Sandia National Laboratories

Physical & Cyber Security Modeling Interfacing Through Dante and ARCADE

Andrew S. Hahn

September 2024
SAND2024-12451R

U.S. DEPARTMENT OF ENERGY

NNSA National Nuclear Security Administration

Sandia National Laboratories is a multimission laboratory managed and operated by National Technology and Engineering Solutions of Sandia, LLC, a wholly owned subsidiary of Honeywell International Inc., for the U.S. Department of Energy's National Nuclear Security Administration under contract DE-NA0003525.

ABSTRACT

Physical security is increasingly facing new threats from cyber attackers, for which there is little research in the way of characterizing this threat. This report discusses the efforts to combine cyber and physical security modeling tools to investigate this novel combinatorial threat space. To acomplish this, the Dante force-on-force modeling and simulation software and the Advanced Reactor Cyber Analysis and Development Environment (ARCADE) were integrated. Dante provides a 3D environment which models the physical world, while ARCADE provides the cyber and control systems world.

ACKNOWLEDGMENT

The author would like to thank Fred Oppel and the Dante team at Sandia for their support as well as Benjamin Liu for his programming efforts.

CONTENTS

LIST OF FIGURES

ACRONYMS & DEFINITIONS

ARCADE Advanced Reactor Cyber Analysis and Development Environment

CAS Central Alarm Station

CSOC Cyber Security Operation Center

FSM Finite State Machine

JSON JavaScript Object Notation

NPP Nuclear Power Plant

OT Operational Technology

PPS Physical Protection System

UCA Unsafe Control Action

UDP User Datagram Protocol

ZMQ ZeroMQ

This page intentionally left blank.

1. INTRODUCTION

Cyber attacks against Operational Technology (OT) systems are increasing at an alarming rate [2]. These attacks present a new risk for all cyber-physical systems but research efforts have largely been focused on the control system domain of OT. Physical protection systems (PPS) have not enjoyed the same measure of concern, though these OT systems are essential to protecting critical infrastructure. Many PPSs rely on air-gaping or isolating their networks as the primary security mechanism, despite the clear evidence that air-gapped networks have not been secure since at least the advent of Stuxnet. Threat actors are now developing even more sophisticated threats that circumvent the air-gap [8], which presents another serious emerging threat, the concept of the combine cyber-physical attack.

A cyber-physical attack can be described as concurrent cyber and physical attacks which assist and amplify the impact of each other. A cyber adversary may compromise the PPS and provide a physical adversary a time advantage the PPS design cannot accommodate. A physical adversary may provide access to protected equipment or networks which allow a cyber adversary to cause consequence beyond what the physical adversary could accomplish alone. These types of scenarios are currently not considered in the designs of physical or cyber security systems and their architecture. Its is imperative that tools are made to model these hybrid threats to begin developing methodologies, protocols, and designs to ensure that our critical infrastructure is defended against the next generation of threats.

In an effort to begin establishing this next generation of modeling capabilities, modeling tools from each domain have been selected for integration efforts. The Advanced Reactor Cyber Analysis and Development Environment (ARCADE) and the Dante force-on-force modeling and simulation software were selected to start integration work towards a more holistic system of systems cyber-physical model. These tools were selected for their advanced capabilities and their compatibilities in solution methods. This section will briefly discuss these tools before detailing integration efforts in the next section.

1.1. ARCADE

ARCADE was developed in response to a need for an environment which could enable the activities in the Tiered Cyber Analysis (TCA) which is outlined in the NRC draft regulatory guide DG-5075 [9]. A virtual environment, provided by Sandia's minimega [1], supports an emulated control system network which linked to engineering simulators via the Data Broker [4] (Figure 1-1). The emulated virtual control system has custom tools integrated to perform unsafe control actions (UCAs) at the command of the cyber attack simulator, which allows ARCADE to simulate the effects of a cyber attack on the control system and measure its resiliency. The cyber-physical analysis system pictured encompasses a number of sub-systems which orchestrate the simulation of many thousands of permutations of different cyber attack effects in many parallel simulations. Together these tools allow ARCADE to rapidly characterize the resilience of a system and identify any Achilles heal which could be solved with simple design revisions.

