Figure 1 illustrates a five-step approach that establishes a framework for the application of system surety concepts [4]. These five steps include system definition, strategy, realization, evaluation, and recovery. The following descriptions of the detailed steps are adapted from [10] and from [11]. Examples from Rome’s water supply infrastructure are used to illustrate the process stages.

**Step 1: Definition**

Step 1 is to understand and define the system problem. This is accomplished by developing system objectives, determining system assets, and identifying system hazards.

**Develop system objectives:** Developing system objectives includes determining the need for a system, what function the system is to perform, and its scope, boundaries, operational interfaces, and high-level system performance requirements, including the surety elements of reliability, safety, and security. A system typically includes organizational culture, operating organizations, and technology.

The system objectives for the Roman water system was to reliably locate, transport, and distribute safe, clean water, with an infrastructure protected from sabotage by enemies [1], [8], [9]. Another system objective was to ensure that each aqueduct, “…took another independent source of supply” [8], presumably for reliability.

**Determine assets:** Determining assets is identifying what needs to be protected from harm or loss. Assets can be diverse and there may be two types in any system—internal or external. Internal assets may be primary, of direct value necessary to achieve the system objectives, or secondary, those that provide the infrastructure for primary assets. External assets may include human life or well being, environmental protection, monetary assets, company reputation, and organizational survival.
The primary internal assets of the Roman water supply system were its aqueducts and associated
distribution systems. Secondary internal assets included the maintenance teams. External assets
included the health of the Roman citizens and of the city of Rome itself, improved by efficient
use of all available water,

"Not even the waste water is lost; the appearance of the City is clean and altered; the air
is purer; and the causes of the unwholesome atmosphere, which gave the air of the City
so bad a name with the ancients, are now removed" [8].

Identify system hazards: Hazards are human, accidental, or natural agents that have the potential
to cause damage to or loss of assets. A hazard can be described in terms of a threat, a mechanism
by which the threat can be realized, and a resulting consequence. Systems design and analysis
generally emphasizes normal operating environments; however, surety requires that off-normal
operating environments also be studied. Operating environments are the general conditions
(demands on the system, weather influences, human factors, and so on) under which the system is
expected to perform its function. An understanding of potential consequences can be used to
drive the level of rigor required in addressing threats, mechanisms, and consequences, and to
evaluate the adequacy of necessary controls.

The Romans identified many hazards (threats, mechanisms, and consequences) for their water
supply infrastructure. For example, Frontoinus noted some human-caused hazards,

"...very often damages occur by reason of the lawlessness of private owners, who injure
the conduits in numerous ways. In the first place, they occupy with buildings or with
trees the space around the aqueducts, which according to a resolution of the Senate
should remain open. The trees do the most damage, because their roots burst asunder the
top coverings as well as the sides. They also lay out village and country roads over the
aqueducts themselves. Finally, they shut off access to those coming to make repairs" [8].

Vitruvius detailed this operational hazard,

"...a great rush of air is generated in an aqueduct, strong enough to break even stones,
unless the water is softly and sparingly let down from the head, and unless in elbows or
bending joints it be restrained by means of ligatures, or a weight of ballast" [9].

Step 2: Strategy

Step 2 leads to the development of a requirements-based surety theme that addresses identified
residual hazards. Residual hazards are those that cannot be completely removed. Hazards can be
removed by eliminating the threat, interrupting the mechanism, or eliminating the associated
consequences. Step 2 is realized by the development of surety requirements and the determination
of a surety theme.

Develop surety requirements: Specific surety requirements are developed for the system to
prevent the loss of previously defined assets in normal, off-normal, and malevolent environments.
Requirements should be logical, consistent, and complete, and include guidance on potential
trade-offs between system attributes, such as reliability, safety, security, cost, and schedule.
The Romans, recognizing priorities and trade-offs, declared, “Repairs to the channel itself should not be made in the summer time, in order not to stop the flow of water at a time when the demand for it is the greatest...” [8].

