

**Office of the Secretary of Defense (OSD)**  
**Assistant Secretary of Defense (Research & Engineering)**  
**14.1 Small Business Innovation Research (SBIR)**  
**Proposal Submission Instructions**

**Introduction**

The OSD/Assistant Secretary of Defense (Research & Engineering) (OSD/ASD(R&E)) SBIR Program is sponsoring topics in the Autonomous Robotics and Information Assurance/Cybersecurity technology focus areas.

The Army, Navy, and Air Force are participating in the OSD/ASD(R&E) SBIR Program on this solicitation. The Service laboratories act as OSD's Agent in the management and execution of the contracts with small businesses.

In order to participate in the OSD/ASD(R&E) SBIR Program, all potential proposers should register on the DoD SBIR/STTR Web site at <http://www.dodsbir.net/submission> as soon as possible. Follow the instructions for electronic submittal of proposals. It is required that all proposers submit their proposal electronically through the DoD SBIR/STTR Proposal Submission Web site at <http://www.dodsbir.net/submission>. If you experience problems submitting your proposal, call the SBIR/STTR Help Desk (toll free) at: 1-866-724-7457.

Refer to Section 4.15 of the DoD Program Solicitation for the process of submitting questions on SBIR and Solicitation Topics. During the Pre-release period, proposers have an opportunity to contact topic authors by telephone or e-mail to ask technical questions about specific solicitation topics, however, proposal evaluation is conducted only on the written proposal. Contact during the Pre-release period is considered informal, and will not be factored into the selection for award of contracts. Contact with the topic authors by telephone or e-mail after the Pre-release period is prohibited. To obtain answers to technical questions during the formal Solicitation period, please visit <http://www.dodsbir.net/sitis>. Refer to the Program Solicitation for the exact dates.

OSD/ASD(R&E) **WILL NOT accept any proposals that are not submitted through the on-line submission site**. The submission site does not limit the overall file size for each electronic proposal; however, there is a **20-page limit**. File uploads may take a great deal of time depending on your file size and your internet server connection speed. If you wish to upload a very large file, it is highly recommended that you submit your proposal prior to the deadline submittal date, as the last day is heavily trafficked. You are responsible for performing a virus check on each technical volume file to be uploaded electronically. The detection of a virus on any submission may be cause for the rejection of the proposal.

Firms with strong research and development capabilities in science or engineering in any of the topic areas described in this section and with the ability to commercialize the results are encouraged to participate. Subject to availability of funds, the OSD/ASD(R&E) SBIR Program will support high quality research and development proposals of innovative concepts to solve the listed defense-related scientific or engineering problems, especially those concepts that also have high potential for commercialization in the private sector. Objectives of the OSD/ASD(R&E) SBIR Program include stimulating technological innovation, strengthening the role of small business in meeting DoD research and development needs, fostering and encouraging participation by minority and disadvantaged persons in technological innovation, and increasing the commercial application of DoD-supported research and development results. The guidelines presented in the solicitation incorporate and exploit the flexibility of

the SBA Policy Directive to encourage proposals based on scientific and technical approaches most likely to yield results important to DoD and the private sector.

### **Proposal Submission**

Refer to Section 5.0 of the DoD Program Solicitation for program requirements and proposal submission requirements. Proposals shall be submitted in response to a specific topic identified in the following topic description sections. The topics listed are the only topics for which proposals will be accepted. Scientific and technical information assistance may be requested by using the SBIR/STTR Interactive Technical Information System (SITIS).

### **Proposer Eligibility and Limitations**

Each proposer must qualify as a small business for research or research and development purposes and certify to this on the Cover Sheet of the proposal. In addition, a minimum of two-thirds of the research and/or analytical work in Phase I must be carried out by the proposing firm. For Phase II, a minimum of one-half (50%) of the research and/or analytical work must be performed by the proposing firm. The percentage of work is usually measured by both direct and indirect costs, although proposers planning to subcontract a significant fraction of their work should verify how it will be measured with their DoD contracting officer during contract negotiations. For both Phase I and II, the primary employment of the principal investigator must be with the small business firm at the time of the award and during the conduct of the proposed effort. Primary employment means that more than one-half of the principal investigator's time is spent with the small business. Primary employment with a small business concern precludes full-time employment at another organization. For both Phase I and Phase II, all research or research and development work must be performed by the small business concern and its subcontractors in the United States. Deviations from the requirements in this paragraph must be approved in writing by the contracting officer (during contract negotiations).

Joint ventures and limited partnerships are permitted, provided that the entity created qualifies as a small business in accordance with the Small Business Act, 15 U.S.C. § 631.

### **Definition of a Small Business**

A small business concern is one that, at the time of award of Phase I and Phase II, meets all of the criteria established by the Small Business Administration which are published in 13 C.F.R § 121.701-705, repeated here for clarity. A small business concern is one that, at the time of award of Phase I and Phase II, meets all of the following criteria:

- a. Is independently owned and operated, is not dominant in the field of operation in which it is proposing, has a place of business in the United States and operates primarily within the United States or makes a significant contribution to the US economy, and is organized for profit.
- b. Is (1) at least 51% owned and controlled by one or more individuals who are citizens of, or permanent resident aliens in, the United States, or (2) it must be a for-profit business concern that is at least 51% owned and controlled by another for-profit business concern that is at least 51% owned and controlled by one or more individuals who are citizens of, or permanent resident aliens in, the United States.
- c. Has, including its affiliates, an average number of employees for the preceding 12 months not exceeding 500, and meets the other regulatory requirements found in 13 CFR Part 121. Business

concerns are generally considered to be affiliates of one another when either directly or indirectly, (1) one concern controls or has the power to control the other; or (2) a third-party/parties controls or has the power to control both.

