

Motivation for a new approach to the US food hazard control system

The food supply in the United States is one of the safest in the world. However, the US Center for Disease Control (Scallan, Hoekstra et al. 2011) estimates that each year 47.8 million food borne illnesses occur, resulting in more than 127,389 hospitalizations and 3037 deaths. The Pew Foundation (Scharff 2010) estimates annual financial losses to be \$152B. The deaths, health care costs, loss of confidence in the food supply, and the loss of productivity make continued efforts to reduce food-borne illnesses a major societal need.

The US food production system is now undergoing unprecedented change. Consumers worldwide are seeking healthy, fresh food regardless of the growing season. These changes to the food system are leading to global supply of foodstuffs that transcend national boundaries. In addition, millions of people are moving from subsistence to middle class lifestyles, upgrading their diets to include animal protein.

These changes are restructuring the food production system. Current approaches to logistics, agronomy, and safety are based on assumptions that are no longer true. Tauxe, et al (Tauxe, Doyle et al. 2010) report on a number of changes taking place in the world food production system that are changing the way food issues should be addressed. For example, methods that kept food safe in the past need re-evaluation as food supplies are shipped globally. A systems view of food safety will bring a new perspective to controlling food borne illness in today's complex and global food production system.

A systems approach to food hazard control

The aim of food safety programs is the prevention of pathogens from reaching the consumer. This prevention is accomplished by a combination of barriers and kill steps. This type of prevention strategy is grounded in a common accident causation model, a chain-of-events model. This model treats accidents as a linear series of events that result in an accident. Therefore, food safety programs prevent accidents by breaking a chain-of-events. This model of accident causation works well for simple systems. This model of accident causation can be seen in the FDA's approach to inspection of facilities and finding violations of standards that then are declared the "cause" of accidents.

As systems become more complex through size, extensive connectivity or computer automation, the simple linear models are no longer adequate. In particular, the simple models are not capable of dealing with component interaction accidents. These interaction accidents are the result, not of component failure, but of complex interaction between components. New and different models grounded in system theory are needed to understand and eventually prevent accidents in complex systems. These system models have developed over the last 20 years.

System models treat safety as an emergent property of the whole system. Rather than focusing on identification and control of failures, system models treats safety as an emergent property of the system. Therefore, the management of safety is handled as a control problem of the system rather than a series of events or failures to be managed. Under a system approach, maintaining safe food

can be thought of as a control problem. Food borne illnesses are the result of ineffective control of processes, such as sanitation procedures, preventive maintenance, or regulatory enforcement.

These system models are based on system control theory. System control theory was developed to understand how complex systems are controlled. Complex systems, like the food production system, can be broken down into hierarchical control structures. According to system theory, the top level of the system enforces control on the one below through a feedback control loop. The second level in turn controls the level below it. This control enforcement cascades down through the system levels until it reaches the bottom level. The resulting structure is called the hierarchical control structure. The control objective is to enforce the system goals and constraints. In food production, the control structure is built of a number of regulations, processes, and technologies.

STAMP: A Systems Approach to Accident Causation

STAMP (System Theoretic Accident Modeling Processes)(Leveson 2004) (Leveson 2011) was developed to model accident causation in complex systems, such as the food production system. Its origins are in software and aerospace safety; STAMP has been applied to pharmaceuticals (Couturier 2010) and water safety (Leveson, Daouk et al. 2003).

Leveson, responding to the need to determine if software is “safe”, described (Leveson 1995) a system theoretic approach to safety. The essence of the approach is to treat safety as an emergent property of the system, rather than a by-product of component reliability. The emergent property is the result of a constraints imposed by the higher levels in the system hierarchy on the lower levels. Successful imposition of these constraints from one level to the next throughout the system results in the emergence of a safe state. The collective imposition of these constraints forms the hierarchical safety control structure of the system. A description of the possibilities of STAMP for food safety were described by Leveson and Couturier (Couturier and Leveson 2009).

STPA, System Theoretic Process Analysis, is a prospective method used to identify hazards during the system design process. STPA has been used on a number of systems, such as air traffic control, and has been shown to identify more hazards than traditional hazard analysis techniques such as fault tree analysis.

STPA in Action

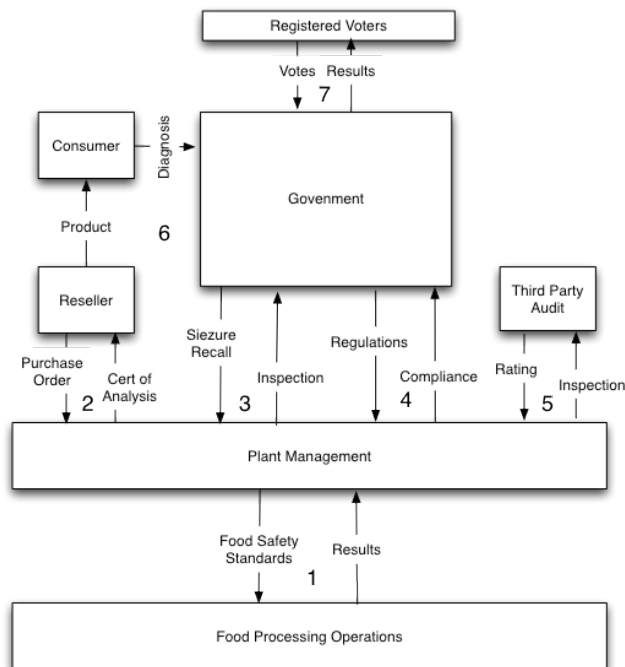
The food system safety constraint to prevent food borne illness is: **No pathogenic bacteria in food at point of consumption.** STPA identifies hazards by examining how the system control structure can be ineffective in enforcing the system safety constraints.

