Determining the Efficacy of Nuclear Security Through Computer Simulation

N. Chornoboy[1] and E. Waller[1]
[1] University of Ontario Institute of Technology, Ontario, Canada
(nicholas.chornoboy@uoit.ca)

A Master's Level Submission

Summary

Currently when creating new security regimes or analyzing current ones it is difficult to determine how effective they are or will be. This leads to many decisions being made using subjective expert opinion or expensive live exercises. While these are useful for determining the effectiveness it would be ideal to have an easy way to simulate and attack through software in order to allow rapid testing of many different scenarios simply. This work focuses on modifying the force on force simulator stage to run these kinds of tests.

1. Introduction

Nuclear security is quickly becoming an important issue that operators and regulators must address. In order to design security protocol's and physical protection systems facilities must first have an idea of what they must be able to withstand. This is referred to as the design basis threat and it consists of the most pessimistic assumptions of adversaries numbers and capabilities [1]. This information is then used by industry experts to design a facility capable of withstanding them [2].

To ensure that a facilities security measures are sufficient live force on force exercises are used in conjunction with expert opinion to determine weaknesses and areas for improvement [2]. The problem is these exercises are expensive and time consuming meaning they are done infrequently. It would be useful to have some way to test the effectiveness of the security of a given facility that can be done on an ongoing basis to supplement these tests. The proposed solution is to model the facility with software and test the security system there.

2. Background

When a nuclear facility is designed it must be ensured that it has sufficient security measures to meet the design basis threat [1]. There are many different approaches for measuring how effective a facility is at meeting a particular threat but one of the most common used for existing facilities are live exercises. Since the threat that a nuclear facility must defend against is known these can be quite accurate if done properly [1] [3]. This however can be challenging as the attacking force will often be other members of the security force leading to possible behavioural discrepancies. These kinds of exercises are also disruptive and expensive for the facility. This can also only be done on a facility that has already been built were it is to late to make design changes.

Another method is to construct what is called an adversary sequence diagram [4]. This is a simple list of barriers that are or will be in place along with their detection probabilities and penetration times. These are then used to calculate the probability of detection before a particular point and then the amount of time available for defenders to intercept. The probability of the defenders winning the engagement must then be estimated separately. This is often done using a simple comparison of the numbers and armament of the combatants on either side. This method works well for known pathways and produces a very quick estimate [4]. It falls down for more complicated systems were there are many possible ways that an adversary could attempt to gain access and detection probabilities and penetration times are not always easy to estimate.

The two previously mentioned methods are what are used for the most part currently however they have some shortfalls as mentioned. Another method that could cover some of these gaps would be to construct a full computer model [5]. This method has more complicated initial set up as the whole facility must be modelled; afterwords however making small changes is simple allowing different approaches to be tried. This is similar to an adversary sequence diagram as detection probabilities and penetration times must be estimated however there is significantly more options when it comes to modifying the scenario. It also has similarities to a live action exercise as the actions of the guard force and adversaries can be tracked throughout the simulation [5] [6]. This is useful for finding gaps in the security. By modelling the facility it allows for a more accurate representation of the physical scenario so allows for better estimations to be made.

This work focus around developing a modelling tool for the nuclear industry to supplement the use of expert opinion and live action exercises. Some modelling solutions already exist and are in use however these are often 'black box' solutions were only a particular scenario has been modelled and it can not be changed [5] [6]. It is hoped to create a model were small changes can be implemented quickly so that many scenarios can be tried in a short amount of time. Its intend goal is not to replace either but to allow computer based testing between live action exercises so that they can be conducted more effectively. This would also allow testing in a more rigorous way facilities that have not been constructed yet.

2.1 Stage Software

The software selected to modify is called Stage and is made by a company called Presagis out of Montreal [5]. The stage software allows for the modelling of the physical facility as well as rudimentary procedures for the guard forces. These can then be used to model a simulated attack in order to determine whether the guard force would be successful or not. The software mostly deals with the force on force part of the problem so the focus of the work is showing that it can be used to model the detection and interception of an adversary as well. This involved the creation and implementation of the multitude of sensors that are used in nuclear facilities within the stage software [6]. These sensors are then given detection probabilities from literature in order to accurately reflect the real sensors. These are then placed into the model and the guard force is set up to reactionary respond in a way reflecting the facilities guard procedures. This allows and attack force to be simulated and the guard force to react in a realistic manner. The simulation also had to be modified to include more probabilistic based outcomes for detection and engagement to more accurately reflect realistic responses [5]. Finally code was then designed to interact with the stage software iteratively running a scenario many times to get statistics on how effective the facilities security was against that attack.

2.2 Lagassi Model

For the purposes of this project a the Legassi theoretical nuclear facility was chosen to be modelled [7]. This is a mock up of a nuclear research reactor used by the IAEA for generic nuclear security exercisers. It was chosen due to its history of use in nuclear security simulations along with its ease of finding information. A layout of the facility as it was modelled is presented in figure 1. The design basis threat for this facility is given as a 5 terrorists armed with automatic weapons and explosives attacking the waste storage in the upper right hand corner with the intention of theft. The research reactor uses highly enriched uranium and also has isotope production [7].

