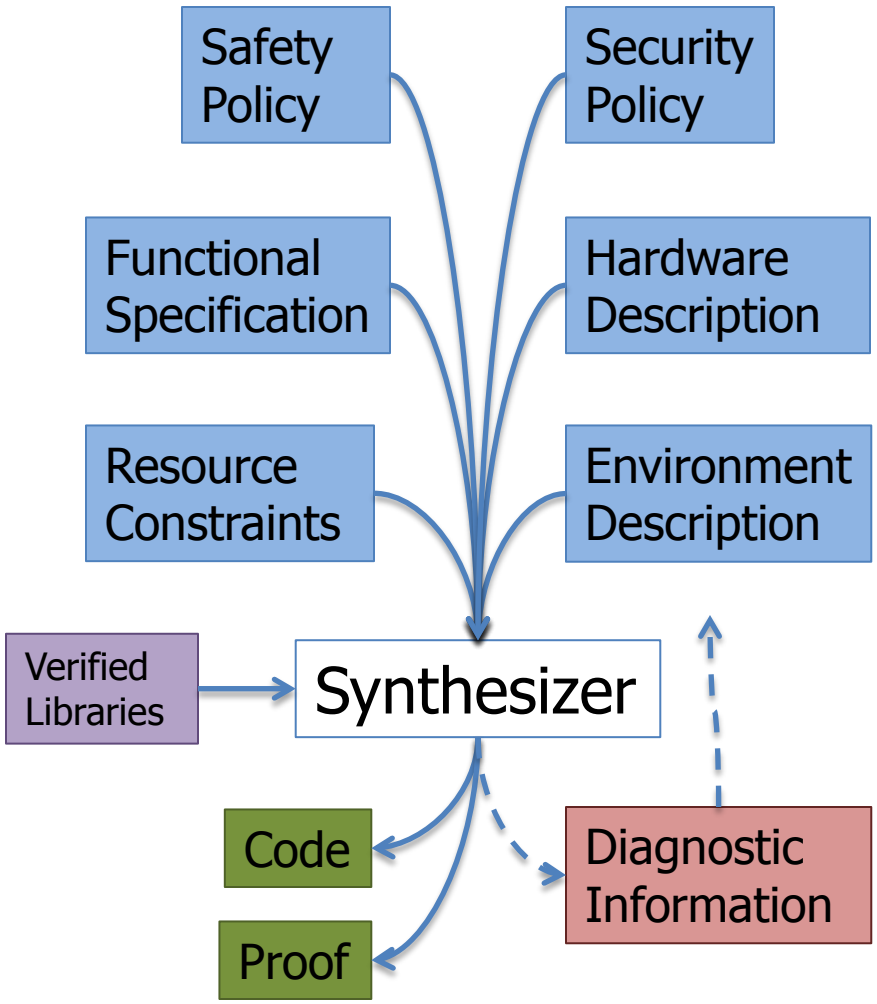
- Anti-virus scanning, intrusion detection systems, patching infrastructure
- This approach *cannot* solve the problem.
  - Not convergent with the threat
  - Focused on known vulnerabilities; can miss zero-day exploits
  - Can introduce new vulnerabilities and privilege escalation opportunities

October 2010 Vulnerability Watchlist

Vulnerability Title	Fix Avail?	Date Added
[illegible]	[illegible]	[illegible]
[illegible]	[illegible]	[illegible]
[illegible]	[illegible]	[illegible]
[illegible]	[illegible]	[illegible]
[illegible]	[illegible]	[illegible]
[illegible]	[illegible]	[illegible]
[illegible]	[illegible]	[illegible]
[illegible]	[illegible]	[illegible]
[illegible]	[illegible]	[illegible]
[illegible]	[illegible]	[illegible]
[illegible]	[illegible]	[illegible]
[illegible]	[illegible]	[illegible]
[illegible]	[illegible]	[illegible]
[illegible]	[illegible]	[illegible]
[illegible]	[illegible]	[illegible]
[illegible]	[illegible]	[illegible]
[illegible]	[illegible]	[illegible]

1/3 of the vulnerabilities are in security software!

