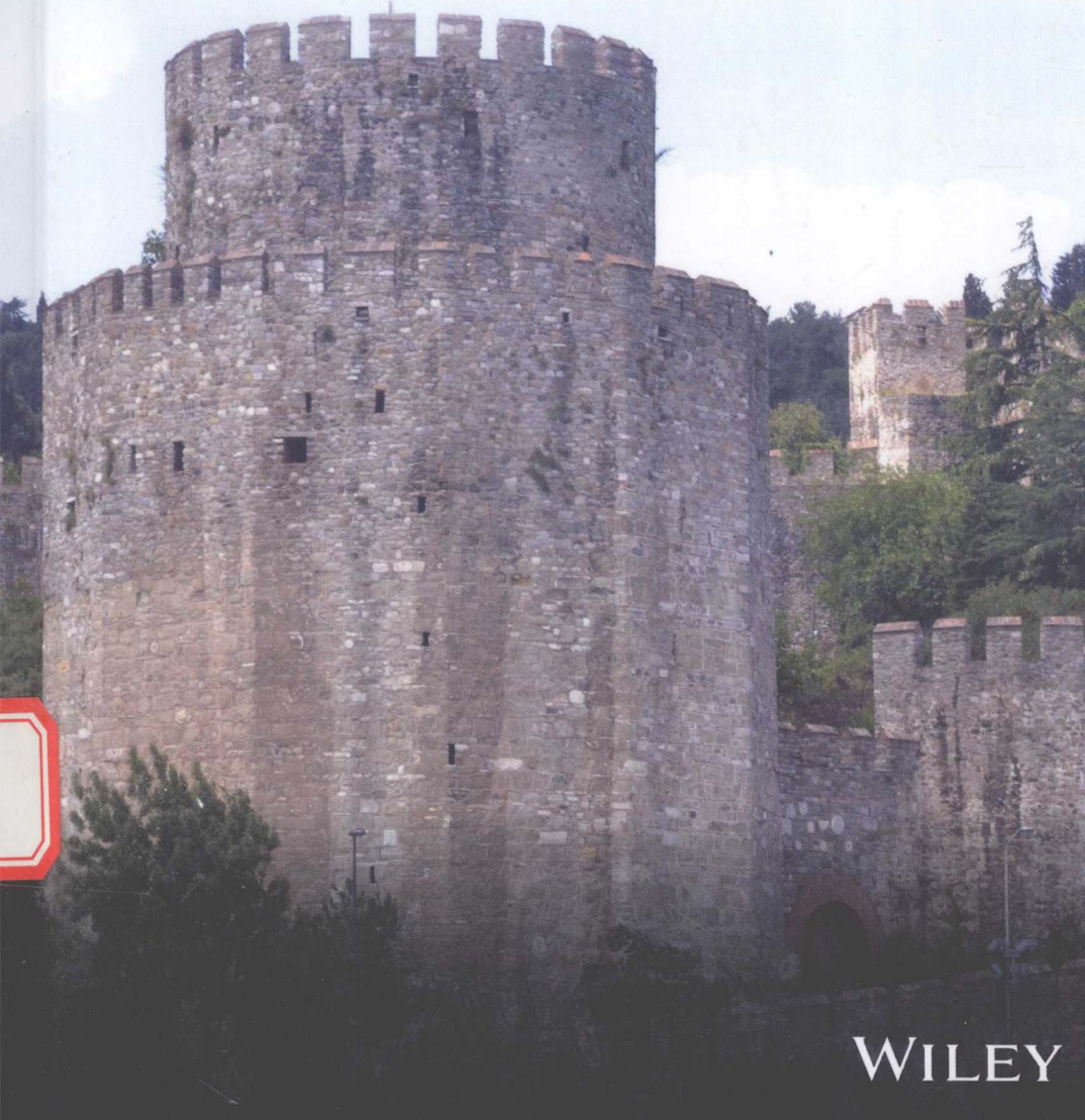
INDUSTRIAL SECURITY

MANAGING SECURITY IN THE 21ST CENTURY

DAVID L. RUSSELL • PIETER C. ARLOW



WILEY

INDUSTRIAL SECURITY

Managing Security in the 21st Century

DAVID L. RUSSELL, PE
President
Global Environmental Operations, Inc.