The first step in a STPA analysis is to determine the safety control structure that enforces the system safety constraints. To explain the hierarchical control concept, consider a simplified control system for a generic food production process. The control loops are described in the table below:

STAMP and Food Safety

August 8, 2011

Food Production: Simplified Safety Control Structure

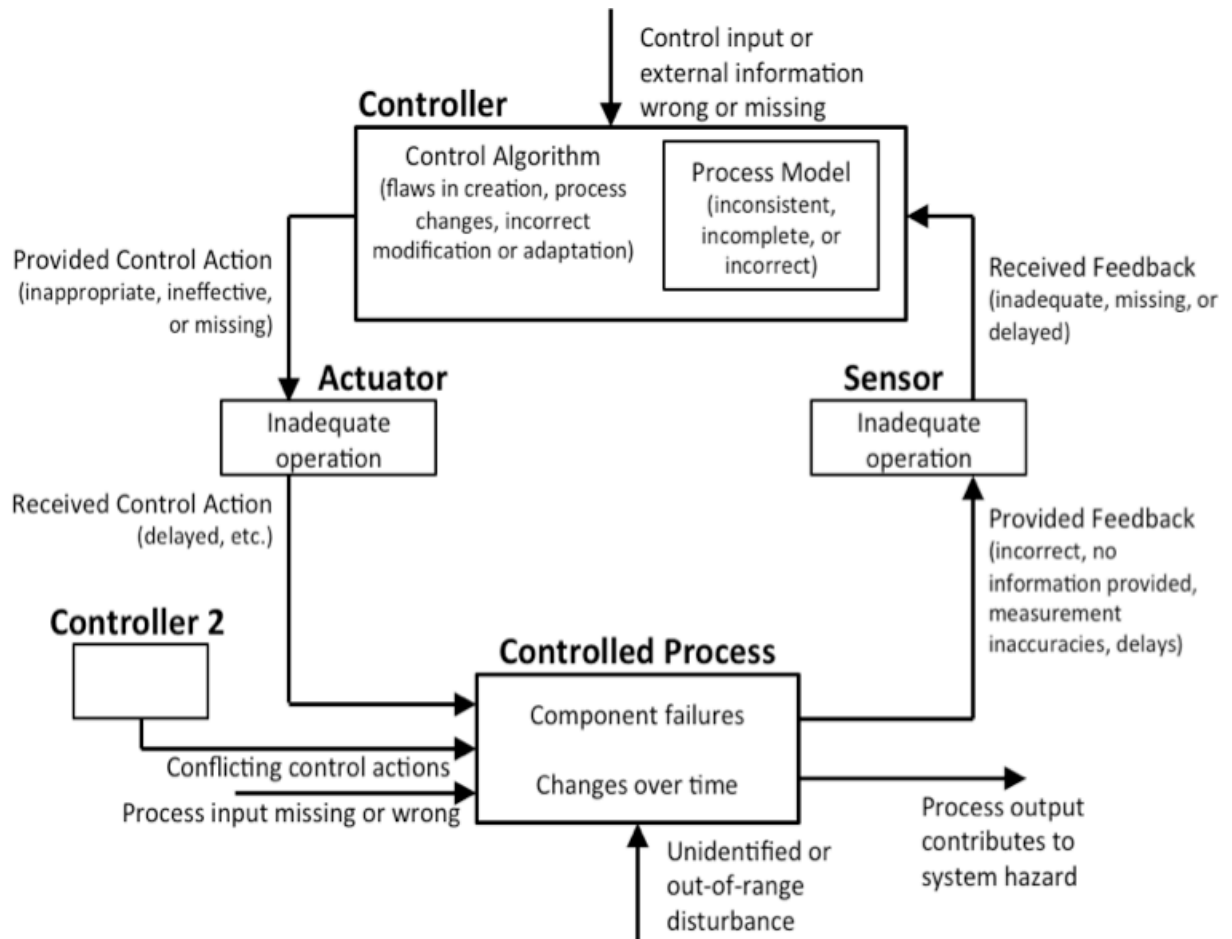


Loop	Control Loop Details
1	Management exerts control on the process by converting regulations into standards that the operations must meet. Loop 1 operates at least daily and enforces the safety constraints at the process level. This loop is designed to prevent the entrance of pathogens into the food or control them if they are present in the food during processing. Loop 1 is based on both GMPs and HACCP.
2	The customer feedback loop. If the product does not meet the customer requirements for safety, the food is rejected and the customer will not re-order. If enough customers are lost, the supplying firm will cease to operate. This is a reactive loop and somewhat slow, but it is powerful as it shuts down the production of food that does not meet the safety constraints of the customer.
3	The regulatory inspection loop. This is operated rather infrequently relative to the operational throughput time, on the order of once a year or less. While slow and reactive, the regulators have it in their power to seize product and suspend licenses resulting in closure of the enterprise.
4	The legislatures and executive branches of the appropriate government establish and enforce food safety laws and regulations to control food establishments
5	The third party audit loop; an independent non-governmental inspection of the facility. This can be paid for by the supplier or the customer and is usually conducted on an annual basis.
6	The actual performance of manufactured products in the marketplace, Loop 6 is only activated when an outbreak occurs.
7	The election, by registered voters, of legislators and executives to manage, among many other things, the food safety regulatory environment.

The next step in the STPA method is to analyze each control loop to understand how the loop enforces the system safety constraints and if it is ineffective in enforcing safety constraints. To explain this, consider this diagram of a control loop:

August 8, 2011

The control loop has four elements, the controller, the sensor, the actuator and the process under control as shown here:



The STPA analysis first examines the controller element of the control loop and asks the following questions:

1. Safety Responsibilities – What specific safety responsibilities does this control loop have?
2. Inadequate control actions – What inadequate control actions are attributable to this loop? Where the control actions incorrect, missing, too early or too late?
3. Context in which decisions made - What pressures from the environment were on the control loop? In what context were control decisions taken in?
4. Process model flaws - What process model flaws were in the controller? What were the gaps between the controller's understanding of the process and the actual process?

For example, how would loop 1 controller be analyzed in a generic food safety accident? In this case, the controller is plant management, the actuator is the safety standards dictated by management, the process is the food manufacturing operation, and the sensor is data regarding food safety compliance from operations.