Idea: Synthesize & Verify High-Assurance Systems



Proof: Generated executable

- implements functional specification,
- satisfies safety and security policies, and
- satisfies resource constraints

when run

- on hardware satisfying the hardware description and
- in an environment satisfying the environmental description.

"If software always worked as specified or intended by its makers, only a small subset would be vulnerable to attack, and defenses would be much easier to implement."
Felix Lindner, Recurity Labs, *CACM*, June 2006

High Assurance: Correctness, Safety, Security

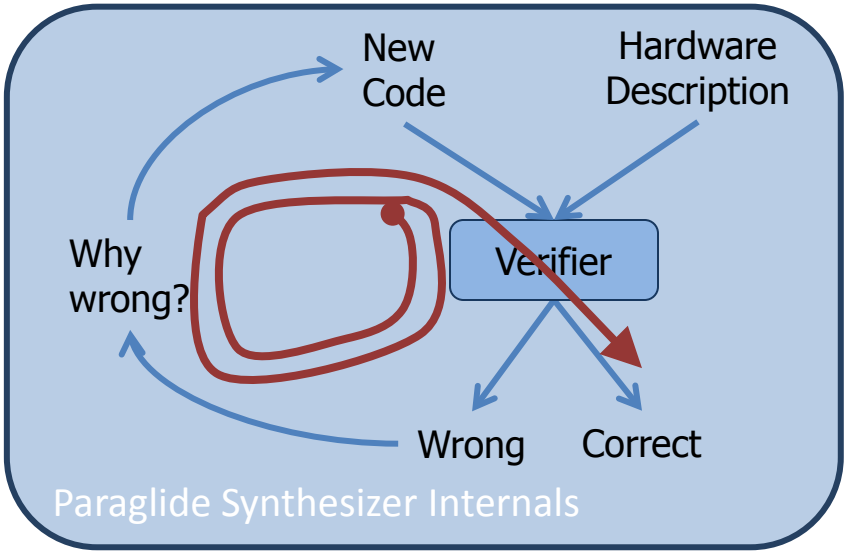
Synthesis Example: Domain of Concurrent Data Structures

C/C++ Highly Concurrent Work Queue

Core of various IBM products

Fragile: ~50 buggy versions, 2 years

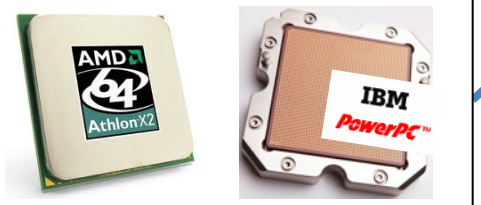
Paraglide generated correct implementation



Program Specification

Concurrent Work Queue Description

Hardware Description



Source: www.amazon.com

IBM Paraglide Synthesizer

SAT solving
Model checking
Abstraction-directed testing
Semantic search

Synthesized Program

```
bool add(int key) {
 Entry *pred,*curr,*entry;
restart:
 locate(pred,curr,key);
 k = (curr->key == key);
 if (k) return false;
 entry = new Entry();
 entry->next = curr;
 val=
 CAS(&pred->next,<curr,0>,<entry,0>);
 if (!val) goto restart;
 return true;
}
```

Vechev and Yahav, *Deriving Linearizable Fine-Grained Concurrent Objects*, in ACM PLDI 2008.
Kuperstein, Vechev, and Yahav, *Automatic Inference of Memory Fences*, in FMCAD, 2010.

SAT Solvers and Infrastructure Development: Critical Enablers for High Assurance Systems