PIETER C. ARLOW
Lieutenant Colonel
South African National Defense Force

WILEY

Published by John Wiley & Sons, Inc., Hoboken, New Jersey
Published simultaneously in Canada

Library of Congress Cataloging-in-Publication Data:

Russell, David L., 1942–
Industrial security : managing security in the 21st century / David L. Russell, Pieter Arlow.
pages cm
Includes bibliographical references and index.
ISBN 978-1-118-19463-8 (hardback)
1. Industries–Security measures. 2. Industrial safety. 3. Risk management. 4. Security systems.
5. Terrorism–Prevention. I. Arlow, Pieter. II. Title.
HD61.5.R87 2015
658.4′73–dc23

2014043896

Set in 10/12pt Times LT Std by SPi Publisher Services, Pondicherry, India

Printed in the United States of America

10 9 8 7 6 5 4 3 2 1

1 2015

For my girls and their girls:
Laura, Jennifer
Edda, Zola, and Miriam
You are all special ladies, and this is for you.
Thanks for being yourselves.
Dave Russell

"In humble submission to my Lord and Savior God,
and dedicated to my children,
Jean-Pierre, Andrich, and Landi,
who are my all here on earth"
Pieter Arlow

CONTENTS

CHAPTER 1

INTRODUCTION TO SECURITY RISK ASSESSMENT AND MANAGEMENT

INTRODUCTION

This course was developed out of a training outline and the course Col. Arlow and I taught together in Manama, Bahrain. Pieter's background is South African Defense Force, and he was responsible for the security of the World Cup in 2011. Dave's background is civilian, industrial chemical, and environmental consulting. Together, we believe that this book will provide a different and practical approach that combines security theory with practice. We hope that it is not just another book that is put on the shelf and used occasionally, but read and considered, and one where our suggestions are put into place.

Security is not just one group's business; it is everybody's business. The combination of security, safety, and environmental protection are critical to the operation of a modern-day chemical or industrial plant. Despite the heightened focus on security by the US Department of Homeland Security and Transportation Security Administration, in many instances, it amounts to little more than a theater of the absurd because the United States is only marginally more secure and it is more a chance of luck than of their expensive, large, and restrictive efforts to increase travel security in particular and homeland security in general. Paperwork does little to provide security.

BUSINESS DEFINITION

The business definition of security is quite straight forward. Webster's Dictionary provides us with the basis for security: "freedom danger, risk of loss, and trustworthy and dependable." That is a very good start. The definition of security crosses a number of lines in the modern industrial plant and has many different definitions. Plant security can be anything from the guard force who keeps out the unwanted intruders to the executive protection service and to the corporate watchdog that looks after the financial and corporate affairs of the plant or the corporation to make sure that there is no theft or leaking of secrets at the highest level of the company.

Industrial Security: Managing Security in the 21st Century, First Edition. David L. Russell and Pieter C. Arlow.

With the advent of the Internet and the digital age, the job of security has been made, if anything, tougher because of the ease of communications and the proliferation of digital devices and the Internet. The communication is much easier, but then so is the ability to penetrate networks and obtain information or compromise security systems in a variety of ways. One has to look no further than the Stuxnet virus and how it delayed the development of the Iranian atomic program by attacking the centrifuges needed to refine the uranium. The success of the virus/worm delayed the development by up to 2 years.

SECURITY VERSUS RISK

In order to get a better working definition of security, we should also have a working definition of risk. Risk is the chance of loss or injury. In a situation that includes favorable and unfavorable events, risk is the probability of an unfavorable event or outcome. We measure risk by examining the certainty that a particular bad outcome or outcomes will occur.

Risk comes in many forms. There is financial risk, enterprise risk, risk of self-organized criticality (failure),[1,2] risk of injury, internal risk (theft, fire, economic loss, etc.), industrial/jurisdictional risk, operational risk, and several other types of often unforeseen and uncontrollable events that create damage. Within the various operations of a corporation, many of these have specific departments to address those risks. For example, safety, health, and environmental departments address specific risks for worker safety and environmental contamination; the IT security department manages risk for intellectual- and computer-related data. We are more concerned with the risks associated with external events such as terrorism, earthquakes, tornadoes, fire, etc. These are external risks. Internal risks might include sabotage and plant accidents resulting in fire, spills, explosion, etc.[3]

Within the scope of plant security, one is primarily concerned with events that are external to or imposed upon the plant, natural occurrences, and man-made occurrences, some of which are preventable and others not. Our working definition will include such elements as terrorism, external attacks, naturally occurring events such as tornadoes and hurricanes, and some limited scenarios for sabotage. Events such as spills, fire, and accidents may be equally unpredictable, but they are often addressable by proper design of facilities, installation of engineering controls, and management of personnel through procedures and training. Logically, we must also look into some of the process control and operational functions as a modern plant uses a variety of computer and wired and wireless control systems that are often open to sabotage or external influences.

