SANDIA REPORT
SAND2007-5792
Unlimited Release
Printed September 2007

Threat Analysis Framework

David P. Duggan and John T. Michalski

Prepared by
Sandia National Laboratories
Albuquerque, New Mexico 87185 and Livermore, California 94550

Sandia is a multiprogram laboratory operated by Sandia Corporation,
a Lockheed Martin Company, for the United States Department of Energy's
National Nuclear Security Administration under Contract DE-AC04-94AL85000.

Issued by Sandia National Laboratories, operated for the United States Department of Energy by Sandia Corporation.

Available to DOE and DOE contractors from
U.S. Department of Energy
Office of Scientific and Technical Information
P.O. Box 62
Oak Ridge, TN 37831

Telephone: (865) 576-8401
Facsimile: (865) 576-5728
E-Mail: reports@adonis.osti.gov
Online ordering: http://www.osti.gov/bridge

Available to the public from
U.S. Department of Commerce
National Technical Information Service
5285 Port Royal Rd.
Springfield, VA 22161

Telephone: (800) 553-6847
Facsimile: (703) 605-6900
E-Mail: orders@ntis.fedworld.gov
Online order: http://www.ntis.gov/help/ordermethods.asp?loc=7-4-0#online

SAND2007-5792
Unlimited Release
Printed September 2007

A Threat Analysis Framework as Applied to Critical Infrastructures in the Energy Sector

David P. Duggan
Networked Systems Survivability and Assurance

John T. Michalski
Critical Infrastructure Systems

Sandia National Laboratories
P.O. Box 5800
Albuquerque, New Mexico 87185

Abstract

The need to protect national critical infrastructure has led to the development of a threat analysis framework. The threat analysis framework can be used to identify the elements required to quantify threats against critical infrastructure assets and provide a means of distributing actionable threat information to critical infrastructure entities for the protection of infrastructure assets. This document identifies and describes five key elements needed to perform a comprehensive analysis of threat: the identification of an adversary, the development of generic threat profiles, the identification of generic attack paths, the discovery of adversary intent, and the identification of mitigation strategies.

Executive Summary

The movement of critical infrastructure communication architectures to publicly accessible communication backbones and the integration of commodity-based information technology into control system architectures have impacted the way control systems are being designed and used today. Although information technology (IT) systems provide a rich set of capability and commonality, they are also inherently vulnerable to a more expansive set of threats.

To be able to reduce the risk from open architectures and IT components introduced into critical infrastructures in the energy sector such as oil, gas, and electric power, there is a continuous need to evaluate the risk of adversary attack. A comprehensive threat analysis process can assist critical infrastructure providers and utility owners to identify how best to apply their limited resources in the protection of their infrastructure from malevolent threat.

To be able to perform proper risk analysis, a framework for threat analysis needs to be created to guide the analyst in the process. This document describes a threat analysis framework that identifies the critical elements associated with threat identification, impact, and mitigation.

This report identifies and describes five key elements that are needed to provide a comprehensive analysis of threat. The first element is adversary identification. The identification of high-level adversaries is normally classified and inhibits the proper dissemination of actionable threat information to appropriate stakeholders. Because of this limitation, the second element of the threat analysis framework allows for the identification of adversary characteristics and the development of threat profiles that can describe capability in an unclassified environment. This allows the analyst to map classified adversary capabilities into an unclassified domain. The third element, based on capabilities defined in the second element, identifies generic attack paths that can be pursued by an adversary against a system under review. The fourth element relies on a process that can discover in near-real time, activities associated with adversaries that may indicate and provide an early warning of an adversary's intent to leverage a discovered vulnerability against a critical infrastructure asset. The final element in the threat analysis framework identifies the best strategies for mitigation, reducing the overall risk of the infrastructure to compromise.

Each of the five key elements described above are to be the subject of follow-on research, development, and reports. When used together, these elements embody a comprehensive threat analysis capability that can be utilized by those in the energy sector to perform a more deterministic threat analysis and to guide the implementation of mitigations toward reducing the risk of successful compromise.

Table of Contents

Table of Figures

Acknowledgements

We would like to acknowledge the expertise associated with the personnel in the Information Assurance and Survivability Center at Sandia National Laboratories who continue to provide new insight in the field of information assurance. The authors would also like to acknowledge the U.S. Department of Energy/Office of Electricity Delivery and Energy Reliability (DOE/OE) as part of the National SCADA Test Bed (NSTB) Program for the funding of this work.

1 Introduction

The need to protect national critical infrastructure has led to the development of a threat analysis framework that can be used by the Energy Sector. This framework can be used to identify the elements required to quantify threats against critical infrastructure assets and provide a means of distributing actionable threat information to critical infrastructure entities for the protection of infrastructure assets.

Each of the five key elements described in this report are to be the subject of follow-on research, development, and reports. When used together, these elements embody a comprehensive threat analysis capability that can be utilized by those in the energy sector to perform a more deterministic threat analysis.

