Brainstorm: Military Electronics Part 2

What is the most pressing issue concerning the deployment of autonomous military robots?

Dr. Kelvin Nilsen, Aonix, www.aonix.com [1]

One critical and largely solvable problem is the common failure to give high-integrity development proper attention. Most autonomous military robots are involved in safety critical activities such as aiming and firing of weapons or gathering and reporting intelligence that influences weapon aiming and firing.

As a company with a long tradition of supporting deployment of safety-critical software, we are frequently consulted by U.S. defense subcontractors. Far too often, software is mostly complete, and now they are ready to begin the long and arduous task of achieving safety certification. Unfortunately, “now” is not the time to begin this effort. Essential to safety certification is an audit of software process, spanning requirements capture, architecture, design, test plans, code, tests, and analysis of test results. Traceability from requirements to end results must be demonstrated. Analysis of test results must demonstrate full test coverage of every condition associated with every branch along all possible execution paths through every procedure.

Most successfully certified software systems have been developed under stringent guidelines designed to enable safety certification. Developers restrict their use of libraries and language features, select operating systems and tool chains designed for safety-critical development, avoid complex algorithms and information flows, and instrument their software to enable comprehensive testing and code coverage analysis. It is extremely difficult, often cost prohibitive, to certify code that was not developed in accordance with certification guidelines.

Part of the fault lies with government technology procurement offices who demand early milestones focused on capability demonstrations under idealized operating scenarios. Safety and security certifications were not mentioned in original calls for

proposals and are sometimes only addressed with change orders issued after program funds are nearly depleted. No wonder so many government sponsored defense programs are over budget.

David Moore, Avnet Electronics Marketing, www.em.avnet.com [2]

Several reports indicate that the US military has more than 5,000 semi-autonomous robots deployed in Iraq and Afghanistan. The majority of these intelligent machines are unmanned aerial/ground vehicles with autonomous navigation capabilities and used primarily for enemy surveillance. Drones, such as the Predator, are equipped with Hellfire missiles and actively used to destroy well-defined targets, but missile strikes are exclusively conducted by a remote soldier with confirmed and approved “eyes on target.” The technology to deploy completely autonomous military robots (operate in a real-world environment without any form of external control) that would actively participate in combat situations is near, but the artificial intelligence required to distinguish between a combatant and non-combatant has simply not been developed and/or tested to a degree of certainty acceptable to the American government. The potential for friendly fire within Allied forces and/or civilian rather than insurgent casualties is still too possible. Although most research will continue to be classified, military developments in the deliberative layer of intelligence will increase robot sophistication in planning, learning and meticulously defined human interaction scenarios.

Since the voting American public is already sensitive to the perceived risks posed by robots, thanks to Hollywood blockbusters like “I, Robot” and “Terminator,” expect field deployment to happen in foreign remote areas, similar to how the South Koreans protect their northern border, long before the U.S. military will engage completely autonomous robots into an urban warfare or battlefield environment.

 **Chris Minter, Components Corp, www.componentscorp.com** [3]

As autonomous robots are emerging in the military sector the most pressing issue to consider is the capabilities of these robots to perform their programmed tasks. Currently, autonomous robots are in use as armed border sentries in Israel, and guarding the border between North and South Korea. Reports state that by the year 2015, the Pentagon wants one third of its forces to be robotic, either remote-controlled or autonomous.

The robots in use presently by the US military are remote-controlled with decisions to use lethal force being made by human fighters at distant locations. The key in this type of robot deployment is just that, “humans” make the decisions.

With developments in technology to create autonomous robots programmed to destroy particular targets without direct human control, the question is raised as to where the ethical component fits in. Should a robot be equipped with artificial intelligence to make decisions about human termination? A US navy document suggests the critical issue is for autonomous systems to be able to identify the legality of targets. “Let men target men” and Let machines target machines”. The robot would then not in fact target a human holding a weapon, but the weapon itself. But how would the robot differentiate between an enemy military operative and an innocent civilian?

In a report funded by the US Office of Naval Research, “a fast approaching era where robots are smart enough to make battlefield decisions that are at present the preserve of humans” is envisioned. …

The report states: “There is a common misconception that robots will do only what we have programmed them to do…modern programs included millions of lines of code and were written by teams of programmers, none of which knew the entire program: accordingly, no individual could accurately predict how the various portions of large programs would interact without extensive testing in the field.” Is this field level testing option even available? A report compiled by the Ethics and Emerging Technology department at Cal PolyTech cautions against complacency or shortcuts as military robot designers engage in a rush to market and the pace of advances in artificial intelligence is increased, risking the deployment of robots with

design or programming flaws.