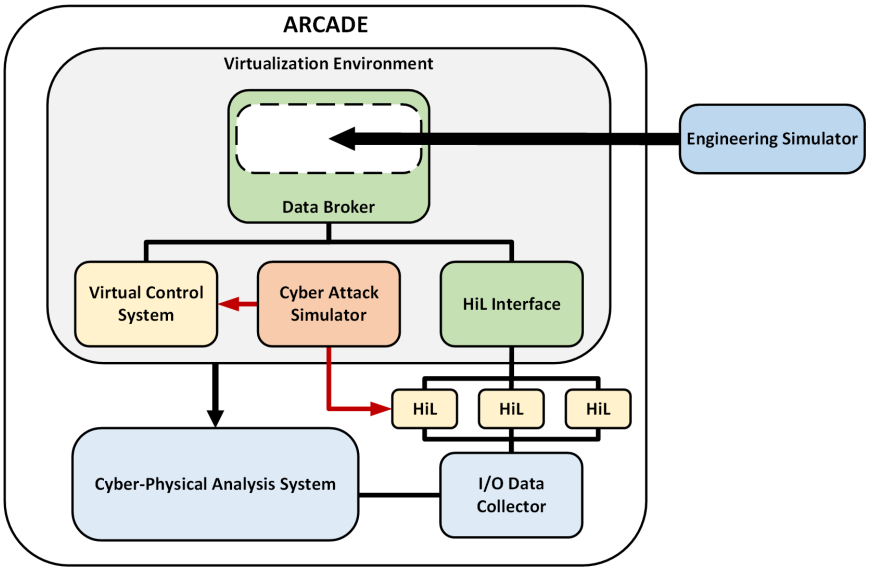

Figure 1-1 Block diagram of the Advanced Reactor Cyber Analysis and Development Environment [5].

A key development goal of ARCADE is modularity, each component is made to be as independent as possible and highly configurable to accommodate unexpected use cases. This has proven to be a boon to other projects which have used components such as the Data Broker for hardware in the loop capabilities. ManiPIO, which the cyber attack simulator is based on, has been used for educational and training applications outside of ARCADE [6]. This flexibility and modularity is what allows ARCADE tools to be adapted to many applications in the cyber-physical space, and makes it an ideal candidate for incorporation with a physical security simulation tool. Ideally the physical security tool we integrate with would be temporally discretized solution method and be amicable to external communication.

1.2. Dante

Dante is a force-on-force simulator which is built on top of the Umbra simulation framework which allows comprehensive simulations of physical security while accurately replicating real-world conditions [7]. Umbra allows the decomposition of simulation problems into collections of modules which govern a single phenomena and its interactions with other phenomena in the simulation [3]. These module groups are referred to as *Worlds* and encapsulate phenomena such as radio communications, or sound propagation. Dante is a set of Umbra worlds which are architected to produce a realistic and holistic simulation environment for force-on-force research. However, Dante is more than an an artifact of a specialized Umbra environment, how it simulates adversary and defender behavior is unique and a powerful predictor of force-on-force outcomes.

How humans interact with their environment and accomplish goals despite changing situational conditions is a highly complex and stochastic problem to simulate. Dante utilizes concepts from cognitive modeling to create agents which determine their actions to accomplish goals through

Figure 1-2 Screenshot of Dante scenario editor.

finite state machines (FSMs). Goals are set by commands issued by the user or by virtual commanders. Commands are packages of FSMs which define the agents behavior, which contains sets of goal oriented actions. The command `MOVE` defines a set of agent actions such as path finding, obstacle avoidance, movement, and agent orientation [7]. This allows agents to adapt to the changing conditions around them and plan future actions to accomplish their sets of goals. Multiple dynamic agents produce stochastic simulations, which is expected of human behavior modeling. Dante runs many simulations of the same scenario to build statistical results and determine the success or failure of defensive and adversary strategies.

