Proceedings of EASCON 1984: 17th Annual Electronics and Aerospace Conference
Washington DC, 11-13 September 1984, pp 215-219

CURRENT TECHNICAL RESEARCH ISSUES OF AUTONOMOUS ROBOTS EMPLOYED IN COMBAT

S. Y. Harmon & D. W. Gage

Code 442, Naval Ocean Systems Center
San Diego, CA 92152

ABSTRACT

The recent upsurge in interest in autonomous robots for combat applications has focused considerable attention on several of the obvious technical issues (e.g, target recognition, autonomous navigation, route planning). However, several technical issues exist which remain unapproached and, in some cases, even unacknowledged by the robotics community. This paper explores three such issues: (1) robot fault tolerance, (2) robot security and (3) multi-robot coordination. These issues are discussed in terms of the technology limitations and the research issues associated with those limitations. A common message which occurs several times during this discussion denotes the importance in modular implementation and well defined interfaces between subsystems in the development of autonomous combat robots.

INTRODUCTION

Interest in combat applications of autonomous and semi-autonomous robots has risen recently with the spreading realization that recent developments in a number of hardware and software technology areas (sensors, processors, knowledge based programming techniques, complex system control) will soon make demonstrations of autonomous combat robots for various missions feasible.

Autonomous robots will eventually change the face of combat as much or more than any other single technology. However, before that can happen the user community must have confidence that autonomous robots are reliable, secure and cost effective options which can be successfully integrated into existing and future command, control and communications (C3) systems. This paper attempts to begin bringing into focus several technical issues that must be confronted to transform the feasibility demonstrations of combat robots of the mid-1980s into the operational systems of the 1990s and beyond. The issues discussed here are robot reliability, combat robot security and coordination of multiple robots. These issues are, for the most part, mainstream issues in computer science and engineering. However, full consideration of their impact upon the implementation of combat robots is critical to the introduction of these autonomous combat robots into the defense inventory. The final section of this paper discusses the risks of and opportunities for deployment of autonomous robots in combat situations.

TECHNICAL ISSUES

Reliability

System reliability is no new problem for the military. Military operations are often critically dependent upon timing. Failure of a single piece of equipment at the wrong time (i.e., just before or during a mission) could cause significant losses of human and materiel resources as well as the potential failure of the mission itself. Of course, the wrong times are precisely when maximum system performance is demanded and expected. The wrong times are also when enemy actions are most likely to reduce system capability.

The word reliability can be used in a number of senses. It can mean susceptibility to failure as a result of flaws introduced during system manufacture. These are the failures to which consumer warranties apply. Reliability can also mean resistance to adverse external influences during operation. These failures are common in the stressful environment of military operations and are not protected by manufacturers warranties but are common in military operations. Military users often do not discriminate between these different types of failures since they often create the same problems. Also, common with complex systems is the reliability problem which arises when the system designer defines the operational problem differently than the system user.

As a result, the system behaves as designed but differently than the user intends and expects. Finally, the treatment of "edge effects" of autonomous robots as a situation encountered differs increasingly from the designed task domain becomes critical when developing systems for actual deployment. In military operations quite bizarre situations can be encountered. For example, how should an infantry robot be programmed to discriminate between a deaf nun and a Soviet soldier pretending to be a deaf nun? Infantry robots may be faced with 10,000 soldiers dressed like nuns should such a vulnerability be discovered by the enemy.

A reliable system must perform its assigned task within the expected time when the task is within the robot's capabilities. Furthermore, the robot must let the user know when it no longer has the ability to perform a requested task. Thus, the system must be able to recognize when it can no longer perform its task and must be able to communicate that knowledge to the user. This type of reliability can be achieved through systematic and accurate design, implementation using reliable components, coordinated redundancy, fault minimization and self repair.

The good design and implementation procedures necessary to ensure a fault free nature are, for the most part, available as computer aided design tools which make exhaustive and systematic design of mechanical, electronic and software components a reality. For hardware, extensive methodical design practices and careful choice of components improves the robot's fault resistance. For software, modern design practices coupled with program specification and verification tools provide the only hope of implementing reliable software in complex systems. Good robot design begins with careful system specification. Care is needed in system specification to insure that the delivered capability corresponds with the desired capability. These observations about robot design are true for any complex system. However, designers of manned systems have taken advantage of the inherent flexibility of humans. Autonomous systems designers will have no such luxury. A successful operational autonomous combat robot will require all the computer aided design capability available.