Control can be exercised through common ownership, common management, and contractual relationships. The term "affiliates" is defined in greater detail in 13 CFR 121.103. The term "number of employees" is defined in 13 CFR 121.106.

A business concern may be in the form of an individual proprietorship, partnership, limited liability company, corporation, joint venture, association, trust, or cooperative. Further information may be obtained at <http://sba.gov/size> or by contacting the Small Business Administration's Government Contracting Area Office or Office of Size Standards.

### **Description of the OSD SBIR Three Phase Program**

Phase I is to determine, insofar as possible, the scientific or technical merit and feasibility of ideas submitted under the SBIR Program and will typically be one half-person year effort over a period not to exceed six months, with a dollar value up to \$150,000. OSD plans to fund three Phase I contracts, on average, and down-select to one Phase II contract per topic. This is assuming that the proposals are sufficient in quality to fund this many. Proposals are evaluated using the Phase I evaluation criteria, in accordance with Section 6.0 of the DoD Program Solicitation. Proposals should concentrate on research and development which will significantly contribute to proving the scientific and technical feasibility of the proposed effort, the successful completion of which is a prerequisite for further DoD support in Phase II. The measure of Phase I success includes technical performance toward the topic objectives and evaluations of the extent to which Phase II results would have the potential to yield a product or process of continuing importance to DoD and the private sector.

Subsequent Phase II awards will be made to firms on the basis of results from the Phase I effort and the scientific and technical merit of the Phase II proposal in addressing the goals and objectives described in the topic. Phase II awards will typically cover two to five person-years of effort over a period generally not to exceed 24 months (subject to negotiation), with a dollar value up to \$1,000,000. Phase II is the principal research and development effort and is expected to produce a well defined deliverable prototype or process. A more comprehensive proposal will be required for Phase II. In order for a small business to be considered for a Phase II award, the firm must be a recipient of a Phase I award under that topic.

All Phase I awardees will be allowed to submit a Phase II proposal for evaluation and selection. The details on the due date, content, and submission requirements of the Phase II proposal will be provided by the awarding technical point of contact and/or the contracting officer by subsequent notification. All SBIR Phase II awards made on topics from solicitations prior to FY2013 will be conducted in accordance with the procedures specified in those solicitations (this means by invitation only).

Under Phase III, the DoD may award non-SBIR funded follow-on contracts for products or processes, which meet the Component mission needs. This solicitation is designed, in part, to encourage the conversion of federally sponsored research and development innovation into private sector applications. The small business is expected to use non-federal capital to pursue private sector applications of the research and development.

DoD is not obligated to make any awards under Phase I, II, or III. For specifics regarding the evaluation and award of Phase I or II contracts, please read the front section of this solicitation very carefully. Phase II proposals will be reviewed for overall merit based upon the criteria in Section 4.3 of this solicitation.

This solicitation is for Phase I proposals only. Any proposal submitted under prior SBIR solicitations will not be considered under this solicitation; however, offerors who were not awarded a contract in response to a particular topic under prior SBIR solicitations are free to update or modify and submit the same or modified proposal if it is responsive to any of the topics listed in this section.

### **Phase II Plus Program**

The OSD/ASD(R&E) SBIR Program has a Phase II Plus Program, which provides matching SBIR funds to expand an existing Phase II contract that attracts investment funds from a DoD acquisition program, a non-SBIR/non-STTR government program or Private sector investments. Phase II Plus allows for an existing Phase II OSD/ASD(R&E) SBIR contract to be extended for up to one year per Phase II Plus application, to perform additional research and development. Phase II Plus matching funds will be provided on a one-for-one basis up to a maximum \$500,000 of SBIR funds. All Phase II Plus awards are subject to acceptance, review, and selection of candidate projects, are subject to availability of funding, and successful negotiation and award of a Phase II Plus contract modification. The funds provided by the DoD acquisition program or a non-SBIR/non-STTR government program must be obligated on the OSD Phase II contract as a modification just prior to or concurrent with the OSD/ASD(R&E) SBIR funds. Private sector funds must be deemed an “outside investor” which may include such entities as another company, or an investor. It does not include the owners or family members, or affiliates of the small business (13 CFR 121.103).

### **Follow-On Funding**

In addition to supporting scientific and engineering research and development, another important goal of the program is conversion of DoD-supported research and development into commercial (both Defense and Private Sector) products. Proposers are encouraged to obtain a contingent commitment for follow-on funding prior to Phase II where it is felt that the research and development has commercialization potential in either a Defense system or the private sector. Proposers who feel that their research and development has the potential to meet Defense system objectives or private sector market needs are encouraged to obtain either non-SBIR DoD follow-on funding or non-federal follow-on funding, for Phase III to pursue commercialization development. The commitment should be obtained during the course of Phase I performance, or early in the Phase II performance. This commitment may be contingent upon the DoD supported development meeting some specific technical objectives in Phase II which if met, would justify funding to pursue further development for commercial (either Defense related or private sector) purposes in Phase III. The recipient will be permitted to obtain commercial rights to any invention made in either Phase I or Phase II, subject to the patent policies stated elsewhere in this solicitation and awarded contract.

The following pages contain a summary of the technology focus areas, followed by the topics within each focus area.

