A Systems Theoretic Accident Model Applied to Biodefense

Joseph R. Laracy
Complex Systems Research Laboratory, Engineering Systems Division, MIT

Preprint of article appearing in:
Defense & Security Analysis Vol. 22, No. 3, pp. 301–310, September 2006

Introduction

The United States and its allies face an ever growing danger from the use of biological weapons as an instrument of terror. Unlike traditional bombs which rely on an uncontrolled release of energy to damage surrounding people and structures, biological weapons utilize the complex dispersion mechanism of disease. Delivery systems range from missiles to aircraft to land dispersal systems such as aerosol spray trucks. The pathogens themselves vary significantly as well. The Anthrax bacteria is spread by a powder or liquid but both a antibiotic and vaccine exist. On the other hand, Hemorrhagic Fever Viruses (HFVs) which are spread by a vector have essentially no treatment options. Clearly, a robust, comprehensive approach must be utilized to manage such a dynamic threat.

New strategies must be developed to prevent an attack as well as manage the aftermath. Informal, ad hoc approaches will almost certainly fall short of accomplishing the desired goal of little to no casualties. The public response which in many ways was encouraged by Federal leadership involving the hoarding of duct tape and plastic wrap during the Anthrax attacks shows the dire need for better strategies. A rigorous, systematic method is necessary to develop an appropriate approach. Traditional mathematical modeling with differential equations[1] and recent work in genetic algorithms[2] have made significant contributions to this end. However, according to John Sterman, "The greatest potential for improvement comes when the modeling process changes deeply held mental models."[3] The author proposes an approach which brings the power of control theory in an accessible way to public health professionals and policy makers involved in Biodefense.[*] Specifically, it changes mental models because it reframes the issue as a control problem as well as shows the

[*] The model's contribution is to Biodefense in general, rather than Smallpox in particular. Smallpox is presented as an example because its properties are well characterized and there is a certain degree of shared knowledge on the topic that makes the article accessible to a large audience.

dynamics of disease and responses to disease in an accessible way that doesn't require mathematical sophistication.

Systems Theoretic Accident Models and Processes (STAMP)

STAMP was developed at MIT by Nancy Leveson as part of a comprehensive investigation of system safety engineering.[4] The theory has led to a rigorous hazard analysis technique, STPA, STamP-based Analysis[5] as well as methodologies for performing accident reconstruction[6] and general safety analysis. STAMP has been applied in systems ranging from aerospace platforms[7] to organizational risk analysis for NASA[8]. It is unique in that while traditional approaches view component failure as the source of accidents, STAMP incorporates dysfunctional component interaction and external disturbances as well. Therefore, accidents occur when there is "inadequate control or enforcement of safety-related constraints on the development, design, and operation of the system." This approach transforms the question into a control problem. Without adequate control, exercises such as Dark Winter have shown that Smallpox would spread in the United States with exponential growth.[9]

There are many ways that inadequate control can lead to an accident. Leveson developed a useful categorization scheme which captures most control flaws. Broadly, they fall into one of three categories: Inadequate enforcement of constraints, inadequate execution of control actions, or inappropriate or missing feedback. The table below provides more detail for categorizing flaws.

1. Inadequate Enforcement of Constraints (Control Actions)

1.1. Unidentified hazards

1.2. Inappropriate, ineffective, or missing control actions for identified hazards

1.2.1. Design of control process does not enforce constraints

1.2.1.1.Flaws in creation process

1.2.1.2.Process changes without appropriate change in control (asynchronous evolution)

1.2.1.3.Incorrect modification or adaptation

1.2.2. Process models inconsistent, incomplete, or incorrect

1.2.2.1.Flaws in creation process

1.2.2.2.Flaws in updating process (asynchronous evolution)

1.2.2.3.Time lags and measurement inaccuracies not accounted for

1.2.3. Inadequate coordination among controllers and decision makers (boundary and overlap areas)

2. Inadequate Execution of Control Action
   2.1. Communication flaw
   2.2. Inadequate actuator operation
   2.3. Time lag
3. Inadequate or missing feedback
   3.1. Not provided in system/organizational design
   3.2. Communication flaw
   3.3. Time lag
   3.4. Inadequate detection mechanisms

Leveson's "Classification of Control Flaws Leading to Hazards" modified for Biodefense[10]

