Refinery Control Systems in National Transportation Fuels Modeling

Andjelka Kelic, Derek H. Hart, Michael L. Wilson, Thomas F. Corbet
Sandia National Laboratories
Albuquerque, New Mexico, USA

***Abstract*—A control system cyber scenario that mimics a real-world catastrophic physical event within a refinery is developed and implemented in the SCEPTRE control system modeling environment. Effects of the associated outages are then explored in the National Transportation Fuels Model to examine the effects within the petroleum sector and determine the availability of transportation fuels.**

Keywords—cyber physical, control systems, refineries, critical infrastructure, petroleum, transportation fuels.

I. Introduction

Cyber security within critical infrastructure has received increasing attention in the policy community, beginning in February 2013 with President Obama's Executive Order 13636, "Improving Critical Infrastructure Cybersecurity[1]," followed by the 2014 National Institute of Standards and Technology (NIST) "Framework for Improving Critical Infrastructure Cybersecurity[2]." Despite the increased focus, significant gaps still exist in understanding the propagation of a cyber attack to potential physical consequences within critical infrastructure. In this presentation, we demonstrate the use of Sandia National Laboratories' (SNL) control system modeling framework, SCEPTRE, along with the National Infrastructure Simulation and Analysis Center's (NISAC) National Transportation Fuels Model (NTFM) to construct a cyber attack on a refinery and explore the potential impacts on the petroleum sector. The capability enabled analysts (1) to study how an attack would propagate into physical consequences, and (2) to explore assumptions about the criticality of various control system components, and how their commonality and implementation may affect both propagation and the ultimate consequences of an attack. Analysis within the NTFM, combined with a prototype refinery control model developed in the SCEPTRE framework, helped determine what additional information is required for a better estimate of consequences.

II. Bridging the Gap: Control System and Transportation Fuels Modeling

The goal of the analysis was to develop a cyber scenario that mimicked a real-world catastrophic physical event within a refinery and then to examine the effects of the associated outages on the availability of transportation fuels. To demonstrate the prototype refinery control-system model, a scenario was developed similar to events leading up to the explosion at the Texas City refinery in 2005[3]. The progression of this scenario was simulated in the refinery control-system model. Refinery outages were then modeled in NTFM under a set of assumptions ranging from a single outage to multiple simultaneous refinery outages.

The SNL SCEPTRE environment deploys components that represent threat and target systems with sufficient fidelity, modularity, and operational confidence to assess the effects of adversarial behavior. Software implementations of industrial control-system protocols are written to standard industrial specification documents. All simulated field devices and control units running in SCEPTRE use the appropriate protocol stacks to communicate using control-system messages.

The control-system model was developed in SCEPTRE's virtual control-system modeling and simulation environment. To model the control-system components, an emulytics testbed was used to deploy the network and all endpoints. Emulytics integrates emulated, simulated, and real devices and networks in a deterministic, variable scale and with fidelity appropriate for the given analysis. The Supervisory Control and Data Acquisition (SCADA) model developed for this analysis is a notional best-approximation and not based on the specific setup, operations, and process of a given refinery; therefore, vulnerability details cannot be assessed.

The petroleum sector modeling was conducted in NISAC's National Transportation Fuels Model (NTFM). NTFM is a dynamic simulation model of the national transportation fuels network that enables analysis of the potential consequences of refinery outages on the availability of transportation fuels. The network model tracks petroleum and transportation fuels movement from oil fields to fuel distribution terminals, including locations and capacities of tank farms, refineries, and terminals, and the pipelines, rail lines, and waterways that connect the network.

In the scenario, the attacker will exploit the connection between the enterprise network and the control-system network in order to disable a refinery. The attacker can gain access to the enterprise network with phishing attacks, downloadable malware on malicious sites, or any other common approach to gaining access. Traditionally, the rigor of security on internal network interconnections is either too lax, misconfigured, or so poorly configured that once access is achieved on one network, it is possible to gain access on another. Refineries are then outaged in NTFM based on assumptions of commonality of control-system implementation and market penetration. The

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 DEAC04-94AL85000. SAND 2015-2563 A. The National Infrastructure Simulation and Analysis Center (NISAC) is a program managed by the U.S. Department of Homeland Security (DHS) and comprised of a core partnership of Sandia National Laboratories (SNL) and Los Alamos National Laboratory (LANL).

three multiple-outage scenarios demonstrated a wide range of impacts for disruption of a given set of 10 refineries. The amount of unmet demand depends very much on the sizes and locations of the refineries.

III. Conclusions

Analysis results suggest that the effects of the outages highly depend on the assumptions regarding commonality of refinery control-system components, their associated implementation, and their inherent vulnerabilities. Refining the assumptions used for commonality of refinery control-system vulnerabilities would enhance assessment of cyber vulnerabilities in refinery control systems and associated physical consequences on the petroleum sector.

References

[1] Executive Order 13636 of February 12, 2013, Improving Critical Infrastructure Cybersecurity, http://www.gpo.gov/fdsys/pkg/FR-2013-02-19/pdf/2013-03915.pdf, accessed 3 April 3, 2015.

[2] NIST, Framework for Improving Critical Infrastructure Cybersecurity, http://www.nist.gov/cyberframework/upload/cybersecurity-framework-021214.pdf, accessed 3 April 3, 2015.

[3] US Chemical Safety Board, BP America Refinery Explosion, http://www.csb.gov/bp-america-refinery-explosion/, accessed 13 May 2014.