System fault tolerance can ensure that a complex piece of equipment will function reliably throughout a mission of prescribed duration. Without a high degree of redundancy a device's likelihood of failure is proportional to its complexity. However, a complex device can be made significantly more reliable than an immensely simpler device through redundancy. Redundancy can be used to detect faults (e.g., though voting), to isolate faults and to recover from faults which are discovered or occur during operation. Analytical techniques are available to determine the level of redundancy necessary to provide the required system reliability for a specified mission. Redundancy is necessary not only in the computing elements of a robot but also in the mechanical components (e.g., two arms, six independently driven wheels). In order to take advantage of such redundancy, the robot must be able to revise its normal strategies when faults occur, as it is often possible to use system components for tasks for which they were not originally intended (e.g., using arms to drag a damaged vehicle a short distance, using pliers as a hammer). This issue of employing conventional resources for unconventional purposes is well beyond the capabilities of existing techniques in automated planning.

The addition of self repair capability can further enhance long term reliability and reduce maintenance and repair costs. This is an option available only to robots and it simplifies the support of the system. At the very least, the robot should provide extensive self diagnostic capability to assist field repair. Unfortunately, beyond automated diagnosis, robot self repair is beyond the state of existing technology.

Security

The use of complex information handling devices always presents a threat to military security. For this reason considerable resources are invested in establishing and maintaining the computer and communications security of military systems. Robots present special security challenges in combat situations. They must interact with many elements of the hostile environment in many different ways to accomplish their missions. These channels of interaction add to the commonly recognized channels of compromise. Furthermore, autonomous robots present significantly more opportunities for compromise because they must interact with the battlefield environment in ways which cannot be predicted when the robots are - first programmed. For a robot, security means prevention of compromise of the

information stored within the robot and minimization of enemy ability to alter the behavior of the robot. How the interactions between an autonomous robot and the enemy can be monitored and controlled without sacrificing the robot's effectiveness has yet to be determined. Elements of classical communications and computer security can be applied to this problem but existing techniques do not provide a complete or even satisfactory solution to robot security.

Autonomous robots must be built upon a reliable foundation to be secure. Autonomous robot designers must also take advantage of existing secure system design techniques. Much of the design care that is required for a reliable system is also necessary for secure system design. Security and reliability both emphasize the need for modular implementations. Computer aided design must also be used to insure that the foundation system behaves as specified. A secure kernal of proven functionality can be used while it is still infeasible to mathematically prove the correctness of all software components. Secure autonomous robot design requires the adoption of security models but existing models inadequately represent the processes of robot systems. Such techniques as capability addressing, system partitioning, encryption, identification friend or foe and more are necessary to realize practical autonomous combat robots. An awareness of system security must be designed into the autonomous robot as part of its task. This awareness can shift some of the burden of security to the robot itself and, thus, make design simpler.

Use of imperfectly secure systems for limited applications is possible but autonomous robots for widespread deployment in combat must be proven secure against enemy penetration and corruption. Autonomous robots which control firepower or electronic countermeasures are particularly sensitive to the security issue because they could inflict significant damage upon friendly forces if compromised. That is, they could not only compromise information but they could also actually adversely affect friendly force elements which have not been compromised.

The very complexity of autonomous robot systems makes them formidable security risks. In addition, as experience with secure computer systems has demonstrated, security imposes considerable overhead. Considering this cost, the security issues pose some of the most interesting questions for future autonomous robot designers. How much of a robot's processing resources should be devoted to analyzing system security? Can the robot identify situations with high security risk and avoid them? The alternative to take action against security violations is an alternative available only to a robot and makes robot security unlike computer or communications system security. Just one step from action to prevent compromise is the most intriguing security question related to autonomous robots. Will a robot ever be able to be a double agent (i.e., make the enemy think that it is compromising itself when it is actually trying to gather information about or to affect enemy capability)?

Multi-Robot Coordination

Autonomous robots will not be used alone in combat. They will always be used to complement available human controlled resources including fully manned systems as well as remotely manned devices such as remotely piloted vehicles (RPVs). Considerable investment has already been made in existing C3 assets and any new system must be integrated into these C3 systems if it is to be accepted and effective. Ideally, autonomous robots can be configured to respond similarly to manned systems. This strategy reduces the alterations necessary to make them an integral part of a combat C3 system. However, this mimicry only solves part of the problem. Considerable research is still necessary to determine how manned and autonomous resources can best be employed cooperatively. Incremental introduction of autonomous robots into the combat environment means more complex communications are required to facilitate the mix of manned and autonomous force elements evolving over time. The best strategy is to design communications between robots that humans can always understand. This strategy also provides an inherent debugging capability. An autonomous robot should, like an expert system, be able to explain the reasoning behind its actions.