FRAMEWORK FOR RISK MANAGEMENT

The basic framework for risk management is a cost-associated function where the general sequence starts with identification of the assets at risk, evaluation of the likelihood of their occurrence, development of a cost and a probability associated

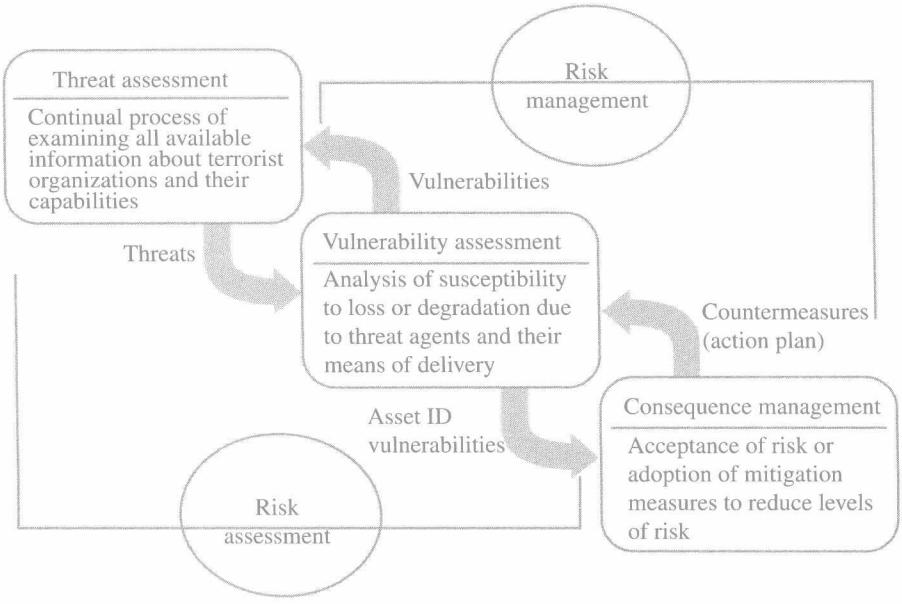


Figure 1.1 Outline of risk management actions.

with the occurrence of an attack or an event, and estimation of the costs to reduce the risk to manageable levels. This is a cyclic process, illustrated by Figures 1.1 and 1.2.

We measure and estimate the cost of a particular event occurring so that we can provide a financial plan for the plant or facility. We develop scenarios and the cost of those occurrences. For example, if we assume an attack by a hostile force, we try to estimate the damage and costs associated with that attack. We may create several scenarios and the associated costs. Things like standoff weapons such as a grenade launcher, a rocket, or a bazooka might have a damage level (cost) of C1 for the first scenario, C2 for the second scenario, etc. C1 might be for a mortar. C2 might be for a car bomb. The objective is to make these scenarios as realistic as possible when one views the likelihood of the attack.[4]

An attack can be any unplanned event and is subject to wide interpretation. Natural meteorological events can be an attack. So can an intruder into the plant. Terrorism is an attack, but then so is a civil unrest. Sabotage is a type of attack, but it is special and separate because it is imposed internally rather than from outside. However, a good risk management plan may want to consider sabotage as an element of a response plan.

Once we have a range of costs and scenarios, we can begin to determine the risk based on the probability of the events. This is often the most difficult and controversial part of the exercise because different assumptions on the likelihood of the event can produce dramatically different outcomes and costs. This is also complicated by the prospect of expenditures for increasing security and estimates as to how much specific improvements will reduce risk.