1.1 Background

A key component of risk analysis is a definition of the threat against the system. The rudimentary defenses put in place on most systems are sufficient to overcome the resources and capabilities of the lowest-level threats, but as an adversary's capabilities, and hence the threat level, increase, it becomes less likely that existing defenses can defeat that adversary's attacks and so the risk to the system becomes greater and more difficult to reduce.

Since the variety of threats is large, it is important to describe the threats in a way that allows them to be categorized. In particular, we are not so concerned with each individual threat but with the adversary that the threat represents. We really want to know the capabilities of the threats we face so we can defend against the range of attacks that a given threat—ideally, the threat we may actually face—might deploy. This enables us to generate an appropriate defensive strategy rather than reacting piecemeal to each individual indication of threat.

Our intent is to segment the continuous threat space based on our understanding of adversarial capabilities so that we can select a defensive strategy that will be effective against the classes of threats facing us, not just against the individual threats for which we have direct evidence. This requires an information framework that represents the relevant relationships between threats, vulnerabilities, and mitigating tactics.

1.1.1 Description

To provide an overall threat analysis capability, a threat analysis framework will be developed that identifies the important elements necessary to identify, characterize, and mitigate the effects of that threat. For the release of actionable threat information that can be used to develop protections for critical infrastructure assets, a series of unclassified threat analysis elements must be developed. Most high-level threat information today is classified to protect its source and collection methods. This "classifying legacy" of threat information also prevents its timely dissemination. To overcome this restriction, an unclassified threat analysis framework will need to be developed to identify needed elements of analysis and

provide a path for classified information to be used in an unclassified manner while maintaining the protection of classified elements.

One of the most important unclassified elements needed for threat analysis is a threat's capability to carry out a specific type of attack. Current analysis methods tend to concentrate on more subjective aspects of political and social motivation structures without identifying relevant objective characteristics that can be used to identify attacks a threat might be able to perform. As part of additional work being conducted[1], a generic set of threat profiles will be created to categorize threats against a cyber control system. This will help quantify the threat's ability to conduct both cyber and physical operations against a critical infrastructure entity's assets. There is currently no other documented work in the area of threat characterization that is developing generic threat profiles to solve this problem. Other solutions are reactive in nature, to a specific threat, while this approach allows the critical infrastructure provider and utility owner to be proactive.

There is an additional issue to be considered when evaluating the risk associated with a given vulnerability or threat: how likely is it that a threat is capable of identifying and exploiting the vulnerability and, indeed, is the threat even thinking along those lines? While many analysts recognize the importance of addressing this question, there is at present little in the way of systematic, comprehensive methods for arriving at good answers. This situation is understandable; the question is a "strategic surprise" problem, and such problems are notoriously difficult. To help address this problem, an "analyst-support" tool will be delivered as part of this work. This tool takes as input, a potentially large class of infrastructure cyber-vulnerabilities, discovers evidence that an adversary is interested in such vulnerabilities, and assesses whether the adversary is capable of exploiting such vulnerabilities.

To be able to utilize elements of the threat analysis framework, a relevant scenario will be developed to identify a threat against a critical infrastructure and the impact to the infrastructure if the threat is realized. This element of the work package will provide threat capability information to all threat-to-consequence modules.

1.1.2 Historical Information

Technology is used to improve efficiency and to reduce operating cost in the commercial business world, and the utility industry is not immune to this desired state of operation. The majority of our nation's critical infrastructure is privately owned and operated, with the asset owners subjected to the same efficient business model stressors as the rest of our commercial society. These efficient business decisions also impact the decisions related to the operation and security of control systems.

Currently, the security of utility systems is often inconsistent and sporadic. Both government and privately-owned critical infrastructure entities are not fully aware of the capabilities of threats that can be leveraged against their assets and thus have not developed mitigation strategies for these types of security risks.

[1] Duggan, D. P., et al. (2007). Categorizing threat: Building and using a generic threat matrix, SAND2007-5791. Sandia National Laboratories.

In spite of these short comings, critical infrastructure providers and utility owners must continually rely on technology to reduce the costs associated with operations, including staff reduction. The reduction of qualified operators, along with an increase in the number of interconnected systems, has resulted in a significant increase in the risks associated with adversary compromise of control systems today.

1.1.3 Significance

The threat analysis elements described in the body of this report create a comprehensive threat analysis framework that enables objective determination of threat capabilities and supports the ability to identify and prioritize expenditures to mitigate the effects from a class of threats, all in an unclassified venue for use by critical infrastructure entities. This report, along with other proposed deliverables, will help reduce the risk of energy disruption by providing a basis for utility owners to best apply their limited resources in the protection of their infrastructure assets from malevolent threat.

