Teaching Strategic Security Using A Case Study of Environmentally Sustainable Design

Matthew M. Mehalik
University of Virginia

I. Abstract

I present a case of a practitioner network that invented a secure environmentally sustainable textile product and production system. Once the practitioners created such a network, they struggled with how it would be possible to ensure that others external to the network, such as customers, were not able to dilute the very specific and documented accomplishments of their environmental analysis through their unintended introduction of less environmentally sound chemicals and processes. In this instance, the network practitioners struggled to protect an ethic of sustainable design from attempts at confusing its articulation and implementation. The practitioners also struggled with constructing a security system to ensure that undesired chemicals would not accidentally enter the manufacturing and logistical supply chain. The paper raises the question of how a sociotechnical network can be strategic in constructing what it deems as necessary security measures and why such issues should be taught to engineering students.

II. Case[1]

In August 1998, Albin Kälin, Managing Director of a Rohner Textil AG, a Swiss textile dye and weaving manufacturing facility, received an alarming phone call from one of his customers. This customer reported that he detected traces of permethrin, a moderately toxic pesticide, in tests he had run on samples of Climatex Lifecycle, Rohner Textil's flagship contract interior textile product that had won numerous environmental and interior design awards since 1995. Climatex Lifecycle had been certified by the independent consulting company, Environmental Protection Encouragement Agency (EPEA), based in Hamburg, Germany to be free from all pesticides, herbicides, carcinogens, endocrine disruptors, heavy metals, and biologically persistent toxic chemicals. The EPEA founders and scientists consisted largely of staff members formerly associated with Greenpeace Germany's Chemistry Division. They used this expertise to ensure that Rohner Textil's products and manufacturing operations were a model to the world in how it was possible to be economically successful and environmentally responsible (stories of the development of Climatex Lifecycle, the history of Rohner Textil AG, and the EPEA have been documented elsewhere).[2,3,4]

Kälin was stunned by this report. He had spent the previous five years assembling an international network[5] of experts and checking systems, such as quality and environmental management, continuous improvement, and outside review systems under the ISO 9001 and ISO

14001 standards, employee training programs, oversight from the EPEA, and the environmental advocacy organization Deutsche Umwelthilfe.[6] These and other checking systems were perhaps the most comprehensive attempt a company had made at ensuring the environmental quality of its products and processes. Kälin was aware that the failure of this system would likely have a devastating impact on his company's reputation in the marketplace if the system consistently permitted the intrusion of permethrin (or other chemicals) into the product. Perhaps the discovery of permethrin was an isolated incident. Perhaps it was something that occurred while the client was handling the product. Or, perhaps Rohner had been shipping contaminated products to many customers. Kälin did not know at the conclusion of the phone call with his client, but he knew he had to find out more about the situation.

He immediately called upon his quality management staff and the EPEA for a plan to discover the source of the problem. The EPEA pointed out that the discovery of permethrin could not be explained in terms of the design, because the EPEA had certified that all of the source materials, dyes, and finishing chemicals were free of pesticides, and all of the suppliers in the supply chain did not use any pesticides in any parts of their operations. The permethrin entered the system in some other way. The team ran tests for six months at various points in the supply chain and manufacturing operations to see if the source could be identified. No source could be identified at that time. Eventually, several months later, the team discovered that the client had used permethrin as a pesticide in its company showroom, and the chemical migrated through the air into the samples that the client had tested and that had shown positive results for permethrin.

At one level, the team was relieved that they had found the source of the chemical. At another level, they were very concerned that Rohner needed to find a way to try to try to influence the way its products are used even after they have left the company and a way to demonstrate that the products that they were making and selling were indisputably in line with the environmental claims they were making about their products. The concept that the team settled upon over the course of the next year consisted of two key parts: 1. Make sure that all parts of the processing chain at the company were well-specified, meaning that employees needed to continually anticipate any possibilities for undesired chemicals to enter the production process and to take actions to make sure they did not. They needed to find out what the indicators might be and what types of sampling should be conducted if something did happen to enter the system. 2. The EPEA would establish a list of chemicals that each supplier and customer used so that there could be risk projections at different parts of the supply chain. That way, if a problem did occur, the likely source of the problem could be tracked down in a matter of a few hours and could be stopped quickly.

In this case, no problems were found in other customers' products, no serious damage to the reputation of Rohner Textil AG, Climatex Lifecycle, or the EPEA occurred, and the reporting customer remained loyal throughout the process. The network continued to win awards for new environmental innovations, and Climatex Lifecycle continued to do well, in spite of very difficult economic conditions with the global manufacturing slowdown that lasted through the last quarter of 2001.

III. Discussion

Security failures and systems that end up doing something other than they were designed or intended are topics that engineering students will undoubtedly pay closer attention to in the wake of the September 11, 2001 attacks. On that date terrorists exploited weaknesses in the security system by sneaking box cutter knives past airport screening posts and took control over four planes, which were turned into weapons instead of their intended design for safely transporting people. In this case immoral actors calculated system weaknesses and exploited these weaknesses. Engineers also face situations in which problems arise because of organizational and representational structures that enable system failures. In many such cases the actors are following engineering codes and what are believed to be best practices at the time.