Just because a plant has *not* had an electronic intrusion (which they know of) does not mean that one will not happen tomorrow. Similarly, adverse weather events

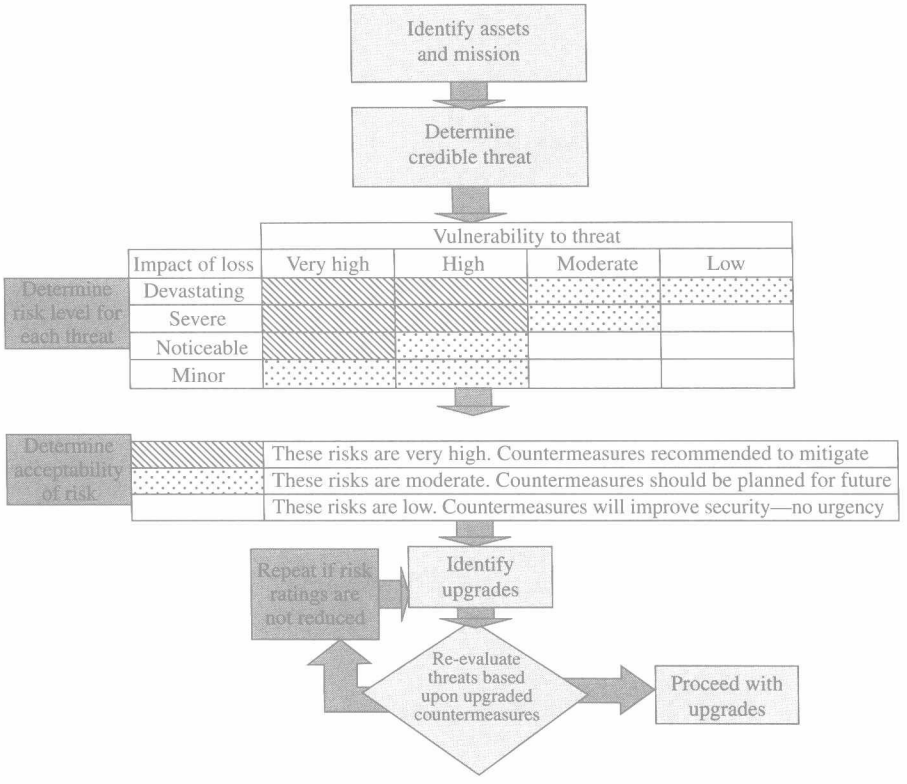


Figure 1.2 A second view of the risk analysis process. The risk analysis matrix is usually in color. Red indicates high risk, yellow indicates moderate risk, and green indicates lower levels of risk, but we have chosen to use stripes, dots, and white spaces to highlight the risk levels, respectively.

may have a record going back 30 years or more with no incidents, but that does not prove anything except that nothing has happened in that time period. History is often a very poor predictor of future events, and one needs to be careful about piling assumptions upon assumptions when and where events occur.[5] The concept of a "once in 100-year storm," popular in flood prediction and rainfall frequency analysis and other similar events, does not mean anything, except that the event was not expected with high frequency. Two of those events could occur back to back in subsequent days.[6]

In some cases, the risk assessment is relatively easy with probabilities in the percentile ranges $P = 1\%$ ($P = 10^{-2}$), while in many other cases, the probability of an event is on the order of 0.0001% ($P = 10^{-6}$) or even less. When estimated costs and damages are high, in the millions of dollars, we have a challenge multiplying a very small probability by a very big cost. Added to this is the idea that costs are ever increasing, and the range of uncertainties is dependent upon a partial or limited database.

Fundamental to the understanding of risk are the concepts of vulnerabilities, assets, and threats. Those three components come together to form the basis for risk.

Assets are the physical structures, the data, the production, the inventory, and almost anything that has a value. Vulnerabilities are the possible methods of

degrading or devaluing the assets. It is often helpful to think of vulnerabilities as the means that threats can accomplish the damage. Threats are the possible events that acting through the vulnerabilities can degrade or destroy the assets. The conjunction of all three is the risk. A word picture might help explain the concept.

A threat could be a terrorist attack by mortar or grenade or car bomb, or infiltration, or sabotage. The vulnerability might be that the main processing reactor at the facility would be damaged and that would lead to an explosion that destroyed the plant and created a fire in the storage areas, destroying them as well. The assets are the reactor, the plant, the storage areas, the inventory, and the data and might include the financial losses due to loss of revenue or accounts receivable from lost production. The assets would potentially be in the millions of dollars, but with careful planning and engineering controls, the assets could be separated to reduce the vulnerability on the scenario:

Risk = Threat × Vulnerability × Assets *and is expressed in monetary terms*

Or to express risk in another way:

Risk = Threat × Vulnerability × current or replacement cost of asset

The cost of an asset depends upon the accounting method employed and the tax structure and other variables. Generally, replacement cost for an asset needs to be updated every few years. The discussion in the following addresses some of this in very general terms.