1.1.4 Literature Review

The comprehensive analysis framework to be developed by this work has not been found to exist in any prior DOE or other literature. However, there is a strong history of this type of approach within Sandia National Laboratories. In 1999, shortly following President Clinton's call for the development of a system for identifying and preventing major attacks to critical infrastructure[2], James Purvis authored a report on the need for a revision of sabotage categories, target types, and consequences and the development of a standardized risk assessment methodology for physical protection at nuclear power plants.[3] Beginning in 1999, researchers at Sandia National Laboratories started to assess threats to all critical infrastructure assets. Work has been completed on approaches to critical infrastructure security,[4] common vulnerabilities of control systems,[5] threat-group dynamics,[6] threat assessment,[7,8] and information sharing.[9] Most recently, David Duggan has been focusing on developing generic profiles of cyber threats[10] to industrial control systems[11]; this work

[2] *The Clinton Administration's policy on critical infrastructure protection: Presidential Decision Directive 63 (NSC-63).* (1998).
[3] Purvis, J. W. (1999). Sabotage at nuclear power plants, SAND99-1850C. Sandia National Laboratories.
[4] Baker, A. B., et al. (2002). A scalable systems approach for critical infrastructure security, SAND2002-0877. Sandia National Laboratories.
[5] Stamp, J., Young, W., & DePoy, J. (2003). Common vulnerabilities in critical infrastructure control systems, SAND2003-1772C. Sandia National Laboratories.
[6] Backus, G.A., & Glass, R. J. (2005). An agent-based model component to a framework for the analysis of terrorist-group dynamics, SAND2006-0860P. Sandia National Laboratories.
[7] Depoy, J., et al. (2006). Critical infrastructure systems of systems assessment methodology, SAND2006-6399. Sandia National Laboratories.
[8] Merkle, P. B. (2006). Extended defense systems: I. Adversary-defender modeling grammar for vulnerability analysis and threat assessment, SAND2006-1484. Sandia National Laboratories.
[9] Hayden, N. K., & Craft, R. L. (2003). The Knowledge Network (KnowNet): Deepening the nation's understanding of terrorist behavior, SAND2004-0476P. Sandia National Laboratories.
[10] Duggan, D. P. (2005). Generic threat profiles, SAND2005-5411. Sandia National Laboratories.
[11] Duggan, D. P. (2006). Generic attack approaches for industrial control systems, SAND2006-0650. Sandia National Laboratories.

continues in the current project by extending the threat profiles to include both kinetic and cyber threats[12].

Similar to the work being performed at Sandia National Laboratories, researchers from Lawrence Livermore National Laboratory (LLNL) presented a methodology for vulnerability a risk assessment using the Homeland-Defense Operational Planning System (HOPS).[13] However, although this work proposes a matrix for analyzing threat, it addresses facility-specific vulnerabilities rather than communication between industry and government regarding generic threats. In addition to this work by LLNL, researchers at Idaho National Engineering and Environmental Laboratory have proposed the Quantitative Threat-Risk Index Model (QTRIM) to compute a quantitative threat-risk index on a system and component level.[14] While the QTRIM approach may be able to predict the probability of attack on specific facilities, it focuses on a threat's selection of a target, seems to require a great deal of classified information, and does not perform the same information sharing service of which a generic threat profile would be capable.

The United States Army has also committed a great deal of time to the analysis of terrorism and the recognition of terrorist threats to U.S. military forces. *A Military Guide to Terrorism in the Twenty-First Century*[15] and its supplemental handbooks[16,17] are intended to support military training and education on the Global War on Terrorism. Although these documents focus solely on terrorist threats, they do stand as a strong reference for identifying threat attributes and for case studies of previous terrorist attacks.

Appendix A of this report includes a full bibliography of papers and reports relevant to this work.

1.2 Purpose

One of the primary problems with threat identification and characterization today is the resultant information is normally classified. The classified nature of threat information inhibits its distribution to entities that need it the most, such as critical infrastructure providers and utility owners. It is the intent of this report to identify and describe essential threat analysis elements that, when developed, will be used to provide the end user, the

[12] Duggan, D. P., et al. (2007). Categorizing threat: Building and using a generic threat matrix, SAND2007-XXXX. Sandia National Laboratories.
[13] Durling, Jr., R. L., Price, D. E., & Spero, K. K. (2005). Vulnerability and risk assessment using the Homeland-Defense Operational Planning System (HOPS), UCRL-CONF-209028. International Symposium on Systems and Human Science.
[14] Plum, M. M., Gertman, D. I., & Beitel, G.A. (2004). Novel threat-risk index using probabilistic risk assessment and human reliability analysis, INEEL/EXT-03-01117. Idaho National Engineering and Environmental Laboratory.
[15] *A military guide to terrorism in the twenty-first century, TRADOC DCSINT Handbook No. 1.* Version 3.0. (2005). U.S. Army Training and Doctrine Command.
[16] *Terror operations: Case studies in terrorism, DCSINT Handbook No. 1.01.* (2005). U.S. Army Training and Doctrine Command.
[17] *Cyber operations and cyber terrorism, DCSINT Handbook No. 1.02.* (2005). U.S. Army Training and Doctrine Command.

critical infrastructure owners and operators, with actionable unclassified threat information to protect their most critical assets.

1.2.1 Reason for Investigation

The primary reason for the development of a threat analysis framework is to capture important elements of threat analysis. Once captured, these elements and their inter-relationships can be described and used to help a threat analyst, or threat advisory group, to best characterize threat. After the creation of an accurate threat characterization, the potential impact of a threat can be described, allowing determination for the best means of reducing or eliminating the risk or mitigating the impact.