2. INTEGRATION EFFORTS

As a first effort a conceptual scenario to integrate around which utilized the strengths of ARCADE and Dante was selected. A simple physical attack against the control system virtualized in ARCADE would suffice to test the connection between the systems. Dante would model the adversary gaining entrance to an fictional NPP and sabotaging the controls for the reactor coolant pump. ARCADE would simulate the effects of the pump going offline and provide warnings and physical plant conditions to Dante. Defenders and operators in Dante would be alerted via the control system, and start attempting to bring the plant to a safe condition while the adversary is attempting to prevent them from accessing the controls necessary to do so. If the pressure in the primary loop exceeded certain limits, a steam explosion would take place and kill any agents in the vicinity. Such a scenario is fictional, but it defines the integration goals and success criteria while demonstrating core functionality of the integration and the potential benefit of such a system of systems model. The next stage is structuring how each system will interact with each other.

Both Dante and ARCADE were designed with modularity and ease of integration as key goals, so its not unexpected that they are highly compatible. ARCADE uses the Endpoints from the Data Broker to establish any ground truth level integration. These Endpoints only follow 2 rules:

receive UDP updates from the Data Broker, and send ZMQ messages with any data updates. The rest of the Endpoint and how it is structured is entirely arbitrary and allowed to conform to the needs of the integration. Likewise, Umbra modules and worlds are as flexible as ARCADE Endpoints, they are able to adapt to functionally any use case. Umbra and Dante have had many external communication solutions developed, and it turned out that a ZMQ module had already been developed in the past. Since the ARCADE team had a lot of experience with ZMQ and it was already integrated with the Endpoint, ZMQ was selected as the primary communication method.

The basic communication method was decided and JSON was selected as the format for the communications since both development teams prefer it and it provides good data structure organization. Now the operational concept had to be determined, how time steps would be managed between systems. Since ARCADE was more sensitive to time in its computations due to the tightly coupled nature of control systems and physics, it was decided that ARCADE would govern time, but the coupling would be loose. Tightly coupling the simulators seemed to be fraught with problems though, as ARCADE timesteps are typically an order of magnitude smaller than Dante. Dante operates in human perception and response time intervals, where ARCADE operates on digital system response time intervals. It was decided that the systems would interact asynchronously, ARCADE would update the time stamp which Dante is allowed to move to before waiting for ARCADE to respond with a new time stamp. If Dante comes across an area which is difficult to compute and it lagged too far behind ARCADE, it would request ARCADE to pause and wait for it to catch up. This loose time synchronization allows each system to be more computationally efficient and the simulation time delta between them of milliseconds would be imperceptible on the human time scales Dante agents operate.

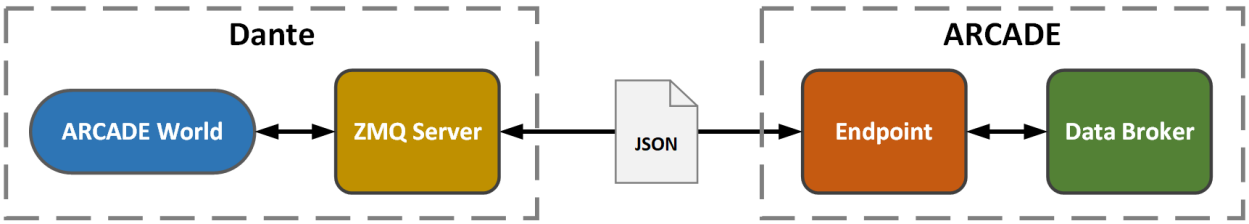

Figure 2-1 Block diagram of Dante and ARCADE communication strategy.

Figure 2-1 shows the basic concept of how the communication link would be established. An ARCADE world would be spawned in Dante via the Umbra framework, and a ZMQ server module would interpret the communications from ARCADE. A Dante Endpoint would be generated to handle communications for ARCADE to Dante. The Data Broker would also need some customization to handle some types of requests. What would be communicated and its syntax still needed to be defined and have room for future expansions and features. After some consideration the below data structure was determined, where functions are divided by ZMQ message topics.

ZMQ Packet

- `Topic = Time`
  - `"time_value" : float`

        * Contains the current ARCADE timestep value.
    - `"hold_time" : bool`
        * Signals ARCADE to hold time until Dante releases it.
    - `"reset" : bool`
        * Signals ARCADE reset the simulator.
    - `"close" : bool`
        * Signals ARCADE end the simulation.
- `Topic = Event`
    - `"explosion" : [string]`
        * Signals Dante that there has been an explosion at a designated location.
    - `"RCP_1" : bool`
        * Signals ARCADE to activate or deactivate the reactor coolant pump.
    - `"warning" : bool`
        * Signals Dante to sound a warning alarm for operators due to unsafe reactor operation.
    - `"evacuate" : bool`
        * Signals Dante to sound a site wide alarm to evacuate.