**Determine surety theme:** The surety theme describes in a unified fashion the philosophy, goals, and approach that will be used to eliminate or reduce the identified residual hazards. Typically, the theme addresses approaches to eliminate or reduce threats, decrease the likelihood or completely eliminate the possibility of initiating events exploiting the mechanisms; and mitigate the effects of the consequences of unexpected events. The theme establishes the focal point for design, development, and assessment efforts and provides a framework in which to communicate various design implementations.

The surety theme is a major element of system surety. Thematic elements used in stating a theme include:

- Isolation (separation, barrierization, diversion, support)
- Inoperability (disablement, destruction)
- Incompatibility (interlocking, entropization, energy incompatibility, information incompatibility)

A detailed description of these elements is provided elsewhere [10].

The theme should make assertions about the predicted performance of the system under various hazard environments. These assertions, which can be modeled or tested, define acceptable system surety performance.

The Romans used isolation as a theme to reserve different aqueducts for separate purposes:

> “It was therefore determined to separate them all and then to allot their separate functions so that first of all Marcia should serve wholly for drinking purposes, and then that the others should each be assigned to suitable purposes according to their special qualities...” [8].

The level of rigor used in the development of a theme depends on the level or type of surety desired. Four types of surety have been defined [4]:

- Reactive surety
- Proactive surety
- Preventive surety
- Fundamental, inherent surety

The four types of surety are a progression from intrinsically lower surety for reactive surety to the highest surety for fundamental, inherent surety. Each of the higher levels of surety depends on the lower levels to make the whole system functional.

**Reactive surety**  Reactive surety relies on the system working as expected. The system has been designed for reliable, safe, and secure operation with no special consideration of off-normal conditions. Insurance, warranties, and reactive responses mitigate consequences.
For example, the Romans planned for occasional damage and subsequent repairs,

“It will moreover be expedient...to build reservoirs at distances of twenty thousand feet from each other, because if damage be done to any part, it will not then be necessary to take the whole work to pieces, and the defective places will be more easily found” [9].

Proactive surety  Proactive surety relies on human action to control the environment, to operate the system reliably, and to respond in case of emergency.

The Romans had special maintenance personnel to respond to emergencies for the aqueducts. The personnel were divided in two groups,

“...some must be outside the City for purposes which do not seem to require any great amount of work, but yet demand prompt attention; the men inside the city at their stations at the reservoirs and fountains will devote their energies to the several works, especially in case of sudden emergencies...” [8].

Preventive surety  Preventive surety relies on positive measures from science and engineering. Positive measures are engineered controls and procedures incorporated specifically to improve surety. These measures are developed and maintained to control the environment, surety performance, and emergency response.

For example, the Romans had engineered an automatic water distribution and metering feature for their reservoirs within the city of Rome, such that, in time of insufficient supply, no water would be wasted on the ornamental fountains,

“...a reservoir (castellum) is built; with a triple cistern attached to it to receive the water. In the reservoir are three pipes of equal sizes, and so connected that when the water overflows at the extremities, it is discharged into the middle one, in which are placed pipes for the supply of the fountains, in the second those for the supply of the baths...in the third, those for the supply of private houses” [9].

Fundamental, inherent surety  Fundamental, inherent surety relies principally on the laws of nature. The goal of this type of surety is to incorporate these laws into the system such that undesired consequences become physically impossible to achieve.

For example, the Romans relied on a basic physical law (gravity) to clarify muddy and discolored water,

“...a settling reservoir was put in beyond the inlet of the aqueduct, in order that the water might settle there and clarify itself...” [8].

These four types of surety provide a framework for assessing the level of surety present in a system and provide guidance for increasing the level of surety when necessary. Selecting the best type of surety strategy to pursue depends on factors such as cost, schedule, feasibility, availability, maintainability, and producibility. However, certain factors, such as system requirements, regulations, and other internal or external drivers, may dictate the type of surety required.
Step 3: Realization

Step 3 designs and creates the solutions addressing the initial system problem. This is accomplished by developing a system model, designing positive measures, and developing metrics related to the surety requirements.