1.2.2 Roadmap Challenges

As referenced in the *Roadmap to Secure Control Systems in the Energy Sector*[18] publication, control systems are evolving from isolated operating environments using proprietary software, hardware, and communications technologies toward scalable inter-connected architectures using commercial off-the-shelf (COTS) products and standards-based protocols that provide high levels of interoperability. High connectivity and interoperability comes with a significant security risk. This risk must be managed and the development of a threat analysis framework is an integral part of the overall risk management process.

1.2.3 Audience

The end user or audience of threat information can be divided into two different groups: the government group and the industry group. The needs of these two distinct customers are not identical. Government customers are interested in formulating information to the following:

1. Can this adversary affect this asset?
2. What assets can this adversary degrade?
3. What threats can affect what assets?

On the other hand, industry customers are formulating their own set of information requirements that are much more aligned with the specifics of operations and tangible assets:

1. What level of capabilities does this threat have?
2. Is my current architecture protected against this threat?
3. What mechanisms or approaches can be used to protect against this level of threat?
4. What are my residual risks?

It is industry and those government branches not affiliated with intelligence gathering that are currently left in the dark when trying to characterize threats due to the classified nature of the threat information and the lack of means to propagate specifics of threat information because of these classified restrictions.

1.2.4 Desired Response

The intention of this research is to provide process control system owners and maintainers with comprehensive, actionable threat information concerning the abilities of adversaries that

[18] Eisenhauer, J., et al. (2006). *Roadmap to secure control systems in the energy sector*. Energetics Incorporated.

will allow them to successfully design, develop, and deploy appropriate defenses. Additionally, there is a goal to provide the U.S. Department of Energy (DOE) with a national perspective of higher-level threats with respect to critical infrastructures.

Producing analytic processes to better define and analyze threats against control systems will provide the DOE Office of Electricity (DOE/OE) with the following benefits:

- The ability to bring national awareness of the risk to the nations' critical infrastructure to cyber attacks,
- A mechanism for ranking mitigation actions to be performed for avoidance of a national disaster,
- A technical threat analysis capability,
- A method for providing unclassified, actionable risk information to control system owners and maintainers,
- A greater understanding by the energy sector of the impacts of a sophisticated threat, and
- The ability for DOE to communicate objective threat information to industry.

The benefit to the nation is that, by protecting critical infrastructure control systems from attacks by higher-level adversaries, DOE can help ensure the reliability of energy distribution to American citizens.

1.3 Scope

One of the primary activities necessary to move classified threat information to the unclassified information environment is the development of generic threat profiles that can characterize many different levels of threat without associating a name with a classified ability. This unclassified threat characterization must be able to bin a full spectrum of classified threat capability to allow for analysts from the classified threat environment to map the characterization of an "unnamed" threat to an equivalent bin or level of threat in the unclassified threat environment. This will then allow analysts in the unclassified environment to identify potential attack paths that could be supported by the asserted capability and identify proper mitigation steps to thwart attacks.

1.3.1 Extent and Limits of Investigation

The framework described in this report identifies the associated elements needed to provide a comprehensive approach to threat analysis. Each element is only described in enough detail to provide the reader with an understanding of its role. Further explanation of the elements will be contained in future publications. Only malevolent threat is considered within the framework.

1.3.2 Goals

The overall goal of this research is to provide a basis for critical infrastructure providers and utility owners to best apply their limited resources in the protection of their infrastructure

assets from malevolent threat. The capability being developed and identified in this report will provide stakeholders (including oil, gas, and electric industry utility owners and operators, control system equipment vendors, policymakers, and other government-related programs and activities, such as the International Electricity Infrastructure Assurance Forum) with actionable information concerning the abilities of adversaries and the likelihood that a threat is capable and willing to attack energy sector resources. A greater understanding of the threat will enable oil, gas, and electric utility owners and operators, government policymakers, and other key stakeholders to better design, develop, and deploy appropriate defenses to defend against the more sophisticated threat.

1.3.3 Objectives

The objective of this research is to better define and analyze threats against the energy sector's process control systems in the following way:

- Provide an overall threat analysis framework for extracting and characterizing threat information (adversary and intent) that originates from various intelligence organizations to better understand the types of threat facing the energy sector's control systems. This will provide a more comprehensive understanding of the full spectrum of threat.
- Develop a generic threat profile matrix that can be used to identify and characterize the different levels of the adversaries and their capabilities. The matrix will reduce the complexity of threat analysis and allow for unclassified, actionable risk information to be distributed to potential stakeholders.
- Implement an analysis tool to identify adversary "chatter" that allows threat analysts to determine the visibility of any discovered vulnerability.
- Develop cyber-based threat scenarios at a local, regional, and national level to provide a deeper understanding of the exploitation of vulnerabilities leveraged against a critical infrastructure by a threat.

2 Approach

To release actionable risk information that can be used to identify mitigation strategies for critical infrastructures, a series of unclassified threat analysis elements must be developed. As seen in Figure 2.1, these elements are required to provide the appropriate threat information to allow asset owners to position their infrastructure assets for protection from adversarial attack.