As artificial intelligence is becoming marketable reality, we need to be cautious of the ethical ramifications.

Blaine R. Bateman, Laird Technologies, www.lairdtech.com [4]

In my opinion, the reliability of embedded systems is the most critical issue. Any autonomous system relies on gathering data from the world around it in order to make decisions; and robots require signal processing (in either analog or digital form) to generate the information necessary to make decisions. Unless a robot has decision-making capability, it is not autonomous; and to be truly autonomous, it must be reliable.

Since a functional autonomous military robot is actually a set of complex embedded systems, it must operate at very high levels of reliability. Embedded electronic systems are subject to many factors that can decrease reliability or cause failures. Electrostatic Discharge (ESD), Electromagnetic Interference (EMI), overheating (Thermal Management), and electrical noise (signal line common-mode and differential-mode noise) can all wreak havoc on embedded systems.

Think about the systems you use everyday – your notebook computer, smart phone, DVR, and other electronic equipment. We all know these systems still have software glitches and can lock up, do unexpected things, lose data, etc. Now imagine that situation with a robot in a military environment – no one available to do a reset, power off/on, remove the battery, etc. Now that’s a pressing concern!

Another key reliability issue is software. Wireless M2M modules are used to send data to and from remote systems and the protocol stacks in those modules need to be optimized and tested for long-term autonomous operation. While there is a lot of buzz about COTS for military applications, not all COTS systems are robust enough for critical applications.

Jeff VanZwol, Micro Power, www.micro-power.com [5]

For autonomous military robots, increased power from the robot's power plant remains one of the most critical areas needing improvement. Increased power output enables an unmanned vehicle to run longer missions and improves maneuverability in hostile terrains (i.e. like climbing stairs in an urban setting).

Smaller Unmanned Ground Vehicles (UGVs) and Unmanned Aerial Vehicles (UAVs) utilize battery power plants to power these vehicles. Two trends in battery technology have extended the range of operation for these unmanned vehicles. First, the capacity levels for cobalt-oxide, lithium-ion cells - such the 18650 (18mm diameter, 65 mm length) cells - has consistently increased over the last few years. 2.2 Ahr Cells were introduced in the early 2000's, and 2.6 Ahr cells are now commonplace. Currently, 2.9 and 3.0 Ahr cells are available in limited production quantities. Although not progressing at the rate of Moore's Law, cell manufacturers have continued to improve cell capacity by stuffing more and more battery active material into the cells.

Second, companies like A123 Systems, E-one Moli, and LG Chemical have introduced high-rate lithium iron phosphate cells. These cells provide up to five to ten times more rate capability than cobalt oxide cells mentioned earlier. Some of these cells can support almost 100 Amp pulses. This higher rate capability substantially expands the range of operations and capabilities of unmanned vehicles.

John Jovalusky, Qspeed Semiconductor, www.qspeed.com [6]

Apart from the ethical and legal issues–such as the Laws of War and the Rules of Engagement–which may initially limit the use of autonomous military robots, there are technical issues that must be considered, since they will affect practical deployability. The primary one that comes to mind is that of security, both of communication to and from the robotic unit as well as accessibility of its programs by unauthorized personnel; particularly, enemy interests.

The latest malware episode–the conflicker worm–reminds us that even though the internet has been around for some time now and internet security has been greatly improved, the dangers of vulnerability to hackers and unwanted programs are still very relevant and pertinent. Given that reality, ensuring that military robots are sufficiently protected from being hacked into and possibly high jacked, or having their communications listened in upon, is no small task. Advanced weaponry ceases to be an advantage if it can easily be rendered useless or, worse yet, confiscated and used against the forces of its original deployers.

To that end, great care and fore thought in the design phase will be an essential requirement, as well as thorough testing–by 'friendly fire' assaulting hackers–to ensure that the program code of military robotic units is not accessible to anyone but authorized persons and that two-way communication with the robots cannot be readily intercepted, decoded or altered. Lastly, it would seem to be prudent that if unauthorized access to a unit is made, the machine can report the security breach and disable itself, if necessary, rather than risk the possibility of being controlled by hostile forces.

Links:
[1] http://www.aonix.com/

[2] http://www.em.avnet.com/
[3] http://www.componentscorp.com/
[4] http://www.lairdtech.com/
[5] http://www.micro-power.com/
[6] http://www.qspeed.com/