Develop system model: Developing a system model depends on decomposing a complex system into smaller, more analyzable subsystems. The subsystems selected must be small enough that their performance can be effectively analyzed, but large enough that the interdependent structural hierarchy of the subsystems remains tractable. Using the system model, metrics are developed to test the system against surety requirements and to weigh possible tradeoffs among the elements of surety or other programmatic issues. The system model also allows the interdependencies of surety elements and system elements to be examined. In this way, hazards that may be introduced inadvertently can be discovered.

While Frontinus held the office of water commissioner of Rome, he had minutely detailed drawings and models developed for the entire Roman aqueduct system, and states,

"By this provision, one reaps the advantage of being able to have the works before one’s eyes, so to speak, at a moment’s notice, and to consider them as though standing by their side" [8].

Design positive measures: Based on the system model, a strategy can be developed for eliminating, reducing, or mitigating the effects of hazards to an acceptable level of vulnerability. This strategy identifies (in a manner consistent with the surety theme and the applicable levels of surety) system and subsystem controls to maintain the desired levels of surety.

For the construction of cisterns for collecting water from rooftops and walls, the Romans described positive measures to maintain water clarity,

“If these receptacles are made in two or three divisions, so that the water may be passed from one to another, it will be more wholesome for use; for the mud in it will be thus allowed to subside, and the water will be clearer, preserve its flavour, and be free from smell...” [9].

Another positive measure practiced by the Romans was to cover well basins and aqueducts to protect the water from the immediate environment and the elements, such as sun and rain. To address the hazards posed by trees and buildings described above, the Romans made use of easements,

“...it is decreed that there shall be kept a clear space of fifteen feet on each side of the springs, arches, and walls; and that about the subterranean conduits and channels, inside the City, and inside buildings adjoining the City, there shall be left a vacant space of five feet on either side; and it shall not be permitted to erect a tomb at these places after this time, nor any structures, nor to plant trees. If there be any trees within this space at the present time they shall be taken out by the roots...” [8].

These examples illustrate that positive measures may include engineered features or administrative controls.
Develop metrics: Metrics must be established for each surety-critical control in order to measure its continued acceptable surety performance during operation.

The Romans were concerned with the amount of water delivered from each source to the city of Rome. They did not want to take more than their water rights allowed, but they wanted to be sure that they received all that they were entitled to. They measured the amount of water at the intake of the conduits, at several intermediate stations, and at the point of delivery. Using this metric, Frontinus states that,

“...it has...been discovered that 10,000 quinariae were intercepted...The cause of this is the dishonesty of the water-men, whom we have detected diverting water from the public conduits for private use” [8].

Step 4: Evaluation

Step 4 ensures the continued effectiveness of the system surety solutions. This step includes periodic assessments, surveillance programs, and configuration control.

Develop surveillance program: A continuous surveillance program is intended to ensure the system will maintain its level of surety throughout its life cycle. Surveillance also takes into account the changing technological and societal environment in order to revalidate the acceptance of residual risk that is inherent in any high-consequence system.

To ensure that the proper amount of water was always being delivered to Rome, Frontinus states,

“Frequent rounds must be made of channels of the aqueducts outside the City, and with great care, to check up the granted quantities. The same must be done in case of the reservoirs and public fountains, that the water may flow without interruption, day and night” [8].

Develop configuration control: Opportunities to compromise system surety by changes made to the system can occur throughout the system's life cycle. Configuration control is the process by which any proposed system changes are considered and approved before their implementation. This process must determine if any new hazards will be introduced or if existing controls will be bypassed if the change is implemented.

The Romans implemented configuration control to ensure that improper changes were not made to water outlets,

“Now whenever a stamped ajutage is larger than its legitimate measure it reveals designing dishonesty on the part of the deputy who stamped it; but when it is not even stamped, it clearly reveals the fault of all, especially of the grantee, also of the overseer. Care should therefore be taken, as often as an ajutage is stamped, to stamp also the adjoining pipe over the length which we stated was prescribed by the resolution of the Senate. For then and then only can the overseer be held to his full responsibility, when he understands that none but stamped pipes must be set in place” [8].
Step 5: Recovery

Step 5 embodies the system surety philosophy of planning for failure. This is realized by establishing an emergency response capability and by incorporating a lessons learned program.