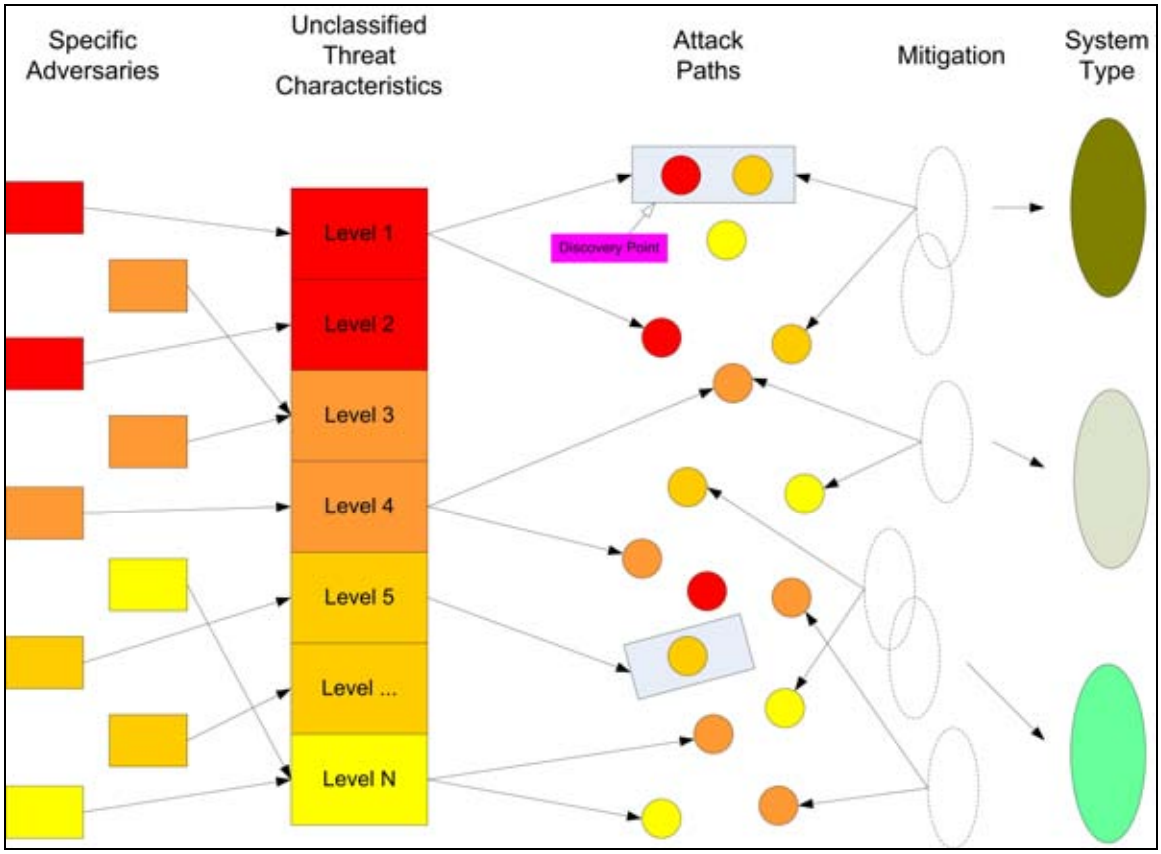

Figure 2.1 Threat Analysis Framework

2.1 Methods

The method used in this research is to identify and generate the needed elements of threat analysis. These can then be used in an unclassified environment to provide a path of analysis that starts at adversary identification and ends at risk analysis and mitigation. The method includes unique approaches to threat that include adversary characteristics that can bin unclassified threat capability, threat discovery that can identify adversary intent, and generic attack vectors that can provide a means of mitigation analysis.

2.1.1 Threat Characteristic Definition

Threat characteristic definition allows for identification of classes of attacks. These attack classes are biased by characteristics that are used to differentiate adversary capability and bin these capabilities into levels. Each level has a different severity of characterization that allows for it to be differentiated from levels that may be of higher or lower in value. For a detailed description of the threat attributes refer to *Sandia National Laboratories SAND report 2007-5791, Categorizing Threat, David Duggan et al. September 2007*.

2.1.2 Threat Attack Paths

Another essential element in threat analysis is the generation of attack paths. Attack paths define the adversary access points and the necessary elements to initiate, sustain, and propagate an attack. For this element to be created, a representative architecture must be used as a system reference model for the system under review.

In the case of an electric or gas utility a reference model has been generated.[19] The reference model allows the analyst to identify assets and all applicable attack paths to the compromise or destruction of the asset. A reference model also allows for a level of abstraction, making it applicable across a wide spectrum of associated systems. Figure 2.2 is an example use of the reference model that was created for control system evaluation.