Some of these commands are not already implemented in the Data Broker, such as `hold_time` and `reset`. To accommodate these commands the Data Broker has to be modified. First, the Data Broker must have a method to receive new commands. This was done by modifying the ZMQ handler to listen for special commands and trigger flags for the responsible threads which will execute those commands. The `hold_time` command is rather simple, a Mutex is held which interrupts the timing control and holds the physics simulation from proceeding. The `reset` command is much more difficult, as the system was never designed to restart the simulator. This is feature is still being developed, but it is not a critical need for establishing the interface between Dante and ARCADE.

3. PROGRESS & FUTURE OPPORTUNITIES

The structure and implementation strategy has been completed for the Dante - ARCADE integration. The core of the communication implementation has been completed as well, however the systems have not been connected together. Test jigs have been used to develop the connection and do work successfully on each system, the programs are ready to integrate. The example scenario in Dante has been developed as described in section 1 and is waiting to be driven by the physics from ARCADE.

It is expected to take very little effort to test and demonstrate this integration in the near future. After which further integration's can be considered. The most obvious integration is to begin leveraging ARCADE's OT network emulation capabilities to accurately replicate the network and the firmware of the PPS devices and Central Alarm System (CAS). This digital PPS simulation could then be tied to physical PPS simulation in Dante using the ARCADE Data Broker, allowing for full-scope simulations of cyber-physical scenarios. This would allow cyber attack digital effects to be represented and cybersecurity monitoring and response architectures to be evaluated and optimized. Truly combined cyber and physical experiments would be possible, where a Cyber Security Operations Center (CSOC) and CAS work in concert to confront cyber-physical threats.

Integrating ARCADE and Dante represents the first step to creating cyber-physical security simulators which can drive research, training, and PPS design. With sufficient interest, such a system of systems simulation will significantly increase the depth of understanding possible regarding emerging cyber-physical threats. Unlike subject matter expert driven simulations, the analytical solutions of Dante and ARCADE remove human bias, progressing cyber and physical security design into empirical and repeatable engineering practices.

REFERENCES

[1] Jonathan Crussell, Jeremy Erickson, David Fritz, and John Floren. minimega v. 3.0, version 00, 12 2015.

[2] CSEC. The cyber threat to operational technology. Cyber Threat Bulletin D96-81/2021E-PDF, Canadian Centre for Cyber Security, Gatineau, QC, 2021.

[3] ERIC GOTTLIEB, RAYMOND W HARRIGAN, MICHAEL J MCDONALD, FRED J OPPEL, III, and PATRICK G XAVIER. The umbra simulation framework. 6 2001.

[4] Andrew Hahn, Raymond Fasano, and USDOE. Ot emulation data broker, version 0.0, 8 2021.

[5] Andrew Hahn, Michael Higgins, Lee Maccarone, Michael Rowland, and Romuald Valme. Lessons learned from advanced reactor cyber analysis and development environment (ARCADE). In *13th Nuclear Plant Instrumentation, Control & Human-Machine Interface Technologies (NPIC&HMIT 2023)*, Illinois, 2023. American Nuclear Society.

[6] Andrew Stuart Hahn. Manipio - manipulate process i/o for industrial control systems. 2 2021.

[7] Brian Hart, Derek Hart, Russell Gayle, Fred Oppel, Patrick Xavier, and Jonathan Whetzel. Dante agent architecture for force-on-force wargame simulation and training. In *Proceedings of the AAAI Conference on Artificial Intelligence and Interactive Digital Entertainment*, volume 13, pages 200–206, 2017.

[8] Kirill Kruglov, Vyacheslav Kopeytsev, and Artem Snegirev. Common ttps of attacks against industrial organizations. implants for remote access. Technical report, Kaspersky ICS CERT, July 2023.

[9] NRC. Draft regulatory guide dg-5075. Technical Report ML23286A278, Nuclear Regulatory Commission, 2023.