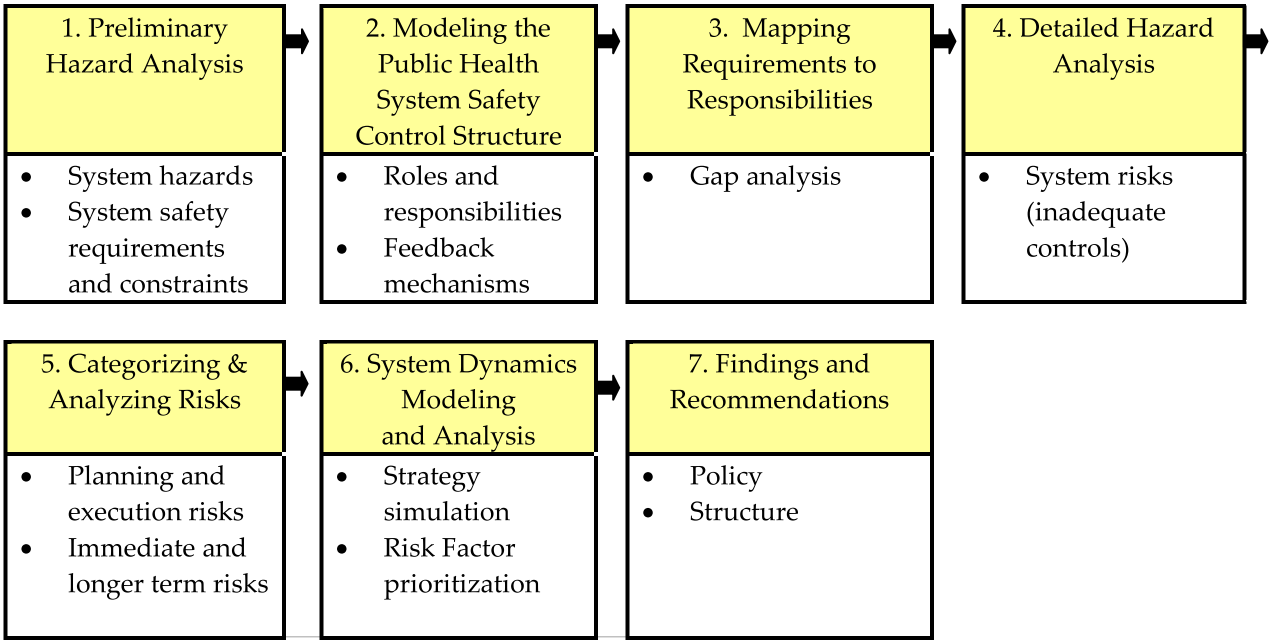
To capture the behavioral dynamics of a system, a socio-technical modeling technique called System Dynamics is used. System Dynamics was developed at MIT in the 1950s by Jay Forrester. Its theoretical basis comes from control systems and non-linear dynamics. Complex systems, whether they are technical, organizational, or some combination, often exhibit highly non-linear behavior where the relationship between cause and effect is not intuitively obvious. System Dynamics models are constructed by a combination or positive (reinforcing) and negative (balancing) feedback loops in addition to stocks and flows.[11] Very simply, a system dynamics model is a system of non-linear differential equations presented in an easy to understand graphical form accessible to policy makers. The models can be easily simulated to obtain numerical results.

Unlike events which are normally termed "accidents," where no individual or group intended for the loss to occur, acts of bioterrorism are obviously purposeful, willed acts. As such, the causation model must take the relevant causal factors into account. David Zipkin's work in modeling computer viruses and internet worms shows that the theory is still applicable in dealing with "non accidental" events.[12]

The system under consideration is the US public health system. It contains the population as well as the healthcare, pharmaceutical, and governmental entities. A complete analysis cannot be presented in a few pages of this journal. This paper will focus on a very specific situation to demonstrate the applicability of the technique. Using the STAMP framework, a Smallpox attack is the accident which must be avoided. Smallpox is a virus which can be spread by aerosol, vector, missile, or human contact. The disease is characterized by an incubation period of seven to seventeen days and a thirty percent mortality rate. A vaccine does exist. As an example in this paper, the suitability of a just-in-time (JIT) vaccination strategy will be explored.

Risk Analysis

The graphic below captures the risk analysis developed by Leveson and Dulac during their work applying STAMP to the NASA Independent Technical Authority organization.[13] It is modified for Biodefense.