2.1.3 Realistic Threat Scenario

The system reference model is supported by the generation of a realistic threat scenario. The threat scenario allows for tangible elements of operation and architecture to be introduced into the analysis. This includes the identification of specific components or assets of the system that are considered critical to the overall operations. Realistic threat scenario development will provide the following aspects for consideration:

1. A relevant critical infrastructure.
2. A viable attack or set of attacks that can lead to a substantial consequence, where the consequence has been provided by a system owner/operator or by the government.
3. The vetting or validation of the scenario's system description, system operations, system architecture with industry partners, subject matter experts and other interested parties.
4. The analysis needed to specify and characterize modeling of the scenario.
5. The dissemination of threat analysis results to all interested parties for review and comment.

2.1.4 Real-Time Vulnerability Analysis

Another important threat analysis element that must be considered when evaluating the risk associated with a given vulnerability is how likely it is that a vulnerability has been identified by a threat. Or, in other words, is an attack being formulated by a threat interested in exploitation? While many analysts recognize the importance of addressing this question, there is at present little in the way of systematic, comprehensive methods for arriving at good

[19] Stamp, J., Berg, M., & Baca, M. (2005). Reference model for control in automation systems in electric power, SAND2005-6286P. Sandia National Laboratories.

answers. This situation is understandable; it is a “strategic surprise” problem, which is notoriously difficult.

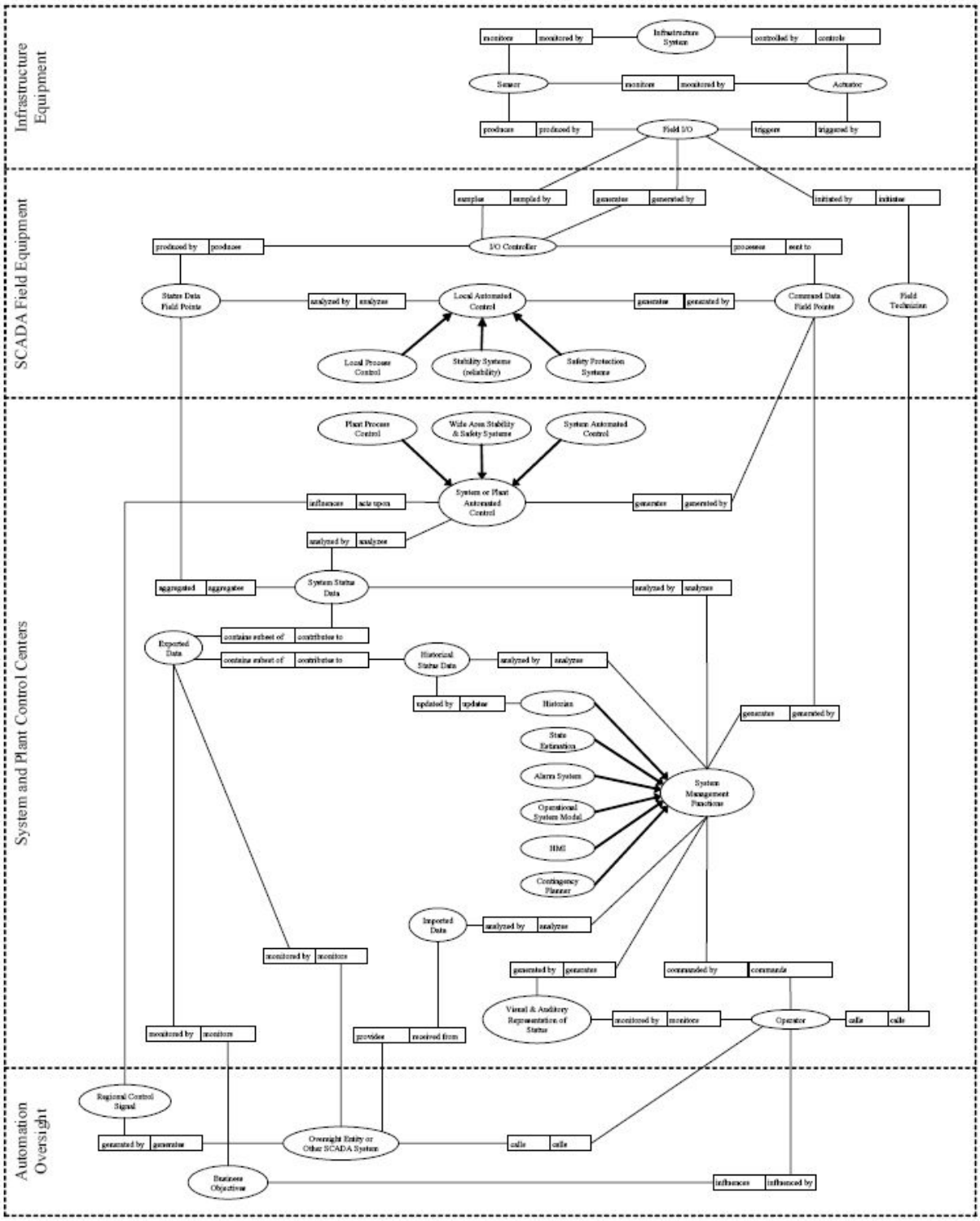

Figure 2.2 Example Use of Control System Reference Model

To address this shortfall, a proof-of-concept design is being developed to answer two primary questions:

1. Are any threats discussing aspects of exploiting a specific vulnerability?
2. Could the threat find enough information about a vulnerability to develop an attack?