If the threat is low and expressed in annual terms, the risk may be a few thousand dollars per year or may be diminishingly small depending upon the statistical basis employed to calculate the likelihood or probability of the threat. As we go through this book, we will try to address some of the concerns and attempt to illustrate methods to reduce the uncertainties using accepted techniques and statistical methods.

"Traditional" risk assessment programs exist to identify hazards arising from work activities to ensure suitable risk control measures are in place. However, incidents continue to happen, either as a result of inadequate risk assessments or failures in the necessary risk control measures.[7]

VALUE AT RISK

Several of the financial companies tend to look at risk a bit differently. The concept of value at risk (**VaR**) has been defined as "*the predicted worst-case loss at a specific confidence level (e.g., 95%) over a certain period of time (e.g., 1 day).*"[8] This model is being used by organizations such as Chase Bank where they take a daily snapshot of their international trading positions to determine their exposure.

The components of value can include such items as earnings, market, projected revenue, cash flow, and asset value: in short, everything. With older facilities, which may have been fully or partially depreciated, these items may be of substantially greater value than the facility itself. It should also be noted that the VaR needs to be benchmarked against a known quantity. The VaR could be actual or virtual, and may include project sales growth against a baseline or something

else. The financial management of the corporation needs to be involved in deciding what is the VaR.

For example, if an attack destroys the manufacturing plant causing lost production for the principal product, the VaR might include the replacement cost of the facility, plus the value of the lost market position (sales and revenue) and lost contracts. The inclusion of these other elements in the VaR will inflate the apparent replacement costs and could conceivably cause the management of the facility and corporate management to acknowledge the value of the facility in different and perhaps improved terms.

CALCULATION OF RISK

There are various methods of calculating the probable risk. Depending upon the accounting and valuation method employed, the risk manager can use linear or nonlinear valuation methods. The methods most commonly used include techniques such as Monte Carlo simulation, parametric simulation, and historical simulation. Monte Carlo methods involved application of statistical parameters and are substantially computer intensive. Parametric and historical simulations use a combination of formulas and may involve case histories for individual cases. In the case of a plant facility, cited earlier, the valuation may require a combination of methods such as Monte Carlo methods for market risk and parametric and historical simulation methods for physical asset risks.[9]

RISK ASSESSMENT VERSUS RISK MANAGEMENT

Risk assessment and risk management are two different things. The former involves a worst-case scenario, perhaps tied to financial programming and projections, while the latter involves preparing action plans, implementing and measuring performance, and proscribing actions and objectives to minimize damage or losses. These management plans can be proactive, based on risk assessments; active, based on safety audits and site inspection; and reactive, based on incident investigation and analysis.

The selection of a particular achievable risk evaluation level is somewhat arbitrary by the plant, but note that it does tie to reality over time. A risk confidence level of 95% would indicate that the company could sustain significant losses once in every 20 days or so. While a 99% confidence interval would indicate a significant loss once every quarter. Obviously, these loss rates are unsustainable when it comes to the physical facility. The projections are more for financial risks and market risks rather than physical risks. Sustainable physical risk rates are on the order of 0.0027% (one loss in 10 years or less), and many facilities throughout the world sustain a physical risk of 0.000059% (one major loss in 30 years) or less. So a combination of loss rates and factors must be used to make an accurate calculation.

Many risks, especially those to the physical plant, are considered insurable. However, many are not. One good example of an uninsurable major risk can be found considering Superfund and CERCLA[10] Litigation. The literature and the case law are

rife with cases where the insurance company had to pay for cleanup of sites contaminated by a company, and many of the insurance companies have demanded pollution riders on their policies or have denied claims for damages and cost recovery from past operations. The claims are frequently made based on real or alleged damages to local populations, health effects, and diminished values for property.[11] A number of these claims, however, are based on continuing practices rather than a specific past incident.[12]

At this point, it is also good to consider something else from the financial services industry, *stress testing*. In the realm of security, the stress test has a physical form. The military uses **red teams**, groups of individuals who are routinely cut loose from the plant structure with the specific instruction to attempt to penetrate the plant security and organize attempted security breaches and incidents. This can go to the point of planting a fake bomb, penetrating secure areas, spoofing software, and introducing harmless viruses into the operating systems of the plant. These red team activities are limited only by the ingenuity of the persons on the team and the resources available, but they should be coupled with regular drills, especially for the security personnel.