1. Preliminary Hazard Analysis
- System hazards
- System safety requirements and constraints

2. Modeling the Public Health System Safety Control Structure
- Roles and responsibilities
- Feedback mechanisms

3. Mapping Requirements to Responsibilities
- Gap analysis

4. Detailed Hazard Analysis
- System risks (inadequate controls)

5. Categorizing & Analyzing Risks
- Planning and execution risks
- Immediate and longer term risks

6. System Dynamics Modeling and Analysis
- Strategy simulation
- Risk Factor prioritization

7. Findings and Recommendations
- Policy
- Structure

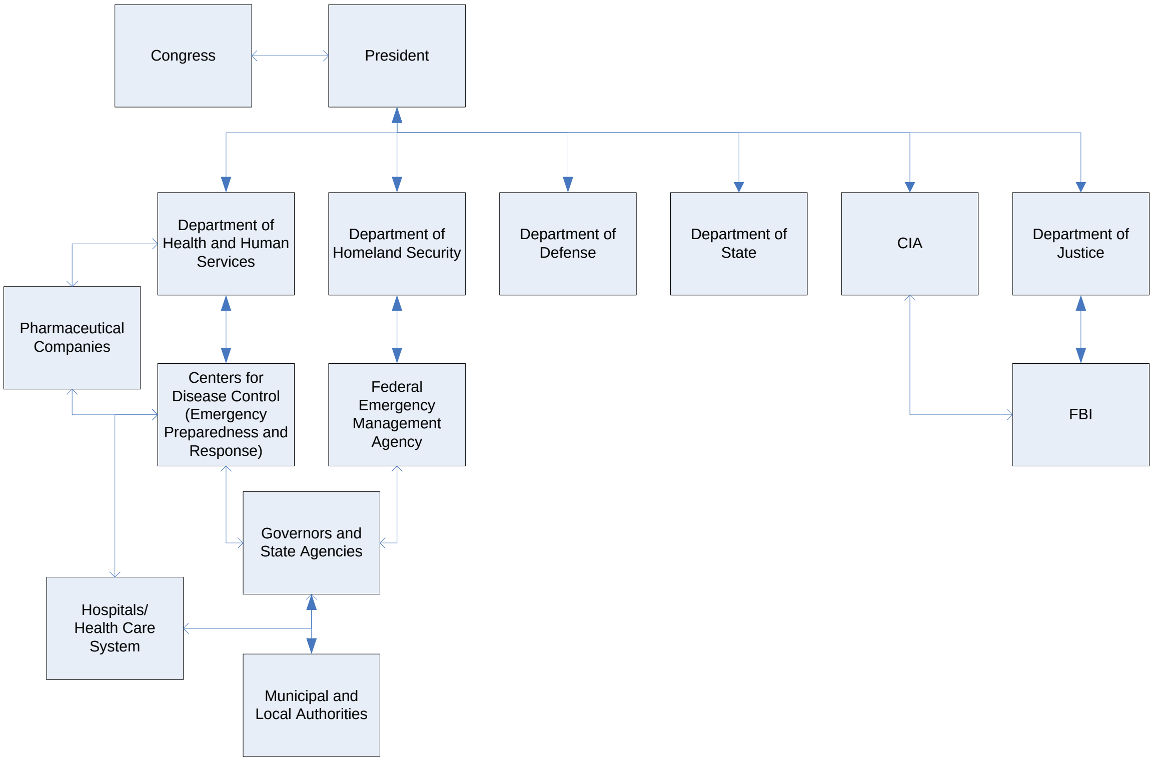
The first step in a STAMP based risk analysis is to define the high-level system hazards. After they are defined, hazards should be transformed into requirements or constraints which manage them. The primary, high level hazard is: Poor planning and decision making permits a biological attack on the US. Once an attack is successfully carried out, the situation shifts so that the hazards listed below become relevant.

Hazards	Requirements/Constraints
Infected people are permitted to spread the infection outside their region.	Infected people shall be quarantined under Federal authority.
The number of people that are permitted to contract Smallpox exceeds the amount of vaccine.	Sufficient vaccine shall be on hand to quickly immunize vulnerable people before an epidemic arises.
First responders are incapacitated by	First responders shall be vaccinated

Smallpox and are unable to execute the Biodefense strategy.	before the outbreak of disease.
Local, State, and Federal response efforts are inconsistent and counterproductive.	A comprehensive, coherent strategy shall include all levels of government.
The medical system is quickly overwhelmed in the very early stages of the outbreak and unable to respond to the attack.	The medical system shall have adequate personnel, supplies, and strategy to respond early and effectively to an outbreak.

More hazards can be defined and the transformation process then continues iteratively as it goes deeper in the US Public Health System.