Autonomous robots offer the opportunity to streamline the operations of multiple combat systems by providing well defined responses to known situations. This streamlining could reduce system response time enough to gain significant advantage over an adversary with superior numbers. Multiple robots used cooperatively as distributed sensors gain improved range,

accuracy and resistance to errors as compared with a single robot. Distributed robots can also be used in a variety of tactical roles to improve the ability to bring coordinated fire upon a single target or a series of distributed targets in coordinated attack. Distributed autonomous robots could provide an ability to coordinate military operations with a precision unknown today if they are secure and reliable as individuals.

Permitting complex cooperation between manned and automated systems further exacerbates the security situation by providing many more complex interaction mechanisms which could be penetrated and compromised. Well defined interfaces between autonomous robots are necessary for their communication and cooperation.

Multi-robot cooperation also raises several questions. For instance, how should function be allocated between the various systems to accomplish a single mission? How should the cooperating systems communicate and how much should they communicate? Should redistribution of functional roles occur during the actual execution of the mission? If so, who should be able to coordinate that redistribution of function and how should they decide? How should the command structure change when the mix of manned systems and automated systems changes (what if ultimately all manned systems were eliminated from active combat roles?)

DEPLOYMENT OPPORTUNITIES AND RISKS

Advances in computer security, fault tolerance and multi-system cooperation will have operational relevance only if the users have an accurate understanding of and well founded confidence in autonomous robots' capabilities. Considerable experience with these systems will be required before this desirable state is developed. Implementation experience will come first through feasibility demonstrations, then through limited applications and, only later, through widespread application. As user confidence in autonomous robots increases so shall the application opportunities (and the corresponding funding of autonomous robot development efforts) increase. As user confidence decreases so shall the application opportunities (and the corresponding robot development funding) decrease. Implementation experience depends upon development activity which depends upon funding. If development funding is decreased then the rate at which autonomous robots are introduced into the operational inventory decreases. This link between user confidence and funding makes maintaining high user confidence paramount. Premature introduction of autonomous robots for combat could have a disastrous effect upon the future development of combat robots. At best, premature fielding of autonomous robots would sour the user community on this new technology and result in inefficient and wasteful application to noncritical missions. At worst, it could lead to significant and unanticipated battlefield losses. Poor user perception of the effectiveness of these systems would certainly dramatically affect their future development and deployment.

There is no reason to suppose that current operational doctrines incorporate the optimal modes of deployment for battlefield robotic systems, which will, for the foreseeable future at least, be more expendable than manned systems, more precise in their response to anticipated situations, and more unpredictable in their response to situations unanticipated by their developers. Operational commanders will have to develop a sense of the capabilities of the systems, and, commanders being human (at least so far) this will most probably be done initially in terms of manned system equivalents. If a commander's model of one squadron of 6 robotic microtanks is that it is equivalent to one platoon of infantry, he will use it in the same way that he would use a platoon of infantry, which may not be fully appropriate. The implication of this is that it is not enough that a robotic system should offer spectacular capabilities that will certainly change the shape of the battlefield in the future; if a system is to be accepted today it must be capable of playing a contributing role in the battlefield of today, using doctrines of today.

Introduction of autonomous robots to combat will be hastened as existing manned assets are retrofitted. This retrofit can occur incrementally as different autonomous subsystem technologies develop. However, flexible system architectures which facilitate incremental implementation will have to be developed and demonstrated for retrofit to be possible. This requirement translates into the need for modular subsystems with well defined interfaces between subsystems. Furthermore, new manned systems should be designed to accommodate this retrofit.

CONCLUSIONS

The most important conclusion one can draw from the present state of autonomous robot development is that modular subsystem implementation with well defined interfaces between subsystems is necessary to robot reliability, robot security, multi-robot coordination and, eventual, operational deployment. Furthermore, modular design readily facilitates system evolution as well as simplifying troubleshooting and repair. Both qualities are necessary for operational deployment in combat.

As a final word of caution against the rising enthusiasm about autonomous combat robots, potential military users should be careful not to interpret near term feasibility demonstrations of autonomous robots for limited combat situations as near term opportunities for operational deployment. In the same light, autonomous robot developers should be careful not to oversell the capabilities of their systems. Premature deployment of autonomous robots will slow the overall development of combat robots. As discussed in this paper, many more critical issues need solution and resolution before operational combat robots can be deployed.

ACKNOWLEDGEMENTS

The material in this paper evolved from discussions with Dr. John Clark and Dr. William Whelan of the Rand Corporation, Dr. Azad Madni of Perceptronics Inc., David Smith of the Naval Ocean System Center and Dr. David Mizell of the Office of Naval Research. Their contributions are gratefully appreciated. The most important contribution has been the funding for this work and for that we are grateful to Mr. Gerald Clapp, manager of the USMC 6.2 Surveillance Block Funding.