## **Autonomy Test, Evaluation, Validation, and Verification**

The Department's investments in Autonomy focus on developing systems that will allow performing complex military missions in dynamic environments with the right balance of warfighter involvement. To implement such capabilities, the Department has established four technical areas of focus for investment in Autonomy: Human and Agent System Interaction and Collaboration (HASIC); Scalable Teaming of Autonomous Systems (STAS); Machine Reasoning and Intelligence (MRI); and Test, Evaluation, Validation, and Verification (TEVV). TEVV is the area within Autonomy that will benefit from additional both investment and technology advancement. This SBIR/STTR theme in TEVV in Autonomy is intended to investigate fundamental methodology such as algorithms, paradigms, platform, and architectures to implement. These topics are supported under the National Robotics Initiatives (NRI).

The following topics in this theme are:

- OSD14.1-AU1 Biometrics for Human-machine Team Feedback in Autonomous Systems
- OSD14.1-AU2 Evaluating the Performance and Progress of Learning-enabled Systems
- OSD14.1-AU3 Evaluating Mixed Human/Robot Team Performance
- OSD14.1-AU4 Safety Testing for Autonomous Systems in Simulation
- OSD14.1-AU5 Distributed Visual Surveillance for Unmanned Ground Vehicles

### **Information Assurance: Research to Enable Secure and Effective Operations in the Cyber Domain**

The cyber realm has emerged as a domain of battle where the DoD faces sophisticated and persistent adversaries pursuing strategic goals, rather than monetary gains or harassment. Even when no outward conflict is occurring, cyber adversaries may be exploiting our systems to gather information and position themselves for advantage in longer-term campaigns.

The challenge for research in cyber operations and security is to develop techniques for operating successfully in this threatened cyber environment, and to reduce or reverse the asymmetry. Techniques, models, and tools are needed that allow cyber systems to accomplish their missions, with the assumption of partial compromise, though the attacks that inflicted it may have gone undetected. Networked systems must persevere, contain effects of incursions, blunt and frustrate attacks, and allow us to hunt and isolate adversaries within our networks, at Internet speeds.

The following topics in this theme are:

- OSD14.1-IA1 Obfuscation to Thwart Un-Trusted Hardware
- OSD14.1-IA2 Detecting Malicious Circuits in IP-Core

## OSD SBIR 14.1 Topic Index

OSD14.1-AU1	Biometrics for Human-machine Team Feedback in Autonomous Systems
OSD14.1-AU2	Evaluating the Performance and Progress of Learning-enabled Systems
OSD14.1-AU3	Evaluating Mixed Human/Robot Team Performance
OSD14.1-AU4	Safety Testing for Autonomous Systems in Simulation
OSD14.1-AU5	Distributed Visual Surveillance for Unmanned Ground Vehicles
OSD14.1-IA2	Detecting Malicious Circuits in IP-Core
OSD14.1-IA1	Obfuscation to Thwart Un-Trusted Hardware

## OSD SBIR 14.1 Topic Descriptions

OSD14.1-AU1                      TITLE: Biometrics for Human-machine Team Feedback in Autonomous Systems

TECHNOLOGY AREAS: Information Systems, Materials/Processes, Biomedical, Human Systems

This topic is supported under National Robotics Initiatives (NRI).

OBJECTIVE: Develop and use biometrics that provides feedback about the status of human-machine team in autonomous systems.

DESCRIPTION: Intense workload and short deadlines place a great deal of stress on warfighters applying computer systems to complete their mission. Biometric techniques show promise for detecting variations in human workload, stress, fatigue, and engagement when these systems are in the testing and evaluation stages of development (Bonner & Wilson, 2002; Murai, Okazaki, & Hayashi, 2004; Hockey, Gaillard, & Burov, 2004). Health monitoring systems could use biometric data collected to make informed decisions about the human operator's condition (Carter, Chevront, Sawka, 2004). Having detected these factors, the software could provide a human impairment profile to better address the human's interaction with the proposed autonomous system. The new sensors must minimize interference with the warfighter's ability to complete the testing sessions or mission. For example the sensors cannot require excessive apparatus or a lengthy calibration training period.

Both psychophysiology and affective computing have explored many avenues of research, including speech, facial expressions, gestures, central nervous system responses and autonomic nervous system responses (Zeng et al., 2009; Calvo and D'Mello, 2010). Among these, autonomic nervous system (ANS) responses such as cardiorespiratory and electrodermal responses hold a great deal of promise in physiological computing since they can be measured more cheaply, quickly and unobtrusively than central nervous system responses.

PHASE I: Identify or design sensors that can unobtrusively monitor human operators for human state assessment with a quantifiable impact on task performance. Design a sensor system and provide proof-of-concept supporting data on the ability of said design to accurately assess the cognitive state of engineers during test activities.

PHASE II: Prototype the designed sensor system. Demonstrate that sensor information improves human operator cognitive state assessment and can lead to improved performance and productivity during test engineering activities. Develop prototype mobile application to facilitate the cognitive state assessment in operational environments.

PHASE III: Fully developed cognitive state assessment systems that have numerous applications relevant to the Department of Defense, especially where fatigue or information overload are responsible for elevated error rates. Industry applications include operation and safety in areas such as transportation, energy and medicine.

### REFERENCES:

1. Bonner, M. A., & Wilson, G. F. (2002). Heart rate measures of flight test and evaluation. *International Journal of Aviation Psychology*, 12, 63-77.
2. Carter, R. Chevront, S.N., Sawka, M.N. (2004) Operator Functional State Assessment. Technical Report Prepared by the North Atlantic Treaty Organization (NATO) Research and Technology Organization (RTO) Human Factors and Medicine Panel (HFM) Task Group HFM-056/TG-008.
3. Hockey, G.R.J., Gaillard, A.W.K., & Burov, A.Yu. (2004). Operator Functional State and Impaired Performance in Complex Work. NATO ASI Series, Series A, Life Sciences, New York: Plenum.
4. Murai, K., Okazaki, K., & Hayashi, Y. (2004, April). Measurement for mental workload of bridge team on leaving/entering port. Paper presented at the 2004 IEEE Position, Location, and Navigation Symposium, Monterey, CA.