Loop	Safety Responsibilities	Inadequate control action	Context in which decisions made	Process or Mental model flaws
1 Controller	Loop 1 enforces the system safety constraint: no pathogens in the food. It does this by establishing food safety standards for operations, ie testing frequency for pathogens in product.	The controller is examined to ensure that food safety standards were complete, correct and communicated in a timely fashion.	Were decisions taken under financial pressure, was the environment around the facility conducive to pathogenic contamination?	The controller's mental or process models do not match the actual process

The following excerpt from a forthcoming paper by Thomas and Leveson, (Thomas, et al forthcoming) describes the process to determine causes of inadequate control actions.

The second step of STPA examines each control loop in the safety control structure to identify potential causal factors for each hazardous control action, i.e., the scenarios for causing a hazard. The figure above shows a generic control loop that can be used to guide this step. While STPA Step One focused on the provided control actions (the upper left corner of the figure above), STPA Step Two expands the analysis to consider causal factors along the rest of the control loop.

Consider a hazardous control action for Loop 1 in the generic food example: product is ordered shipped before pathogen test results are received. STPA Step Two would show that one potential cause of that action is an incorrect belief that the pathogen testing results have been received and were negative (an incorrect process model). The incorrect process model, in turn, may be the result of inadequate feedback provided by a failed sensor or the feedback may be delayed or corrupted. Alternatively, the designers may have omitted a feedback signal.

Once the second step of STPA has been applied to determine potential causes for each hazardous control action identified in STPA Step One, the causes should be eliminated or controlled in the design.

References

Checkland, P. (1981). "Systems thinking, systems practice." NY,NY, John Wiley

Couturier, M. and N. Leveson (2009). "Re-engineering the United States food safety system." Food Protection Trends **29**(9): 571-576.

Couturier, M. M. J. (2010). A case study of Vioxx using STAMP. Technology and Policy Program Masters Thesis. Cambridge MA, MIT.

Leveson, N. (1995). SafeWare : system safety and computers. Reading, Mass., Addison-Wesley.

Leveson, N. (2001). Evaluating Accident Models using Recent Aerospace Accidents, NASA IV&V Report. June 28,2001

Leveson, N. (2004). "A new accident model for engineering safer systems." Safety Science **42**(4): 237-270.

Leveson, N. (2011). Engineering a Safer World. Cambridge MA, MIT Press.

Leveson, N., M. Daouk, et al. (2003). Applying STAMP in accident analysis NASA CONFERENCE PUBLICATION 2003, ISSU 212642, pages 177-198

Scallan, E., R. M. Hoekstra, et al. (2011). "Foodborne illness acquired in the United States--major pathogens." Emerging infectious diseases **17**(1): 7-15.

Scharff, R. L. (2010). "Health-Related Costs From Foodborne Illness in the United States." Produce Safety Project at Georgetown University.

Thomas, J., Leveson N. (forthcoming) "Performing Hazard Analysis on Complex, Software- and Human-Intensive Systems"

Tauxe, R., M. Doyle, et al. (2010). "Evolving public health approaches to the global challenge of foodborne infections." International Journal of Food Microbiology **139**: S16-S28.