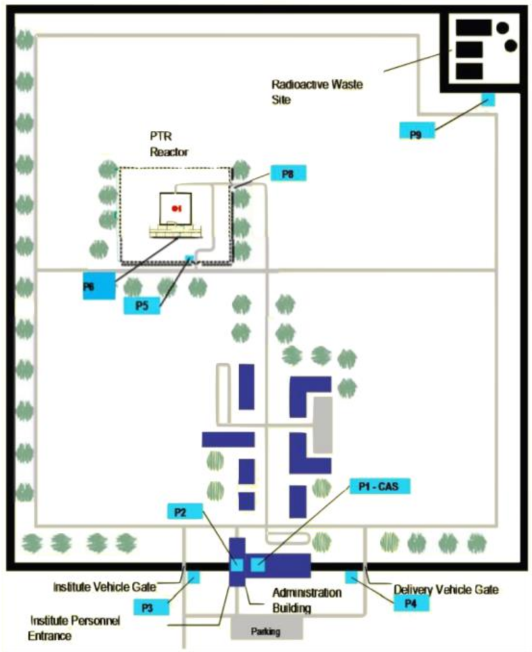

Figure 1 Layout of the Lagassi facility [7]

3. Results

In order to prove the validity of using Stage for this kind of work it must first be bench-marked using some other form of engagement data. The easiest way to do this is set up a simple scenario with two groups of otherwise equal combatants and vary their numbers to compare win rates. In a Sandia national laboratory report on physical protection systems they present an analytical approach to force on force engagements similar to the first method mentioned previously [6]. This data was then compared to that found in the scenario set up in stage. To acquire this data the weapons implemented were as close to those used in the Sandia report as possible and simply creating a scenario with the number of combatants simply lined up [6]. It was found that these results were quite close to the sandia numbers showing that stage could reliably simulate the combat portion of the problem. With the combat portion base-lined this means that everything is in place to continue with the modifications for detection of the full scale model of the facility in stage and the analysis of its security through a monte carlo method.

The sensors created were placed in logical parts of the facility based on research of security at real world facilities [6]. With the defenders set up to react to these sensors an attack scenario was devised based on the design basis threat. This was run many time to get the probability of effectiveness of the defenders. This information was then used to improve the simulation further. This is similar to what is currently done with expert opinion and adversary sequence diagrams however is much easier to visualise and modify and allows for more complexity. The scenario was then modified to show a different attack and showcase the versatility of the model. It was shown using the constructed tool that changes could be made within reasonable time scales to allow testing of new scenarios quickly to a fair degree of accuracy.

4. Conclusion

Based on preliminary results it would appear that Stage is a valid tool for testing the efficacy of nuclear security regimes. As a force on force simulator it allows for accurate simulation of the combat portion of a security event. The additions of various sensors allow for modeling of the detection portion of the event. The combination of these tools and the iteration program allow for a reasonably accurate and complete prediction of the out come of an engagement. It is our hope that we can prove this technique to be a useful tool to add to operators repertoire allowing them to better predict security out comes more simply.

5. Future Work

With the validity of the modelling in Stage tested the next step will be to fully implement the Lagassi facility. This will involve 3D modelling with another one of Presagis' products Creator. Once the 3D modelling is done it can be imported to Stage and used as the basis for the attack scenarios. Further defence procedures will also be implemented into the software so that the defence force reacts realistically. This will then be used to run a scenario many times similar to monte carlo to get the effectiveness of the defence force in each scenario. This information will then be used to improve the model iteratively while attempting to minimise cost. It is hoped this will show the utility of this approach.

6. References

[1] M. L. Garcia, *The Design and Evaluation of Physical Protection System,* 2nd ed. Burlington, MA: Butterworth-Heinermann, 2008

[2] J. S. Nye, “Nuclear Learning and U.S.-Soviet Security Regimes,” MIT Press, vol. 41, no.3, 1987

[3] L. J. Fennelly, *Effective Physical Security,* 4th ed. Burlington, MA: Butterworth-Heinermann, 2013

[4] M. J. Hicks, “Physical Protection Systems – Cost and Performance Analysis: A Case Study,” IEEE AES Systems Magazine, 1999

[5] L. P. Maguluri, “STAGE Atmosphere: To Reduce Training Costs in EW Simulations,” from *Advanced Computing, Networking and Informatics,* 2nd ed. Switzerland, Springer, 2014

[6] M.K. Snell, "Report on Project Action Sheet PP05 Task 3 between the U.S. Department of Energy and the Republic of Korea Ministry of Education, Science, and Technology (MEST)," Sandia, Albuquerque, NM, SAND2013-0039, 2013

[7] IAEA,"Hypothetical Facility Description for Physical Protection exercises," IAEA, Vienna, Austria, 2000