5. Zeng, Z., Pantic, M., Roisman, G.I., Huang, T.S., 2009. A survey of affect recognition methods: audio, visual and spontaneous expressions. IEEE Transactions on Pattern Analysis and Machine Intelligence, 39–58.
6. Calvo, R.A., D’Mello, S., 2010. Affect detection: an interdisciplinary review of models, methods and their applications. IEEE Transactions on Affective Computing 1, 18–37.

KEYWORDS: T&E, Cognitive Assessment, biometric, human performance

OSD14.1-AU2                      TITLE: Evaluating the Performance and Progress of Learning-enabled Systems

TECHNOLOGY AREAS: Information Systems, Materials/Processes

This topic is supported under National Robotics Initiatives (NRI).

OBJECTIVE: Develop methodology to evaluate and measure the performance and progress for learning –enabled systems.

DESCRIPTION: A long term goal of machine learning is to develop systems that learn complex behaviors with minimal human oversight. However, future systems that incorporate learning strategies will not necessarily have a fixed software state that can be evaluated by the testing community. In some cases, most of the training occurs in the development process using large databases of training examples. Testing may involve a series of challenge scenarios, similar to the DARPA autonomous mobility challenges, designed to examine the performance of the system-under-test in relevant conditions. Design of the scenarios and performance metrics are open research questions.

As autonomous systems are used in increasingly complex scenarios, supervised training during the development phase, by itself, may not be sufficient to allow the system to learn the appropriate behavior. Learning from demonstration uses examples, often supplied by the end-user of the system, to train the system. Examples include flying in specific environments, bi-pedal locomotion on different terrain surfaces and, throwing objects of different sizes or densities. In this case, the tester needs to stand in for the end user and “train” the systems before testing it. Test procedures need to evaluate not only the performance of the system in various scenarios, but the amount of time it takes to train the system and the required level of expertise for the “expert” trainer.

Finally, some applications include continuously adapting models that adjust over time to compensate for changes in the environment or mission. Current research is exploring the use of on-line learning in areas such as terrain adaptive mobility and perception. This case presents a particularly challenging evaluation problem, performance in a given scenario is not static – it may improve over time.

In this solicitation we seek a methodology that answers the following three questions:

- a) What is an appropriate testing methodology for learning-enabled systems? This includes testing procedures that apply to systems with supervised learning components, as well as user-trained or continuously adapting systems.
- b) Are there general testing principles that can be applied to learning-enabled systems regardless of the specific applications?
- c) Can we predict the evolution of a learning-enabled system over time? For adaptive systems, can we predict how much time is required to adapt to a new environment? What are the potential impacts on military autonomous systems?

PHASE I: The first phase consists of initial methodology development, metrics and a set of use cases to evaluate and measure the performance of learning-enabled systems. This methodology must address supervised, re-trained and continuously adaptive systems. Documentation of the methodology and use cases is required in the final report.

PHASE II: Prototype the methodology by using it to examine test cases for each type of learning-enabled system in simulated test environments. The prototypes should address the 3 questions states above. Deliverables shall

include the prototype system and a final report, which shall contain documentation of all activities in the project and a user's guide and technical specifications for the prototype system.

PHASE III: Fully developed systems that evaluate the performance learning-enabled systems in either real or simulated scenarios. Potential commercial applications could be a system that to assess the performance of autonomous driving systems, logistics systems, and autonomous UAV applications such as power line inspection in which the UAV must adapt its flight parameters to changing wind characteristics. Deliverables shall include the methodology, test case scenarios and some general principles that the test and evaluation community can use to develop test procedures for specific systems.

#### REFERENCES:

1. Bengio, Yoshua, and Yann LeCun. "Scaling learning algorithms towards AI." *Large-Scale Kernel Machines* 34 (2007).
2. Caruana, Rich, and Alexandru Niculescu-Mizil. "An Empirical Comparison of Supervised Learning Algorithms."
3. Erhan, Dumitru, et al. "Why does unsupervised pre-training help deep learning?." *The Journal of Machine Learning Research* 11 (2010): 625-660.
4. Ngiam, Jiquan, et al. "On optimization methods for deep learning." *Proceedings of the 28th International Conference on Machine Learning (ICML-11)*. 2011.
5. Vasquez, Dizan, et al. "Intentional motion on-line learning and prediction." *Machine Vision and Applications* 19.5-6 (2008): 411-425.
6. Zhou, Shengyan, and Karl Iagnemma. "Self-supervised learning method for unstructured road detection using fuzzy support vector machines." *Intelligent Robots and Systems (IROS), 2010 IEEE/RSJ International Conference on*. IEEE, 2010.

KEYWORDS: Learning-enabled systems, supervised and unsupervised learning

OSD14.1-AU3

TITLE: Evaluating Mixed Human/Robot Team Performance

TECHNOLOGY AREAS: Information Systems, Materials/Processes, Human Systems

This topic is supported under National Robotics Initiatives (NRI).