Emergency response: At times, designs and products will fail, people will make mistakes, operational sequences will be out of control, and unexpected environments will occur. Personnel must periodically train, both in the classroom and in the field, to handle emergency conditions.

The Romans were prepared to deal with water distribution in emergency situations,

“In all parts of the City also, the basins, new and old alike, have for the most part been connected with the different aqueducts by two pipes each, so that if accident should put either of the two out of commission, the other may serve and the service may not be interrupted” [8].

Incorporate lessons learned: Understanding problems encountered on past and related systems can increase the possibility of finding latent failure modes and thus lead to more predictive assessments and advances in system surety. Rapid access to lessons learned is also essential for emergency response when events occur rarely and personnel have limited first-hand experience with similar incidents.

Frontinus was the first to collect information useful as a lessons learned program for the Romans,

“I have gathered in this sketch (into one systematic body, so to speak) such facts, hitherto scattered, as I have been able to get together, which bear on the general subject, and which might serve to guide me in my administration...The present treatise also may be found useful by my own successor” [8].

Role of Culture

The key to making the system surety approach succeed is a prevalent “bottom-to-top” organizational attitude concerning the importance of individual attitudes about surety [10]. But what is most important is upper management commitment that establishes and environment that promotes a surety culture. This surety culture in an industry or organization is the general attitude and approach to surety reflected by those who participate in that industry or organization. This includes all levels of staff, management, and government regulators. Major accidents often stem from flaws in this culture, especially overconfidence and complacency, a disregard or low priority for surety, or flawed resolution of conflicting goals [12]. Frontinus summarized his surety culture as the water commissioner of Rome,

“...the duties of water commissioner, an office which concerns not merely the convenience but also the health and even the safety of the City, and which has always been administered by the most eminent men of our State, now therefore I deem it of the first and greatest importance...” [8].

Organizational culture and independent assessment are synergistic. Culture should also differentiate between assessments and audits. An assessment evaluates the effectiveness or fundamental approach to an engineered process (validation). An audit evaluates compliance to a specified process (verification).
Some specific issues in organizational structure can enhance surety. These include concentrating responsibility and authority for surety along with decision making at high levels of management; independent surety organizations in the management structure; high-level status for surety personnel and their inclusion in critical surety decision making; and open communication channels for surety-related information.

**Role of Independence**

Basic management principles—the need for delegation of responsibility, authority, and accountability, and the establishment of clearly delineated lines of communication, cooperation, and administration—apply to surety just as they do to any other quality goals. The fundamental organizational component to ensure an effective system surety approach is the provision for independent assessment. Independent review and assessment is applied throughout the entire system surety approach. The independence of a surety assessment organization is critical to prevent the submersion of important surety issues when in conflict with other system needs.

The Romans also understood the need for independent assessment with regard to their aqueduct systems,

“...those who urge the construction or extension of the works cannot always be trusted. The water commissioner...must consult not only the architects of his own office, but must also seek aid from the trustworthy and thorough knowledge of numerous other persons...” [8].

**Applying System Surety to the Water Supply Infrastructure**

Important aspects of water supply infrastructure surety include water system reliability, water purity and safety, facilities safety and security, information safety and security, and interdependencies on other critical infrastructures, such as telecommunications, electrical power, and banking and finance.

To the degree that issues of water reliability, safety, and security are addressed, some elements of water supply infrastructure system surety are already practiced in the water industry today. The primary surety focus for the water supply industry is to provide a reliable supply of high-quality water that complies with all federal, state, and local safe drinking water laws. Included in this focus are water supply, treatment, and distribution systems.