Interactive Theorem Provers

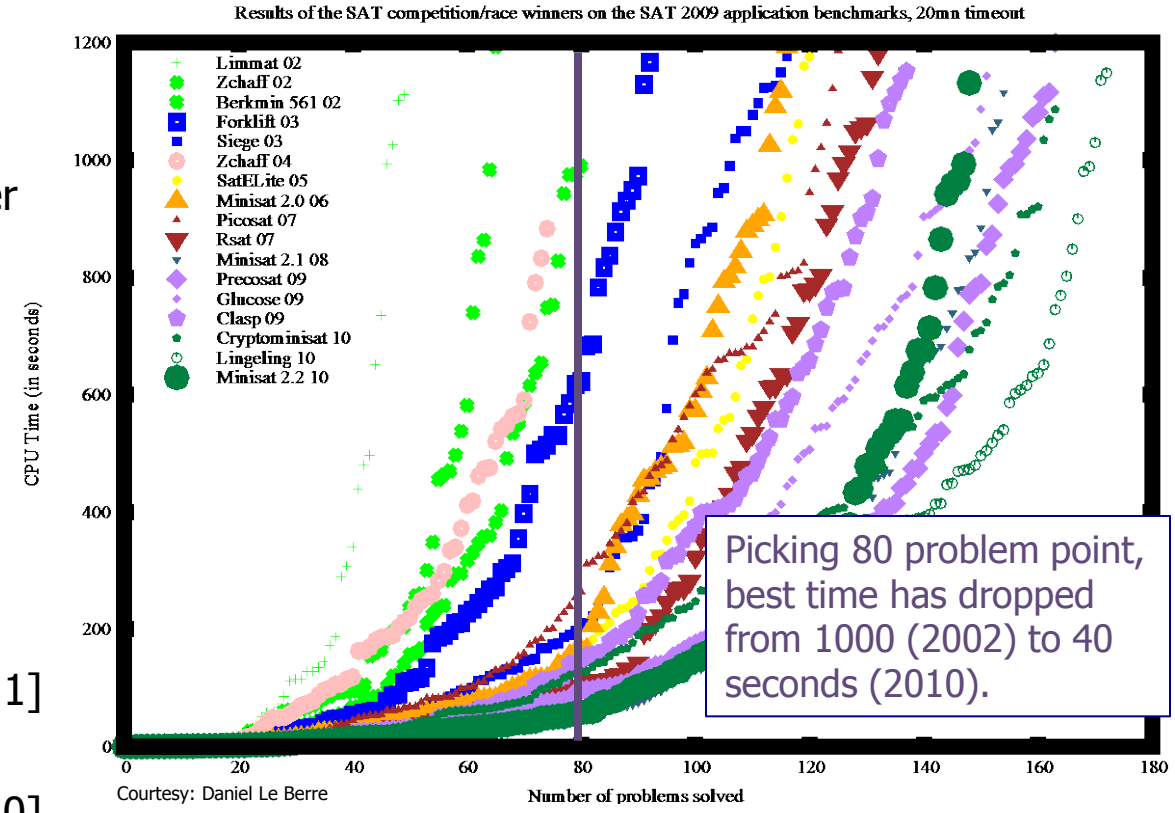
- seL4 microkernel
  [9000 LoC:C, SOSP 09]
- compCert verifying C compiler
  [6K LoC:ML, POPL 06]

Automatic Theorem Provers

- Verve OS Nucleus
  [1.5K LoC:x86, PLDI 10]
- Baby Hypervisor
  [1K LoC:C, VSTTE 10]

Model Checkers

- Microsoft device drivers
  [30K LoC:C, PLDI 01, CACM 11]
- ADGS-2100 Window Manager
  [16K Simulink blocks, CACM 10]