For example, the fire department runs or should run regular drills where they test their response by getting out the hoses and practicing fighting real fires. At airports, the fire companies regularly have drills that use an aircraft shell and douse it in fuel and then practice putting it out. But, there are a number of types of drills that can test the plant security and that may be appropriate. How often do we run spill drills? Similarly, if security is important, how ready is the security force able to respond to multiple incidents such as a fire or a spill *and an intruder*?

The literature is full of instances where refineries and other facilities with large tank storage have had spills that led to fires and explosions in the tank farms.[13] The point is that industry has regular firefighting drills, but when do they have security and other disaster drills? These are stress tests of the system, and the answer is, unfortunately, not so frequently. People stay sharp when they are challenged and regularly exercised on topics of concern, and increased awareness benefits everyone in the plant.

Note that in some areas, risk prevention may cross over into activities normally considered as the province of plant safety, and vice versa. If an employee is injured on the job or cannot perform his/her function, it does represent a risk to the plant finances. Similarly, the risk of employee theft or asset diversion or sabotage is also a risk. The principal difference between these and some of the previous risk factors mentioned earlier is the idea of preventable risk versus nonpreventable risk.[14] Preventable risk, such as employee risk, is often covered by safety training, procedures, and equipment. Theft, diversion of assets, and financial misappropriation are often covered by corporate security, and in the modern society, the operation and security of the plant's computers and data are protected by a special function within the information technology department. But, plant security needs a place at the "table" whenever the plant is expanded or when there are major changes to the process equipment to insure that the process is secure from outside intrusion.

Risk assessment of technological processes (chemical, petroleum, power plants, and electromechanical systems) is a complex process that requires enumeration of all possible failure modes, their probability of occurrence, and their consequences. This risk is managed through thorough analysis and technical review and playing "what if" analyses. This type of analysis is also known as HAZOPS.

RISK MANAGEMENT PLANS

We are going to march through some of the theory around risk management and develop a scenario or two and then present risk management analysis. In the following, we will not get into Monte Carlo simulation, which is often the preferred way of performing the risk analysis, but some statistics are inevitable. A good risk management plan has to cover a lot of variables and examine a lot of options. But it starts with an assessment of assets.

The first step is to start with a replacement cost assessment of the facility and its assets. This should include a valuation of the replacement cost for all equipment and might even include the cost of obtaining new or replacement permits for equipment, including such items as air pollution studies, water pollution evaluations, etc. This by itself is going to be a major effort. The risk management department of the company or the insurance provider can provide some guidance and a lot of help.

Step 1 is to obtain or develop a cost estimate for replacement of the facility.

The cost estimate should be as recent as possible, but even if it is a few years old, a fairly accurate adjustment can be made from various cost estimating handbooks, and such sources as RS Means, cost estimation, and McGraw-Hill/*Engineering News Record*'s construction cost index. The cost estimate generally should not be any closer than two or three significant figures. Any other level of accuracy is unwarranted. The cost estimate should be broken into as many different significant production units as existing within the plant and should also include the value of associated assets and inventory. The inventory should be broken out separately, because the value of that inventory can change more rapidly than inflation.

For example:

It is the total replacement cost for the facility that will serve as the baseline for our assets in the estimation of the risk (Tables 1.1 and 1.2). Oftentimes, the asset analysis for Unit A might look like the following if we assume that Unit A is an ammonia production facility:

Remember that $\mathbf{Risk = Vulnerability \times Assets \times Threat}$

TABLE 1.1 Cost analysis for replacement of a chemical plant

Item no.	Description	Original cost (millions)	Replacement cost (2012) (millions)
1	Unit A	11.2	22.4
2	Unit B	3.7	4.1
3	Raw materials inventory A (current $)	1.1	1.1
4	Raw materials inventory B (current $)	0.3	0.3
5	Finished inventory current values A and B	5.4	5.4
6	Associated buildings and support	3.9	12.0
	Total replacement costs		44.3