**Surety Needs for the Water Industry**

Discussions between Sandia and water industry representatives have determined the need for a system surety approach to the water infrastructure. Identified needs include:
• Formalized surety tools and techniques relevant to the water industry
• Incorporating the system surety approach for evaluating the interdependence of regional water, wastewater, and solid waste disposal facilities and operations
• A surety evaluation regarding how to protect the total water, wastewater, and solid waste disposal infrastructure from shortfalls in maintenance, planned replacements, regional coordination, emergency response capabilities, and security

Surety Benefits to the Water Industry

Benefits to the water industry of implementing Sandia’s system surety approach may include:

• Highlighting the need for an independent water system assessment capability
• Providing tools for validating management decisions
• Developing dynamic models that incorporate economic justification for change
• Providing a regional and industry-wide look at water surety issues
• Providing a structured systems approach that gives water industry management additional credibility when addressing other government bodies

The system surety approach provides a proactive approach that can result in water systems exceeding standards of compliance. The surety approach can be applied to water transmission, treatment, distribution, and wastewater collection and treatment. Several ancillary systems and operations associated with the water supply infrastructure can also be included in a water system surety program. These ancillary systems include hydropower systems, dams and reservoirs, waterborne commerce and transportation, water recreation, and associated environmental issues.

A Brief Example of Applying Surety to a Water Supply System

This paper has explained the concepts of system surety using the water supply system for ancient Rome as examples. Now, however, it is necessary to see how these concepts work in a modern setting. Given the need for a new water supply system, how might the system surety approach be applied to the design and development of such a system? Examining all the subsystems of the supply system and all the details of the system surety approach as it relates to these subsystems would unnecessarily burden this introductory paper. However, a high-level look at how the approach can be applied to a hypothetical water supply may help to clarify the approach.

Portions of the five-step approach to system surety are addressed here: “Establish system objectives,” “Identify hazards,” “Determine surety theme,” “Design positive measures,” “Develop configuration control,” and “Emergency response.” Many more threats and synergies among threats and system operations exist for the hypothetical water supply than are treated in this example, but these few steps are sufficient to demonstrate the approach.
Step 1 Definition:

Establish system objectives  Customers expect “safe water, on demand, and at sufficient pressure” [7]. These three conditions constitute the objectives of the hypothetical water supply.

Identify hazards  Three hazards mentioned earlier in this paper that might emerge from any number of environments are water-borne disease, cyber-terrorists, and aging system components. The consequences of any of these hazards occurring could be a failure to meet the three system objectives of “safe water, on demand, and at sufficient pressure.”

Step 2: Strategy:

Determine surety theme  A surety theme based on isolation (through barriers and by providing continuous support) and incompatibility (using interlocking steps to prevent access to controls and by information incompatibility) can be used to address the hazards described above.

Step 3: Realization:

Design positive measures  Assuming the theme of isolation and incompatibility has been determined to be the correct one to address the identified hazards, what positive measures can be used to implement barriers, continuous support, interlocking steps, and information incompatibility?

Water-borne disease

Barriers and continuous support (isolation) were identified in the surety theme as necessary to deal with the hazard of water-borne disease. A barrier is defined as “…a method of blocking a threat from reaching a protected asset…” [10]. A filter designed to remove bacteria or viruses from water in the system can provide such a barrier. Continuous support is defined as “…protection through intimate association with an asset…” [10]. Continuous monitoring of water delivered to community storage tanks can ensure that the water is indeed free from contaminants. Such monitoring could be performed either by personnel or by remote instruments. A “trade-off” analysis of the benefits and drawbacks of these two courses of action would result in a decision about which method to implement. In other words, an appropriate type of surety is selected for this positive measure.