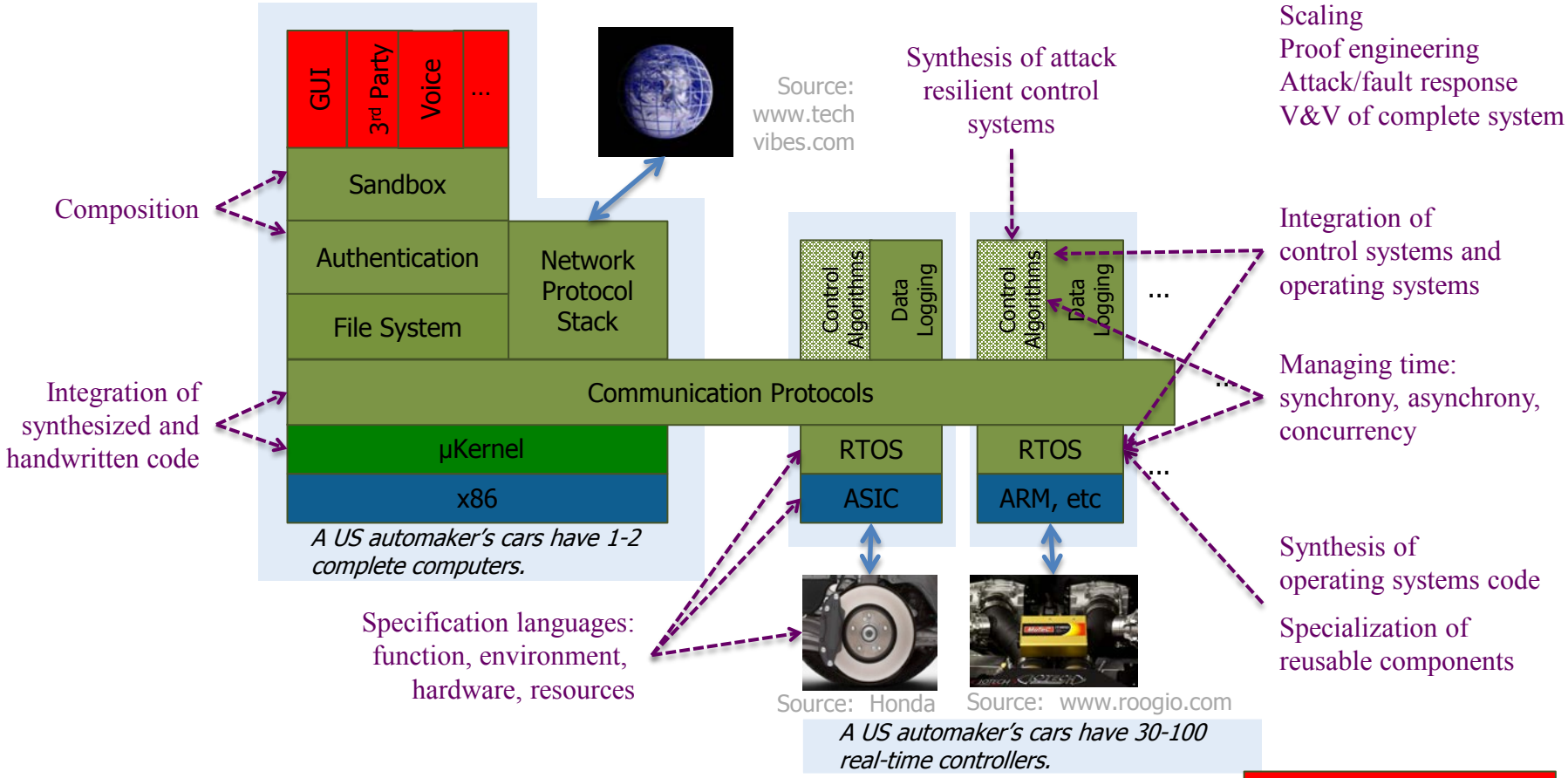
[A] significant part of the effort in existing projects was spent on the further development of verification tools, on formal models for low-level programming languages and paradigms, and on general proof libraries. The sharing of substantial parts of the verification tools between Verisoft and L4.verified demonstrates that there is a significant degree of re-usability... Future efforts will be able to build on these tools and reach far-ranging verification goals faster, better, and cheaper.

Gerwin Klein, *Formal OS Verification—An Overview*.

High-Assurance Vehicle of the Future: Built from Synthesized Components

Research Challenges

Scaling
Proof engineering
Attack/fault response
V&V of complete system



Key:

- Unassured modules
- New assured modules
- Existing assured modules
- Hardware

Focus on vehicles, but techniques will apply to other domains.