OBJECTIVE: Develop methodology to evaluate mixed human/robot team performance

DESCRIPTION: Introducing robotic assets to a military or civilian unit should increase the level of performance for the team. We evaluate human teams by scoring their performance on specific tasks; they can be a single score for the team, or an aggregate of individual member scores. Likewise, we need to extend this idea to tasks performed by mixed teams. The conceptual team can be a single human acting as "robot operator or handler" and a single robot. However, of equal important is the team of multiple humans with one or more robots. Evaluation of the human component performance, the robot component performance, and the mixed team performance is critical in both T&E settings, where meeting performance thresholds will be key, as well as research environments where identification of weaknesses will assist in advancing the technology. Unfortunately, evaluation of a mixed human/robot team performance is much more complicated and complex than a human only team evaluation. In addition, mission space of a mixed human/robot team may be different than that of a human only team – in some ways the mission space may be more limited (e.g., terrain may limited robot mobility); in other ways, the mission space may be expanded (e.g., through additional sensor capabilities).

There is a wide range of scenarios in which human-robot teams may increase overall mission performance. Some examples of possible scenarios include some combat operations (both mounted and dismounted) such as

reconnaissance; installation personnel transport; construction; road clearance; logistics; and, medical evacuation. These scenarios will require certain tasks to be performed by the human-robot team members, in various environments, to certain expected levels of performance.

In this solicitation, we are looking for a methodology and/or algorithm that can answer the following three questions:

- a) What are appropriate lists of tasks, in what environments, for a mixed human/robot team? This would include defining different kinds of military or civilian human/robot teams, with differing capabilities, and expected performance characteristics?
- b) Are there techniques/methodologies that can evaluate the performance of the robotic asset(s) within the team mission? Are there techniques/methodologies that can evaluate the combined performance of robots and humans in the team mission?
- c) How does performance on scenario-based task/environment/capability combinations relate to additional, new combinations (can we use the techniques/methodologies to establish performance envelopes across a range of scenarios and unmanned systems?)

**PHASE I:** Determine the feasibility of developing a methodology and/or algorithm to evaluate and measure a mixed human/robot team performance. From the scenarios above (or identify others) where human-robot teams are likely to increase mission effectiveness, choose two to three scenarios to use as developmental scenarios. Within the chosen scenarios: 1) Identify potential military human/robot team characteristics, 2) identify possible tasks that the robot/human/team will perform (both scenario/mission specific and general/universal), 3) define environment characteristics that will impact robot/human/team performance, and identify potential and appropriate robot/human/team performance measurement metrics. From this large matrix space (scenario/team/task/environment/metrics), identify one or more methodologies and/or algorithms for assessing mixed human/robot team performance. Documentation of methodology tradeoffs and projected methodology strengths and weaknesses shall be required in the final report.

**PHASE II:** Define in detail and prototype the methodology(ies) and/or algorithm(s). Test the methodology(ies) and or algorithm(s) in real or simulated scenarios, with particular attention to validated (or defensibly appropriate) models of robot and human performance. Demonstrate the feasibility of the answers to the above three questions. Define methods to valid the solution set. Show applicability across a range of scenarios (i.e., not just the scenarios chosen in Phase I). In addition, the final product of Phase II should be able to evaluate and compare team performance between a human only team and a mixed human/robot team. Deliverables shall include the prototype methodology(ies) and/or algorithms and a final report, which shall contain documentation of all activities in the project and detailed instructions for using the prototype approach.

**PHASE III:** The final product is expected to be fully developed systems that can evaluate the performance of any combination of human only teams and mixed human/robot teams. Potential military applications would be by the Test and Evaluation community for use in determining the performance envelope of candidate systems or in the research community for use in describing performance in R&D. Potential commercial applications could be for robotic systems developed to assess performance during system development across a range of applications or by commercial enterprises interested in developing and assessing autonomous driving.

#### REFERENCES:

1. Finn, A., Jacoff, A., Del Rose, M., Kania, B., Overholt, J., Silva, U. and Bornstein, J. (2012), Evaluating autonomous ground-robots. *J. Field Robotics*, 29: 689–706. doi: 10.1002/rob.21433  
<http://onlinelibrary.wiley.com/doi/10.1002/rob.21433/full>
2. Schreckenghost, Fong, Utz, Milam (2009). Measuring robot performance in real-time for NASA robotic reconnaissance operations., *PerMIS'09, Proceedings of the 9th Workshop on Performance Metrics for Intelligent Systems*, 194-202. <http://dl.acm.org/citation.cfm?id=1865950>
3. SM Singer and DL Akin (2011). 41st International Conference on Environmental Systems, A Survey of Quantitative Team Performance Metrics For Human-Robot Collaboration (doi: 10.2514/6.2011-5248)

4. Singer, SM (2012) Creating an Objective Methodology for Human-Robot Team Configuration Selection. Dissertation from Univeristy of Maryland. <http://hdl.handle.net/1903/13539>
5. A. Steinfeld, T. Fong, D. Kaber, M. Lewis, J. Scholtz, A. Schultz, and M. Goodrich, "Common metrics for human-robot interaction," 1st ACM SIGCHI/SIGART conference on Human-robot interaction, Salt Lake City, Utah, USA, pp. 33-40, 2006.
6. R. Murphy and D. Schreckenghost (2013) Survey of metrics for human-robot interaction. 2013 8th ACM/IEEE International Conference on Human-Robot interaction (HRI), pp. 197-198.

KEYWORDS: human/robot, measuring performance

OSD14.1-AU4

TITLE: Safety Testing for Autonomous Systems in Simulation

TECHNOLOGY AREAS: Information Systems, Materials/Processes, Human Systems

This topic is supported under National Robotics Initiatives (NRI).