Cyber-attack

Interlocking steps and information incompatibility (incompatibility) are used to thwart cyber-attacks in this hypothetical water supply system. An interlocking feature is one that “…requires a threat to take distinctly different combinatorial and/or sequential dependent steps to reach a protected asset” [10]. The system pumps will be provided with backup power that is independent of the primary electrical grid. If a cyber-attack shuts down grid power to the pumps, the backup power system will automatically take over. Additional pumps will be provided at specific places along the pipes. These pumps will start automatically if water pressure drops dangerously low. These “makeup pumps” will not be dependent on or even connected to the primary electrical grid for power and will not be connected to the control network, but will require manual intervention to shut down. In order to prevent the system from supplying water on demand and at sufficient pressure, the cyber-attack would need to disable backup power to the main pumps and physically disable the makeup pumps, themselves.
To prevent a cyber-attack from reaching the main pumps in the first place, the system theme requires that the pumps respond only to information that is "...independently generated...in a prescribed...sequential pattern..." [10]. This is information incompatibility. In the case of this hypothetical water supply system, pump control information will only be considered valid if the pump controller receives two separate, but identical, control commands that have been routed through different nodes in the control network. A packet of control information will query the nodes through which it moves and collect information from each node that allows the packet to provide the controller at the pump with a sequence of nodes. If, and only if, both control commands show their correct path through the nodes will the pump controller respond to the commands. Each pump has a different set of "node maps" to which its controller will respond.

### Aging

Once again continuous support is used to provide protection against the hazards of aging pipes, pumps, or other system components. A regular, methodical inspection routine will determine components that need replacement.

**Step 4: Evaluation:**

*Develop configuration control*  Configuration control is intended to ensure that the positive measures are implemented correctly and that alterations of or revisions in the system design do not compromise these measures. For this water supply system, the filters designed to remove bacteria, viruses, and other contaminants must be a specific brand, model, and constructed with specific materials. The utility will randomly inspect filters from each lot provided by the supplier to ensure these requirements are met *before* any filters are accepted for initial installation or replacement.

Monitoring for water-borne diseases will be performed according to documented procedures by the utility at its facilities. An independent testing laboratory will inspect the utility's monitoring facilities periodically at unannounced intervals to ensure that the utility is producing valid test results during its monitoring.

Regular inspections by utility crews will look for system components that need replacement due to aging. An independent "watchdog" group will also perform random spot inspection of pipes, pumps, and other system elements several times during the year. These inspections will immediately follow those of the utility inspection crew in order to confirm the utility crews have properly diagnosed aging problems. The watchdog group will also inspect maintenance and monitoring logs for irregularities.

**Step 5: Recovery:**

*Emergency response*  No method or procedure will be able to account for every hazard: nature is too complex and human ingenuity too great. If the system is unable to meet its objectives ("safe water, on demand, and at sufficient pressure") at any time, a final plan for meeting at least some of the objectives is needed. In the case of this hypothetical water supply, the utility will have contracted with a number of water carriers to provide affected communities with safe water in some amount. In this way, at least one of the system objectives can be fully met (safe water) and another partially met (on demand) in off-normal conditions.

Several questions about implementing positive measures in this hypothetical water supply system may arise, or perhaps problems may be noted with the theme and its suggested positive measures.
The system surety approach is intended to elicit such questions as “What if?” “What about?” “Can we?” “Should we?” “Will it?” The iterative nature of the approach ensures that as many potential design or implementation pitfalls are discovered and addressed as possible before the final system design is settled on. And unlike many traditional engineering design approaches, system surety directly confronts the interaction of design decisions in one part of the system with those in another. In this way, the system surety approach attempts to provide an optimal solution to system design despite the numerous constraints imposed on any engineering project.

Conclusion

The executive branch of the United States government has acknowledged and identified threats to the water supply infrastructure of the United States. These threats include contamination of the water supply, aging infrastructure components, and malicious attack. Government recognition of the importance of providing safe, secure, and reliable water supplies has a historical precedence in the water works of the ancient Romans, who recognized the same basic threats to their water supply infrastructure the United States acknowledges today.

System surety is the philosophy of “designing for threats, planning for failure, and managing for success” in system design and implementation. System surety is an alternative to traditional compliance-based approaches to safety, security, and reliability. Four types of surety are recognized: reactive surety; proactive surety; preventative surety; and fundamental, inherent surety. The five steps of the system surety approach can be used to establish the type of surety needed for the water infrastructure and the methods used to realize a sure water infrastructure.

The benefit to the water industry of using the system surety approach to infrastructure design and assessment is a proactive approach to safety, security, and reliability for water transmission, treatment, distribution, and wastewater collection and treatment.

Acknowledgement

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

References