The next step is to model the safety control structure. The organizational configuration of the US Public Health System must be analyzed to determine where essential communication or feedback is occurring and where it needs to be improved. It also must map responsibilities for enforcing constraints and thereby maintaining control to specific roles in the organizations. Below is a high level diagram showing the important organizations as well as lines of communication and control.


Congress
President
Department of Health and Human Services
Department of Homeland Security
Department of Defense
Department of State
CIA
Department of Justice
Pharmaceutical Companies
Centers for Disease Control (Emergency Preparedness and Response)
Federal Emergency Management Agency
FBI
Governors and State Agencies
Hospitals/ Health Care System
Municipal and Local Authorities

For example, zooming in on the Department of Homeland Security (DHS), a list of constraints is defined to enforce the hazards where DHS maintains some responsibility.

Department of Homeland Security

Safety Requirements and Constraints:

1. DHS shall define a National Response Plan. It is "an all-discipline, all-hazards plan that establishes a single, comprehensive framework for the management of domestic incidents. It provides the structure and mechanisms for the coordination of Federal support to State, local, and tribal incident managers and for exercising direct Federal authorities and responsibilities. The NRP assists in the important homeland security mission of preventing terrorist attacks within the United States; reducing the vulnerability to all natural and man-made hazards; and minimizing the damage and assisting in the recovery from any type of incident that occurs." (http://www.dhs.gov/dhspublic/display?theme=14)
2. Through direction of the US Customs and Border Protection and coordination with the Department of Justice as well as State and local law enforcement agencies, quarantine and other control mechanisms shall be enforced in the event of an attack.
3. DHS shall ensure that all essential personnel involved in the National Response Plan are vaccinated prior to an attack.
4. DHS shall work with the CDC to ensure that hospitals and other health care providers have the information and materials needed for an effective response to a Smallpox attack.

In the example above, one could even go further to specify the responsibilities of the Directorate for Preparedness and the Office of Operations Coordination within the DHS. Additionally, Howard and Kelly have developed practical templates for capturing relevant information for hazards, constraints, control structure components, and control actions. For example, by capturing the relevant information for a control structure component in a standardized way such as defining fields for component description, responsibility, authority, and accountability, everyone involved in the planning can readily understand the role that each component plays.[14]

Organizational systems evolve with time as people and structures change. As organizations change, it is necessary to ensure that essential feedback mechanisms are preserved. When feedback was disrupted in the Walkerton Water Contamination Case, about 2000 people in a town of 4800 became ill and seven people died. In this incident, the Canadian government privatized water testing laboratories but did not ensure that reports continued to be sent to the Ministry of the Environment and the Department Health. [15] This tragedy shows the importance of maintaining appropriate feedback mechanisms in safety-critical activities.

After a constraint-roles/responsibilities mapping has been defined, a STAMP based analysis then seeks to identify gaps in the control structure that would permit a constraint not to be enforced. For example, are there any situations where two or more Federal agencies think that the other agencies are responsible for part of the NRP when in reality they are responsible? When a physician in private practice diagnoses a patient with Smallpox, how is the presence of Smallpox in the US communicated to the agencies of the NRP?

Finally, to define the *system risks*, a detailed hazard analysis is performed to discover how inadequate control could lead component agencies to fail in executing their responsibilities as defined above. Risks can be grouped into the following categories:

1. Decisions and actions in response to an attack are not made in a timely fashion.
2. Bad decisions and actions are made in the planning or execution of a response.
3. Good decisions and actions are made but outside forces prevent them from being effective.