OBJECTIVE: The Army is interested in adding autonomy to its vehicle convoys [1], but how can we certify that these autonomous algorithms are safe? Currently, live testing of full vehicle systems is the only acceptable method, but even after hundreds of hours of successful live testing, a single hidden failure point in the algorithms would disprove the hypothesis that the proposed autonomous system is safe. Furthermore, live testing can be cost prohibitive, and is (not surprisingly) far from exhaustive. Instead, we seek to develop a safety testing environment (STE) that will exercise our current autonomy algorithms with software/hardware in the loop in parallel with live testing that will validate the STE.

DESCRIPTION: Recent advancements in sensor simulation tools [2] have improved our ability to model radar, lidar, camera, and GPS with software/hardware in the loop. Of course, our ability to model the physics of heavy trucks [3] is quite mature as well. To address the challenge of developing the STE, we will provide our autonomy algorithms as Government Furnished Equipment (GFE).

The focus of this topic is: 1) to build an environment that mirrors actual test data to provide a departure point for Monte Carlo simulations. 2) research the failure modes for autonomy algorithms within the capabilities of current sensor models and 3) simulate the corner cases that would exercise these failure modes.

This topic is not focused on improving physics-based simulation of heavy trucks or building better sensor models. Neither do we seek to develop new algorithms for autonomous behavior, but rather to leverage existing GFE autonomy algorithms to study the open research question of how we can test these algorithms in simulation, and certify that they are safe to the fullest extent possible within current simulation environments.

PHASE I: In Phase I we seek a System Architecture for the Safety Testing Environment (STE). This prototype STE may be outlined with cursory autonomy algorithms rather than with the GFE algorithms. Define sensor models, processor and software requirements. Propose metrics for highlighting the impact and reliability of the STE. Provide a detailed concept of operations (CONOPS) and overview (OV) graphics.

PHASE II: Integrate GFE algorithms into a fully functional STE of an operationally relevant scenario such collision mitigation braking, adaptive cruise control, or lane departure, etc. We desire a model of a M915 or Marine Corps AMK23 Cargo Truck for the STE. Demonstrate the effectiveness of this STE within the metrics defined in Phase I. The STE should be able to simulate ambient noise, sunlight, occlusions between the following and leading vehicle and fully simulate radar, lidar, camera and GPS. The objective is a full military environment.

PHASE III: Work to have the proposed system become a part of the AMAS program.

REFERENCES:

[1] <http://www.unmannedsystemstechnology.com/2012/10/lockheed-martin-wins-contract-to-develop-autonomous-operation-of-tactical-vehicles/>

[2] <https://www.tassinternational.com/prescan>

[3] <http://www.carsim.com/products/index.php>

**KEYWORDS:** Autonomous Mobility Appliqué System, safety testing environment (STE), simulation, Safety Testing, Autonomy, Hardware in the loop, Vehicle to Vehicle, Connected Driving

OSD14.1-AU5

**TITLE:** Distributed Visual Surveillance for Unmanned Ground Vehicles

**TECHNOLOGY AREAS:** Information Systems, Ground/Sea Vehicles, Sensors

This topic is supported under National Robotics Initiatives (NRI).

**OBJECTIVE:** Develop a system to identify, classify, and analyze visual data from unmanned ground vehicles and stationary visual surveillance sources to enable real-time on-board decisions and system-wide planning regarding route, speed, and tasks.

**DESCRIPTION:** Distributed visual surveillance has a major role in the future of Unmanned Ground Vehicles (UGV's). Distributed visual surveillance refers to the use of cameras networked over a wide area to continually collect and process sensor data to recognize and classify objects in the environment. Analyzed data will inform unmanned decision-making and fleet management to optimize a transportation system. Sensors and camera systems mounted on UGVs will augment stationary surveillance hardware. An area of interest for this research is data fusion, co-operative multi-sensor tracking methods, and distributed processing. Also of interest is the reconciliation, classification, and prioritization of data; storage and accurate retrieval of archival references; and the selection of an appropriate action/response to the data.

Although there are many potential sensors that can be used in distributed surveillance, in this topic we are focusing on visual (and perhaps infrared) imaging sensors whose cost, reliability, and availability makes transition to the field or commercialization much more likely. Communications bandwidth is and will remain a limited resource. Even with video compression technologies, there is insufficient bandwidth to upload all video and high-resolution still images from all network nodes. Artifacts due to heavy video compression would degrade most analysis applications and viewing all the data would overwhelm analysts. Local processing is therefore preferable to central processing to extract actionable information from the sensor data and to plan UGV position adjustments. An individual node can determine whether or not there has been a significant change in the situation that would warrant transmitting a package of sensor-level data.

The scenario to be addressed in this topic is that a small fleet of 10-15 UGVs deployed at a CONUS installation in order to safely transport personnel, on-demand, from various point around one building one-third mile sharing pedestrian sidewalk, across an uncontrolled four-lane roadway, through a busy parking lot to another building on the installation. Vehicles will operate at speeds from 3mph (in mixed pedestrian traffic) up to potentially 25mph which is the limit for Neighbourhood Electric Vehicles. Vehicles must recognize and respond appropriately to pedestrians, unconnected vehicles, and other environmental objects. Approximately 12 networked cameras fixed across along the route and around the test site will provide visual coverage of the area. Sensors will have a priori visual background data and UGV location will be known (landmarks, GPS positioning, etc.) enabling temporal differential or background subtraction to locate objects. Capabilities desired for the UGV include ODOA, correct positioning and speed regulation with respect to moving and stationary objects, coordinated and optimized system-wide responses across the fleet, data collection and/or communications, and extracting actionable information from the sensor stream. Information of interest includes detection and behaviour analysis of humans and vehicles, analysis of traffic patterns, and identification of suspicious activities or behaviors. The intended platform is an electric vehicle with size on the order of 500-600 Kg (roughly golf-cart sized). The platform is expected to manage its own energy

usage and recharge itself, wirelessly, so energy efficient algorithms are of interest. UGV platform and payload development, including sensors and communications, are outside the scope of this topic.