These questions and similar ones are addressed through an automated computational exploration of open-source data sets, primarily the World Wide Web (WWW). Data sets to be used for this threat discovery and assessment are expected to include the World Wide Web (e.g., the Dark Web Portal[20] hosted at the University of Arizona), intelligence community reporting, and open-source literature and media.

The process of answering these questions involves an actively archived collection of web pages and other web objects which are associated with potential threats. A Net Discovery methodology automatically explores large regions of these archives and discovers web pages that are authoritative in the WWW and that explicitly encourage the search for aspects of the threat scenario. The second question is answered by applying a Net Discovery "interesting science" discovery tool to both the WWW and other publication data sets to identify potential attack information. The extraction of information from both of these types of queries allows the analyst to determine the imminent viability of an attack.

2.1.5 Protection Strategies

The final element of threat analysis constitutes threat mitigation. This element provides the information necessary to properly thwart a threat. The level, or rigor, of mitigation will be directly proportional to the level of threat. This will take into account how much resources must be expended to neutralize the threat. Each mitigation strategy will allow the critical infrastructure owner or operator to select mitigation techniques that limit the restriction to operations but maximize the protection from the threat. The threat mitigation element will also include the residual risk remaining after a mitigation strategy is chosen.

2.2 Assumptions

No assumptions were made in the development of the threat analysis framework concerning the type of control system or energy sector participant.

[20] "Dark Web Terrorism Research." (2005). University of Arizona. http://ai.arizona.edu/research/terror/index.htm.

3 Conclusions

The elements identified in this document allow for a full-spectrum approach to threat identification and management. Using the process embodied in the framework, it will be possible to answer questions from government on the security of the critical infrastructure systems and those questions from industry about the capabilities of threats as well as possible mitigation strategies to protect against those threats.

4 Recommendations

We recommend pursuing the plan objects outlined in this report. The plan outline included the identification and development of the following elements:

- Provide an overall threat analysis framework for extracting and characterizing threat information (adversary and intent) that originates from various intelligence organizations to better understand the types of threat facing the energy sector's control systems. This will provide a more comprehensive understanding of the full spectrum of threat.
- Develop a generic threat profile matrix that can be used to identify and characterize the different levels of threat adversaries and capabilities. The matrix will reduce the complexity of threat analysis and allow for unclassified, actionable risk information to be distributed to potential stakeholders.
- Implement an analysis tool to identify adversary "chatter" that allows the threat analysts to determine the visibility of any discovered vulnerability.
- Develop cyber-based threat scenarios at a local, regional, and national level to provide a deeper understanding of the exploitation of vulnerabilities leveraged against a critical infrastructure by an adversarial threat.

Bibliography

Ackerman, G., et al. (2007). *Assessing terrorist motivations for attacking critical infrastructure*, UCRL-TR-227068. Lawrence Livermore National Laboratory.

Backus, G. A., & Glass, R. J. (2005). *An agent-based model component to a framework for the analysis of terrorist-group dynamics*, SAND2006-0860P. Sandia National Laboratories.

Baker, A. B., et al. (2002). *A scalable systems approach for critical infrastructure security*, SAND2002-0877. Sandia National Laboratories.

Baybutt, P. (2002). "Assessing risks from threats to process plants: Threat and vulnerability analysis." *Process Safety Progress*, 21:4, 269-275.

Bush, G. W. (2003). *Homeland Security Presidential Directive (HSPD-7): Critical infrastructure identification, prioritization, and protection*.

Cragin, K., & Daly, S. A. (2004). *The dynamic terrorist threat: An assessment of group motivations and capabilities in a changing world*. RAND, Project AIR FORCE.

The Clinton Administration's policy on critical infrastructure protection: Presidential Decision Directive 63 (NSC-63). (1998).

Cyber operations and cyber terrorism, DCSINT Handbook No. 1.02. (2005). U.S. Army Training and Doctrine Command.

Dagle, J. (2001). "Vulnerability assessment activities." *Proc. 2001 IEEE PES Winter Power Meeting*, 108-113.

Dark Web Terrorism Research. (2005). University of Arizona. http://ai.arizona.edu/research/terror/index.htm.

Depoy, J., et al. (2006). *Critical infrastructure systems of systems assessment methodology*, SAND2006-6399. Sandia National Laboratories.

Duggan, D. P. (2005). *Generic threat profiles*, SAND2005-5411. Sandia National Laboratories.

Duggan, D. P. (2006). *Generic attack approaches for Industrial Control Systems*, SAND2006-0650. Sandia National Laboratories.

Duggan, D. P., et al. (2007). *Categorizing threat: Building and using a generic threat matrix*, SAND2007-5791. Sandia National Laboratories.

Durling, Jr., R. L., Price, D. E., & Spero, K. K. (2005). *Vulnerability and risk assessment using the Homeland-Defense Operational Planning System (HOPS)*. UCRL-CONF-209028. *Proc. International Symposium on Systems and Human Science*.