Program Structure

- 4.5-year effort split into three 18-month phases
- Five Technical Areas (TAs)
  - TA1 - Military Vehicle Experts
  - TA2 - Formal Methods and Synthesis for OS Components
  - TA3 - Formal Methods and Synthesis for Control Systems
  - TA4 - Research Integration
    - Sub-area 1: Formal-Methods Workbench
    - Sub-area 2: Integration of High-Assurance Components
  - TA5 - Red Team
- Government will group performers of TAs 1-4 into one or more design teams
  - Produce a high-assurance vehicle
  - Performers may participate on more than one team
  - Teams will not be competitively evaluated
  - No anticipated down-selection
- Strong interaction between all participants

Technical Area 1: Military Vehicle Experts

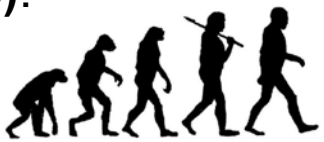
- Identify appropriate defense vehicles

Source: www.militaryfactory.com

Source: www.smartplanet.com

Source: Bluefin Robotics / MBARI

- **Progression**: Single component → multiple components → complete system
- High-assurance version of a key portion of a complex vehicle more persuasive than high-assurance of complete but simple vehicle
- **System evolution (Phase 3)**: demonstrate the use of the tools on multiple versions of the identified vehicles



Source: http://edublogs.org/

- Vehicles and vehicle components higher than SECRET are highly discouraged

Source: http://conservatard.worldpress.com

Source: www.coastappliances.com

- Educate other performers about the technical challenges in producing high-assurance versions of the defense vehicles
- Develop unrestricted and unclassified challenge problems for **Formal Methods and Synthesis** performers
- Apply research results from other TAs to develop high-assurance vehicle
- Provide **Red Team** performer access to functioning original versions of the defense vehicles by month 3 of Phase I

Technical Areas 2/3: Formal Methods and Synthesis

- Develop synthesis tools and formal methods-based techniques for operating system components (TA2) and control systems (TA3)
- **Clean-slate approach**
- Demonstrate tools on challenge problems, and at least one of the open-source platforms, e.g. the LandShark, Ardupilot, or AR Drone

Source: Black-I Robotics

Source: electronicsinfoline.com

Source: Parrot AR Drone

- NOT required to address all research challenges
- May address research challenges other than those mentioned

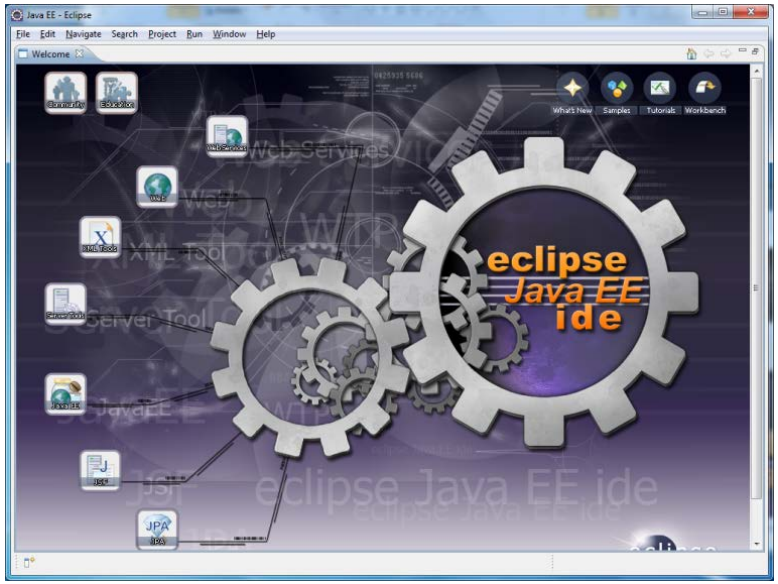
Source: www.coastappliances.com

- Support **Military Vehicle Expert** performers by learning about defense vehicles
- Consult with **Military Vehicle Expert** performers on the application of the developed tools to the defense vehicles
- Work with **Research Integration** performers to incorporate produced tools into a formal-methods workbench

Technical Area 4: Research Integration

(Sub-area: Formal Methods Workbench)

- Integrate tools into a unified Eclipse-like workbench



Source: https://facwiki.cs.byu.edu

- Design appropriate APIs, translators, and/or common representations to enable this integration
- Large research effort, not simply an engineering task