PHASE I: The first phase consists of scenario/capability selection, initial system design, researching sensor options, investigating signal and video processing algorithms, and showing feasibility on sample data. Documentation of design tradeoffs and projected system performance shall be required in the final report.

PHASE II: The second phase consists of a final design and full implementation of the system, including sensors and UGV software. At the end of the contract, a database of behavioural characteristics will be available enabling both improved M&S and T&E as well as improved autonomous local maneuvering shall be demonstrated in a realistic outdoor environment. Deliverables shall include the prototype system and a final report, which shall contain documentation of all activities in the project and a user's guide and technical specifications for the prototype system.

PHASE III: The end-state of this research is to further develop the prototype system and potentially transition the system to the field or for use on military installations and bases. Potential military applications include monitoring highways, overpasses, intersections, buildings and security checkpoints. Potential commercial applications include monitoring high profile events, border security and commercial and residential surveillance. The most likely path for transition of the SBIR from research to operational capability is through collaboration with robotic companies from industry or through collaboration with the Robotic Systems Joint Project Office (RS JPO).

#### REFERENCES:

1. <http://ieeexplore.ieee.org/stamp/stamp.jsp?tp=&arnumber=1425326> (Intelligent distributed surveillance systems: a review)
2. <http://mac.sagepub.com/content/35/7/209.short> (A Distributed Surveillance System for Improving Security in Public Transport Networks)
3. [http://ieeexplore.ieee.org/xpl/login.jsp?tp=&arnumber=1068001&url=http%3A%2F%2Fieeexplore.ieee.org%2Fxppls%2Fabs\\_all.jsp%3Farnumber%3D1068001](http://ieeexplore.ieee.org/xpl/login.jsp?tp=&arnumber=1068001&url=http%3A%2F%2Fieeexplore.ieee.org%2Fxppls%2Fabs_all.jsp%3Farnumber%3D1068001) (Distributed surveillance and reconnaissance using multiple autonomous ATVs: CyberScout)
4. [www.sciencedirect.com/science/article/pii/S0031320303004114#](http://www.sciencedirect.com/science/article/pii/S0031320303004114#) (Distributed intelligence for multi-camera visual surveillance)
5. [www.sciencedirect.com/science/article/pii/S1084804506000439](http://www.sciencedirect.com/science/article/pii/S1084804506000439) (A network of sensor-based framework for automated visual surveillance)
6. <http://www.dtic.mil/srch/doc?collection=t3&id=ADA497188> (Automated Knowledge Generation with Persistent Surveillance Video)
7. <http://www.ee.washington.edu/research/nsl/papers/iscas-08.pdf> (Human Activity Recognition for Video Surveillance)
8. [http://www.robots.ox.ac.uk/~lav//Publications/robertson\\_reid\\_cviu2006/robertson\\_reid\\_cviu2006.pdf](http://www.robots.ox.ac.uk/~lav//Publications/robertson_reid_cviu2006/robertson_reid_cviu2006.pdf) (A General Method for Human Activity Recognition in Video)
9. <http://mha.cs.umn.edu> (Monitoring Human Activity)

KEYWORDS: robotics, surveillance, autonomy, image processing, ground vehicle, human activity

OSD14.1-IA2

TITLE: Detecting Malicious Circuits in IP-Core

TECHNOLOGY AREAS: Information Systems

**OBJECTIVE:** Develop technologies and tools for detecting potential malicious/backdoor logics in hardware IP-core, toward reducing supply-chain vulnerability in embedded computing and system on chip environment.

**DESCRIPTION:** This topic solicits the development of technologies and tools which perform analysis on gate-level netlist of hardware IP-core to identify potentially malicious wires and logics, related to hardware backdoors. Compromise at hardware level is very powerful, difficult to detect and generally not addressable via software running on it. The solicited tool can be used to screen, detect and disqualify components/IP-cores which contain backdoor circuitry.

Tactical computing devices often rely on the system-on-chip embedded computing hardware commonly found in embedded computing devices, often used in mobile computing and networking appliances, as the underlying processing infrastructure. Modern large and complex embedded and system-on-chip (VLSI/FPGA circuit) design often integrates large number of pre-designed components, acquired from third parties. These IP-core components are generally delivered as gate-level netlist. Currently, there is no practical way to ensure that these third party components (IP-cores) do not contain any backdoor or malicious circuitry, which can stealthily compromise the design (system) after deployment. Compromise circuitry embedded within the hardware is generally very hard to detect and defeat.

State of the art methodology for verifying VLSI design includes running unit test on the individual component, as well as performing comprehensive regression test on the full-chip (VLSI) design. However, these tests can only address functionality described in the specifications. They rarely uncover the stealthy, out-of-specification malicious logics, which can only be triggered (activated), by hidden, rare and very-specific occasions. A new approach is needed to uncover these elusive circuits.

If successful, the tools developed in this SBIR can be used to screen these third party IP-cores to ensure that they do not contain any backdoor/malicious logic. They prevent compromised IP-cores from being integrated into the design and enhance the security of the system.

**PHASE I:** Investigate and develop creative methods, techniques for reliably discovering malicious/backdoor logics in hardware IP-core, normally delivered in the form of gate-level-netlist. Develop proof of concept prototype and identify the metrics that determine the prototype's efficacy.

**PHASE II:** Develop and enhance the prototype into a fully functioning tool. Demonstrate and evaluate the capability of the tool on actual (real world scale) set of benign IP-Cores and IP-cores with malicious-circuit/ backdoor.