In his book *Inviting Disaster*, James R. Chiles[7] chronicles a history of engineering disasters ranging from boiler explosions from the mid-19th Century through the crash of the Concorde in July 2000. Chiles points out that most failures result from the coupling of several system weak points into what eventually become chains of failure. With a glimpse of hope, Chiles writes that even when several events along a failure chain begin to become linked, there are "opportunities for people to break the chain and stop a system failure before it reaches its peak. But their chances to respond may be difficult to recognize, fleeting in time, and even more difficult to act upon. Managers and supervisors may resist; workers may not care enough or know enough to do anything."[8] It is this last point that I argue needs to be discussed in engineering education. Engineering students need to become engaged in conducting analyses in order to sensitize them to how such chains of failure come to be and how they can take actions in an organization to break the chain. Discussing case studies such as the Rohner Textil case are helpful. Such discussions are most effective when paired with some analytical tools that teach students how to be strategic about discovering, analyzing and making decisions in the midst of a system's operation to limit or prevent the capacity for failure.

In her book analyzing the Challenger launch decision Diane Vaughn[9] discusses the concepts of structural secrecy and normalization of deviance in organizations that can (and did) contribute to system failures. Structural secrecy refers to the compartmentalization of one component of an organization from another; therefore, people working in one component do not know what is happening in another component. NASA managers may not have agreed to launch the Challenger if some of the reservations in other contractors and parts of NASA could have been communicated before the launch. Structural secrecy made it difficult for these reservations to surface and make a difference to stop a chain of failure.[10] Normalization of deviance refers to cases in which work-around procedures, which serve as temporary ways of completing tasks or making decisions, in effect, become the routine. This puts added pressure on systems and can lead to overconfidence in the system's capabilities, enabling chains of failure.[11]

The Rohner Textil case illustrates the efforts that the protagonists made to try to reduce structural secrecy in the supply chain and the manufacturing processes. First, the EPEA required that all components of the raw materials and production chemistry be open to an audit to certify that they did not contain harmful chemicals. Second, once a problem was detected, they further attempted to reduce structural secrecy by requiring customers to provide information about their practices in an attempt to gage the risks of potential product contamination. The case also shows how the network of practitioners tried to eliminate normalization of deviance in the production chain. Once they detected the presence of the polluting chemical, they changed their policies so that employees documented their procedures while paying attention to any special risks due to contamination. The ISO 14001 system and its auditors ensured that all documented processes were up-to-date and reflected the actual practices, therefore reducing/eliminating the number of work-around procedures.

In *The Logic of Failure*, Dietrich Doerner[12] describes some of the characteristics of successful and unsuccessful groups who participated in decision exercises designed to simulate the operation of complex systems, such as food distribution in developing villages. Among many other characteristics, Doerner noted that participants who did well in making decisions tended to formulate a large number of hypotheses about what were the critical problem areas. The successful participants also attempted to test their hypotheses in as many ways as possible. Participants who did not do as well tended to stick with fewer hypotheses and resisted testing or scrutinizing them.[13] Another characteristic of decisions that lead to potential system failures is the tendency to think in terms of isolated cause and effect relationships, or a tendency to simplify events over time, space and side effects.[14]

In the Rohner Textil case, the practitioners engaged in a comprehensive review of the entire production chain, from raw materials to the customer practices in order to try to find the source of contamination. They did not focus on a single hypothesis, but tested multiple hypotheses that ultimately led them to the customer's showroom. No single cause led them to this source; instead, it took many iterations and revisions that led to the discovery.

Patrica Werhane[15] argues that moral imagination is necessary for making good design and business decisions that can limit the possibility of failure. Exercising moral imagination involves: 1. Disengaging oneself from one's role, one's particular situation or context. 2. Becoming aware of the kind of mental model one has adopted. 3. Creatively envisioning new possibilities. 4. Evaluating the old scripts and mental model, any alternative frame, schema or mental model, and new possibilities.

In the Rohner Textil case, several members of the network had engaged in moral imagination in order to resolve the issue of contamination. The customers shifted perspectives in order to permit the EPEA to document aspects of their operations in order to gage the risks of contamination. This was a shift from a strict perspective of proprietary concerns to one of more open sharing directly related to the use of the product. The EPEA personnel shifted from the perspective that there could not be contamination because the upstream levels of the supply chain were certified to be free from any harmful production processes that could have permitted the entry of a pesticide in the system. Kälin shifted perspectives in order to make sure that changes could occur at his production facility to promote greater security in operations.