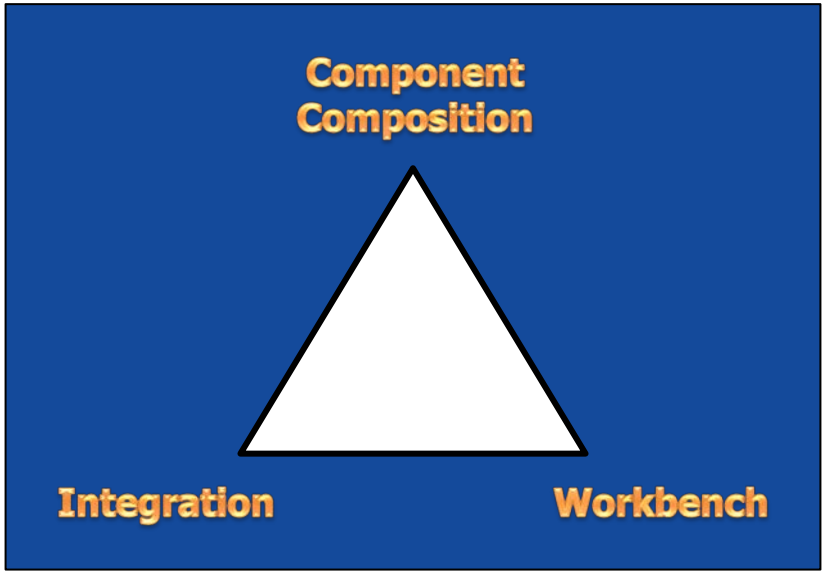
Source: www.coastappliances.com

- Integrate tools developed by **Formal Methods and Synthesis** performers allowing **Military Vehicle Expert** performers and other end users to access all of the tools from a single application

Technical Area 4: Research Integration

(Sub-area: Integration of High Assurance Components)

- Integrate high-assurance components to produce high-assurance composites
- Key technical challenges
  - Understand how to architect components so their composition produces the desired safety and security properties of the composite
  - Develop tools and techniques for coping with different notions of time



Source: www.coastappliances.com

- Support **Military Vehicle Expert** performers by learning about the defense vehicles
- Consult with **Military Vehicle Expert** performers on the application of the developed tools to the defense vehicles
- Integrate high-assurance components developed by **Formal Methods and Synthesis** performers into high assurance versions of the challenge problems and the open-source vehicles.

Technical Area 5: Red Team ("Voice of the Offense")

- Assess security of the targeted vehicles
  - Static and dynamic assessments
  - Baseline security assessment of open-source platforms by month 3 and assessment of defense vehicles by month 6 of Phase I
- Successful Attack
  - Injection of arbitrary code
  - Force sensors to deliver bogus values
  - Prevent users from achieving mission objectives