**PHASE III DUAL USE APPLICATIONS:** Inclusion of third party IP-cores is a common practice in system-on-chip design and development in private sector and in military industry. These SOCs hardware have been the backbones for embedded and mobile computing devices in the commercial sector as well as in the military uses. System-on-chip (SOC) hardware (semiconductors) is widely used in commercial application such as network appliances and mobile computing. Security and financial motive for the insertion malicious circuits exists in these applications. Commercial chip provider/manufacturers have interest for ensuring that their product is free of malicious circuits. If successful the tool developed within this SBIR should find its market in the commercial sector as well as military sector.

#### REFERENCES:

1. D. Agrawal, S. Baktir, D. Karakoyunlu, P. Rohatgi, and B. Sunar. Trojan Detection using IC Fingerprinting. In Security and Privacy, 2007. SP '07. IEEE Symposium on, pages 296 –310, may 2007.
2. S. T. King, J. Tucek, A. Cozzie, C. Grier, W. Jiang, and Y. Zhou. Designing and implementing malicious hardware. In Proceedings of the 1st Usenix Workshop on Large-Scale Exploits and Emergent Threats, pages 5:1–5:8, Berkeley, CA, USA, 2008. USENIX Association.
3. S. Rowley, S. Thorne, A. Bousetta, C. Perry, and C. Dutton. Comparative study of two kla-tencor advanced patterned wafer inspection systems. In Advanced Semiconductor Manufacturing Conference and Workshop, 2000 IEEE/SEMI, page 141, 2000.

4. M. Tehranipoor and F. Koushanfar. A Survey of Hardware Trojan Taxonomy and Detection. Design Test of Computers, IEEE, 27(1):10-25, Jan.-Feb. 2011

5. Waksman and S. Sethumadhavan. Silencing hardware backdoors. In Proceedings of the 2011 IEEE Symposium on Security and Privacy, SP '11, pages 49–63, Washington, DC, USA, 2011. IEEE Computer Society.

KEYWORDS: hardware IP-core; gate-level netlist; system-on-chip; malicious logic

OSD14.1-IA1

TITLE: Obfuscation to Thwart Un-Trusted Hardware

TECHNOLOGY AREAS: Information Systems

OBJECTIVE: To develop innovative methods for mutating or obfuscating the processes of network security appliances or tactical communication systems. To make the path of the processes and data through hardware non deterministic, thereby thwarting any supply chain attacks that rely on the deterministic nature of computing to exfiltrate data and compromise operations. To mask the data and processes such that information exfiltrated from compromised hardware is not useful to an adversary.

DESCRIPTION: With more and more of the hardware that the U.S. Army relies on for critical communications and security being manufactured in whole or in part in countries not sympathetic to the goals of this Nation, supply chain tampering is of a greater and greater concern. Tampering with components as they are produced can have catastrophic effect. From a security perspective, the possibility of supply chain attacks undermines the trust that can be placed on a system. Supply chain attacks can involve the insertion of hardware modules or embedded code into hardware devices. These insertions can exfiltrate data or allow backdoor access into systems by the parties responsible for their insertion. Detecting these insertions is costly and difficult, especially with many components coming from many places; all of which could have any of these types of insertions. These inserted modules rely on the user being unaware of their presence, and performing tasks in a predictable manner.

The aspect of a predictable manner is very important to the developers of the supply chain attacks. In the case of network security appliances, the hardware's intended use is known at the time of manufacture, and its use can easily be predicted. In many cases the behavior of the software is very well known, and its path through the hardware can easily be predicted. This can give the adversary easy access to usernames, passwords, and data that should be encrypted. It can also provide the adversary with the means to stealthily bypass the security features on the system. If network security appliance or tactical communication system processes and data can be masked or modified in such a way that if exfiltrated it is no longer useful, or even harmful, to the adversary it will restore trust to the system. If the processes can be rerouted through the hardware, such that its path is unpredictable, these malicious insertions would no longer be able to reliably exfiltrate useful data, or attack processes.

Developing a means of restoring trust by the software architecture is a novel idea. It will lead to a more secure computing environment, because we will be able to place more trust in the systems. It will also prevent the cost of construction and operating new and trusted computer components manufacturing facilities, or embedding inspectors at factories around the world.

PHASE I: Define software architecture that would be compatible with network appliance and/or tactical communication hardware that would enable security applications or tactical communication systems to operate in a trusted manner on hardware assumed to be untrusted. Describe and develop creative methods, techniques, and tools that would allow for the implementation of such an architecture.

PHASE II: Develop, implement and validate a prototype system that utilizes the architecture, tools, and methods from Phase I. The prototypes should be sufficiently detailed to evaluate scalability, usability, and resistance to malicious attack. Efficiency is also an issue that should be explored, although it is less critical than overall scalability.

PHASE III DUAL USE APPLICATIONS: The increasingly global market for computer hardware will continue to put the production of hardware in places not sympathetic to the United States Military or commercial sector. This application will have a broad market in the commercial sector as well where the protection of intellectual property is becoming increasingly difficult.

REFERENCES:

1. Popick, Paul R., "Requirements Challenges in Addressing Malicious Supply Chain Threats," July 2013. Available online at: <http://www.acq.osd.mil/se/docs/ReqChallengesSCThreats-Reed-INCOSE-Vol16-Is2.pdf>.
2. "Non Deterministic Algorithms," Available online at: <http://cs.nyu.edu/courses/spring03/G22.2560-001/nondet.html>.

KEYWORDS: Networks, trust, data integrity, security appliance, supply chain