Eisenhauer, J., et al. (2006). *Roadmap to secure control systems in the energy sector*. Energetics Incorporated.

Guzie, G. L. (2004). *Integrated survivability assessment*. ARL-TR-3186. Survivability/Lethality Analysis Directorate, Army Research Laboratory.

Guzie, G. L. (2000). *Vulnerability risk assessment*.ARL-TR-1045. Survivability/Lethality Analysis Directorate, Information & Electronic Protection Division, Army Research Laboratory.

Hayden, N. K, & Craft, R. L. (2003). *The Knowledge Network (KnowNet): Deepening the nation's understanding of terrorist behavior*. SAND2004-0476P. Sandia National Laboratories Advanced Concepts Group.

Lemley, J. R., Fthenakis, V. M., & Moskowitz, P. D. (2003). "Security risk analysis for chemical process facilities." *Process Safety Progress*, 22:3, 153-162.

Luiijf, E. A. M. (2005). "Energy sector threats and vulnerabilities." *Proc. 3rd EAPC/PfP Workshop on Critical Infrastructure Protection and Civil Emergency Planning*.

Merkle, P. B. (2006). *Extended defense systems: I. Adversary-defender modeling grammar for vulnerability analysis and threat assessment*. SAND2006-1484. Sandia National Laboratories.

NetBreaker analytical tools identify terrorist groups, members, capabilities. (2007). Argonne National Laboratory.

A military guide to terrorism in the twenty-first century, TRADOC DCSINT Handbook No. 1. Version 3.0. (2005). U.S. Army Training and Doctrine Command.

Olson, D. T. (2005). *The path to terrorist violence: A threat assessment model for radical groups at risk of escalation to acts of terrorism*. Naval Postgraduate School.

Oman, P., Schweitzer, III, E. O., & Roberts, J. (2001). *Safeguarding IEDs, substations, and SCADA systems against electronic intrusions*. Schweitzer Engineering Laboratories.

Plum, M. M., Gertman, D. I., & Beitel, G. A. (2004). *Novel threat-risk index using probabilistic risk assessment and human reliability analysis*. INEEL/EXT-03-01117. Idaho National Engineering and Environmental Laboratory.

Post, J. M., Ruby, K. G., & Shaw, E. D. (2002). "The radical group in context: 1. An integrated framework for the analysis of group risk for terrorism." *Studies in Conflict & Terrorism*, 25:2, 73-100.

Post, J. M., Ruby, K. G., & Shaw, E. D. (2002). "The radical group in context: 2. Identification of critical elements in the analysis of risk for terrorism by radical group type." *Studies in Conflict & Terrorism*, 25:2, 101-126.

Purvis, J. W. (1999). *Sabotage at nuclear power plants*, SAND99-1850C. Sandia National Laboratories.

Salmeron, J., Wood, K., & Baldick, R. (2004). "Analysis of electric grid security under terrorist threat." *IEEE Transactions on Power Systems*, 19:2, 905-912.

Salmeron, J., Wood, K., & Baldick, R. (2003). *Optimizing electric grid design under asymmetric threat*. Naval Postgraduate School.

Salmeron, J., Wood, K., & Baldick, R. (2004). *Optimizing electric grid design under asymmetric threat (II)*. Naval Postgraduate School.

Security hazard assessment intentional threat matrix. (2002). AcuTech Consulting Group.

Stamp, J., Berg, M., & Baca, M. (2005). *Reference model for control in automation systems in electric power*. SAND2005-6286P. Sandia National Laboratories.

Stamp, J., Young, W., & DePoy, J. (2003). *Common vulnerabilities in critical infrastructure control systems*. SAND2003-1772C. Sandia National Laboratories.

Terror operations: Case studies in terrorism, DCSINT Handbook No. 1.01. (2005) U.S. Army Training and Doctrine Command.

Appendix B: Acronyms

COTS	Commercial off-the-shelf
DOE	Department of Energy
DOE/OE	Department of Energy Office of Electricity
HOPS	Homeland-Defense Operational Planning System
IT	Information Technology
LLNL	Lawrence Livermore National Laboratory
NSTB	National SCADA Test Bed
QTRIM	Quantitative Threat-Risk Index Model
WWW	World Wide Web

Appendix C: For More Information

National SCADA Testbed (NSTB) Project	Jennifer DePoy, Manager (**jdepoy@sandia.gov**) Critical Infrastructure Systems Sandia National Laboratories P.O. Box 5800 Albuquerque, New Mexico 87185
ieRoadmap	http://www.energetics.com/csroadmap/index.aspx Interactive Energy Roadmap to Secure Control Systems Energetics Incorporated

DISTRIBUTION:

1 MS 1221 Marion Scott, 05600
1 MS 0671 Gary E. Rivord, 05620
1 MS 1368 Jennifer M. Depoy, 05628
1 MS 0672 R.L. Hutchinson, 05629
1 MS 0672 David P. Duggan, 05629
8 MS 0785 J.T. Michalski, 06516

1 MS 0899 Technical Library, 09536 (electronic copy)