Mehalik and Gorman[16] have proposed a three-state framework to help structure the ability to use moral imagination. They have written that by articulating some of the social structures in which a decision maker works, the decision maker can have a more sophisticated picture in which moral imagination can function as a strategic tool. The three states incorporate some of the strategic characteristics discussed so far in this paper. The framework focuses on how various components of a complex system and network can function in various states of alignment with the intended purpose of the system. In a state 1 system, all components are in close alignment with a single perspective, with each component playing a singularly defined role. An example of such a system is a totalitarian regime. In a state 2 system, the components are in alignment with two or more competing perspectives, but the system still functions because trading zones are created that permit dual or multiple roles of the components. Most contractual arrangements for supply chains operate in this way. In a state 3 system, the components are free to organize themselves in according to whatever roles they may play, as long as there is continual sharing of any changing perspectives that may occur in the system. An example of such a system may be partners in a business. [17]

In the Rohner Textil case, increased security resulted from a shift from old state 2 relations (for example, between suppliers) to a state 3 in which new roles for the network members could be re-negotiated to incorporate the changes in the supply chain. Once the new roles were negotiated, the system settled back into state 2 trading relationships throughout the supply chain. Capability in shifting states (using moral imagination) was one way in which the network prevented additional problems in its supply and customer chain operation and in which the permethrin problem was resolved quickly. The result of this ability to shift was increased security in the way that system functioned.

This result is exactly the opposite of what many people would think promotes more security. Current trends are to shift into even more rigidly constructed roles aligned according to a single perspective (state 1). Shifting to a state 1 does reduce any deviance in the network, but it also promotes structural secrecy by narrowing the ability of network components to interact. It also reduces the ability for network members to construct and test multiple hypotheses, to look for more complex linkages of cause and effect, and to facilitate the use of moral imagination. In other words, a shift into a state 1 situation may provide more control in alignment with a single perspective; however, this does not guarantee that the system will be more secure. In fact, it will likely reduce the security of how the system functions.

IV. Conclusion

Integrating all of these conceptual tools and teaching them in the context of case studies of real world complex system operations provides students with a more sophisticated way to be strategic about their decision making skills and to be more capable of understanding the consequences of technology in operation. Unintended consequences of technology cannot always be anticipated. However, as Chiles mentions, “When an organization develops people who are capable experts at picking out the subtle signals of real problems from the constant noise of routine difficulties, and when the boss allows them to report and take prompt action, that organization is doing the same thing that chess masters do.”[18]

The Rohner case is an example that illustrates that failures can occur even when engineers, scientists, and managers are following a rather stringent, proactive approach towards socially responsible design. The case also shows that it is likely that such best practices prevented the problem from becoming a major disaster that could have produced contaminated products and distributed them to a wide network. It also shows that once a problem was detected, the network of practitioners responded quickly to isolate the problem, find its source, and revise its practices to make the system even more sensitive and responsive to chemical security issues along the production chain. The case illustrates that the decision makers exhibited some of the characteristics that others have put forth associated with increasing the chances for keeping systems operational, and it illustrates some characteristics that point to ways for increasing the security of its intended use.

Bibliography

1. Information about this case was supplied through telephone email correspondence with Albin Kaelin, Managing director, Rohner Textil AG, from July – September 1999.
2. Gorman, M. E., M. M. Mehalik, and Patricia Werhane. (2000). Ethical and environmental challenges to engineering. Englewood Cliffs, NJ, Prentice-Hall.
3. Kälin, Albin. (2001). "The Development of Climatex Lifecycle, a Compostable, Environmentally Sound Upholstery Fabric." Sustainable Solutions: Developing Products and Services for the Future. Martin Charter, Ed. Sheffield, UK: Greenleaf Publishing.
4. "Welcome to Rohner Textil AG, Manufacturer of Climatex Lifecycle." Corporate Website. Online Posting, 15 January 2002. <http://www.climatex.com>.
5. Mehalik, M. M. (2000). "Sustainable Network Design: A Commercial Fabric Case Study." Interfaces: *Special Issue: Sustainable Business*. Vol. 30, No. 3 (May-June). 180 – 189.
6. Mehalik, M. M. (2000). "Technical and Design Tools: The Integration of ISO 14001, Life Cycle Development, Environmental Design and Cost Accounting." ISO 14001 Case Studies and Practical Experience. Ed. Ruth Hillary. London: Greenleaf Publishing.
7. Chiles, James R. (2001). Inviting Disaster: Lessons from the Edge of Technology. New York: Harper Business.
8. Chiles 7.
9. Vaughan, Diane. (1996). The Challenger Launch Decision: Risky Technology, Culture, and Deviance at NASA. University of Chicago Press, Chicago.
10. Vaughan 397 - 399.
11. Vaughan 409 - 415.
12. Doerner, Dietrich. (1996). The Logic of Failure. Reading, Massachusetts: Perseus Books.
13. Doerner 19 – 28.
14. Doerner 34 – 35.
15. Werhane, Patricia Hogue. (1999). Moral Imagination and Management Decision Making. Oxford University Press.
16. Mehalik, Matthew M. and M. Gorman. (2001). Understanding Moral Imagination: Applying A Network State Framework to Cases of Inventing for the Environment. Proceedings of the American Society of Engineering Education. Albuquerque, NM.
17. See Mehalik & Gorman for more examples and clarifications regarding the tree states framework.
18. Chiles 15.

MATTHEW M. MEHALIK

Matthew Mehalik is a postdoctoral teaching and research associate in the Division of Technology, Culture and Communications at the University of Virginia. He holds a Ph.D. in systems engineering and an ethics and policy option from the University of Virginia, a program completed in May 2001. His research area involves exploring sociotechnical network analyses for new technology and process designs.