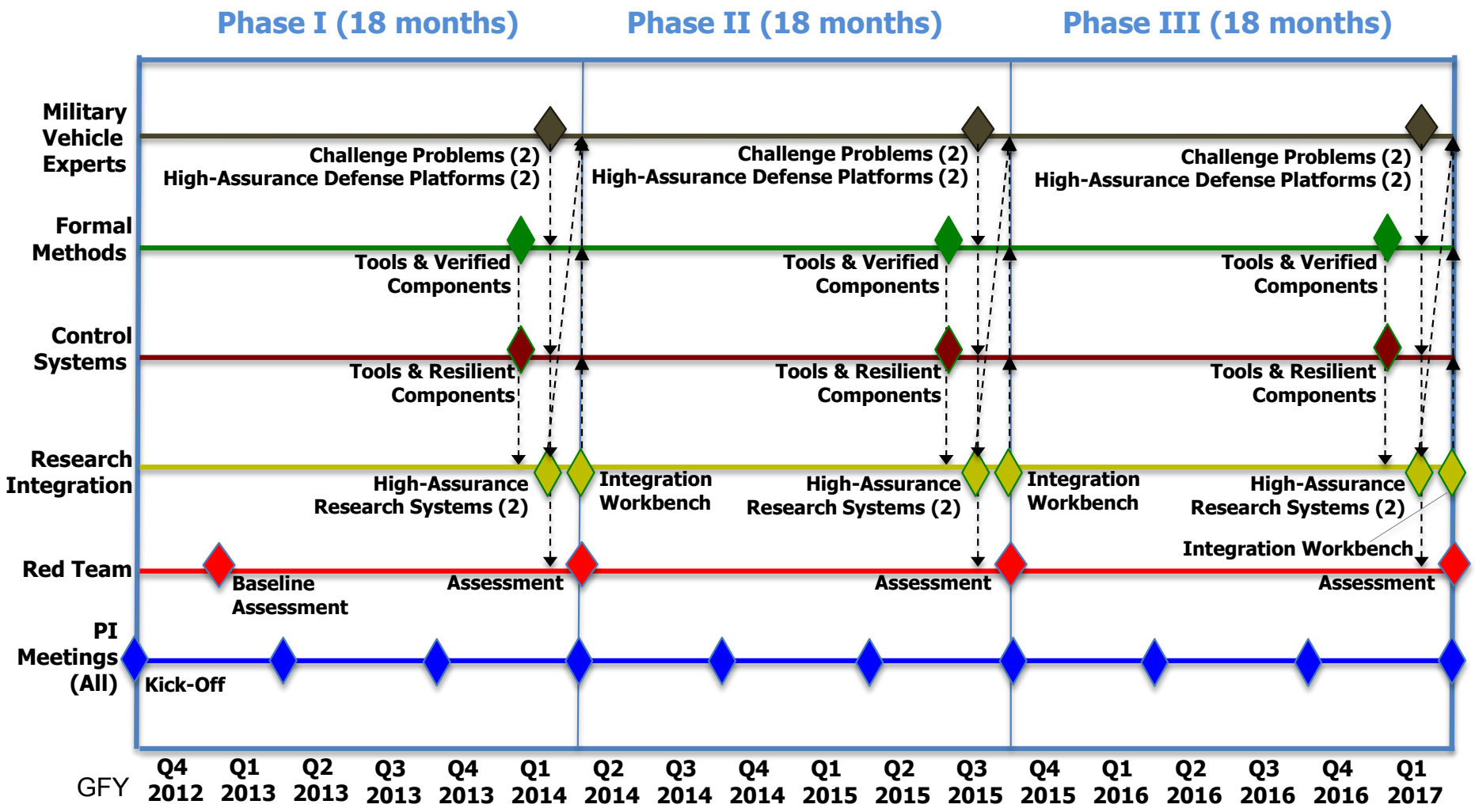
Source: The Telegraph

- Allowed to communicate directly with the control systems if periphery security mechanism fails
- Focus on components built by HACMS performers

Source: www.coastappliances.com

- Work with **other performers** to understand potential security flaws throughout the program
- **TA 1-4 performers** will provide access to functioning, high-assurance versions of the target vehicles at month 17 of each phase
- Produce security assessments by the end of month 18 of each phase.

Putting it all together



Examples of Open-Source Platforms

Source: Black-I Robotics

LandShark UGV

- Developed by Black-I Robotics
- Various payload options
- Linux OS
- Open modular architecture (openJAUS)
- On-board Ethernet connectivity for easy integration of payloads
- External networking available
- Processor: AMD 500 MHz Geode LX800

Source: www.electronicsinfoline.com

ArduPilot UAV

- Developed by DIY Drones
- Based on the Arduino open-source hardware platform
- Complete UAV system: RC aircraft, Arduino-compatible autopilot board, IMU, GPS module, and telemetry kit
- Autopilot board: 16MHz ATMega2560 processor; total onboard processing power ~ 32 MIPS; 256K of flash program memory; 8K of SRAM; and 4K of EEPROM

Source: Parrot AR Drone

AR Drone UAV

- Developed by Parrot
- Front camera, vertical camera, and an ultrasound altimeter
- Connects to external networks using an on-board WiFi system.
- Runs Linux along with AR Drone's open-source software.
- Powered by a 468 MIPS CPU; 256 Mb of RAM; 32Mb of NAND flash memory;