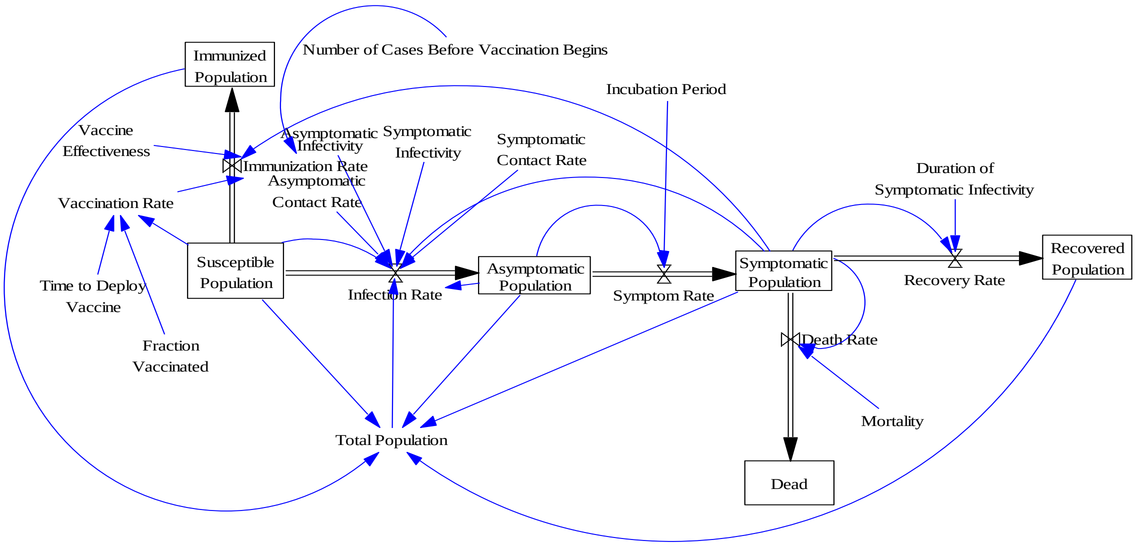
Risks in these categories include the President hesitating to order a mandatory quarantine of an infected region of the country, first responders are not vaccinated, become ill, and therefore ineffective in executing the NRP, and the CDC orders additional vaccine from abroad but foreign governments do not wish to share their vaccine supply. Very quickly, a long list of risks will be developed. Further categorizations might be useful such as planning risks versus execution risks or immediate risks versus long term risks in order to maintain intellectual manageability of the problem.

The last step of the analysis is System Dynamics modeling. Through simulation, the risks previously identified can be prioritized by quantitatively assessing their impact on important system safety variables, such as the number of deaths and the infection rate. Additionally, response plans can be tested on the model to assess their effectiveness. A complete model would include all the agencies identified in the safety control structure as well as the physical world such as the US population and the disease itself. Below is a part of the model showing how the disease could spread from one individual to the US population. It is based on the Kermack and McKendrick SIR model.[16]

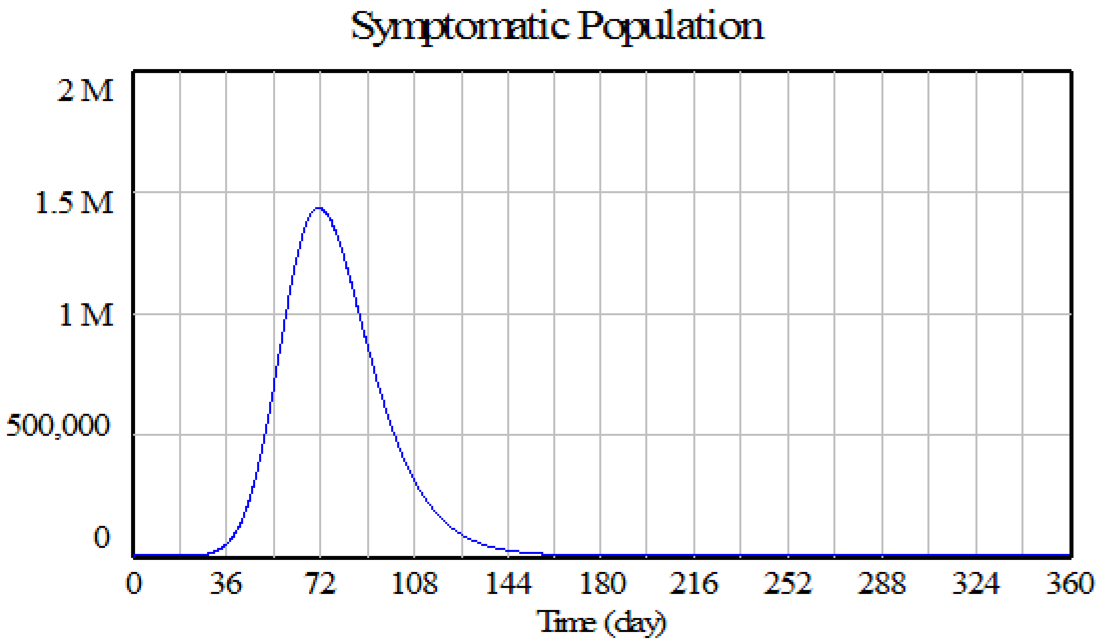
Some initial assumptions:

- 30% mortality
- 12 day incubation period
- 4 days of high symptomatic infectivity
- 99% effective vaccine
- 30 day vaccine deployment
- 85% of the population become vaccinated
- 280 million person initial population

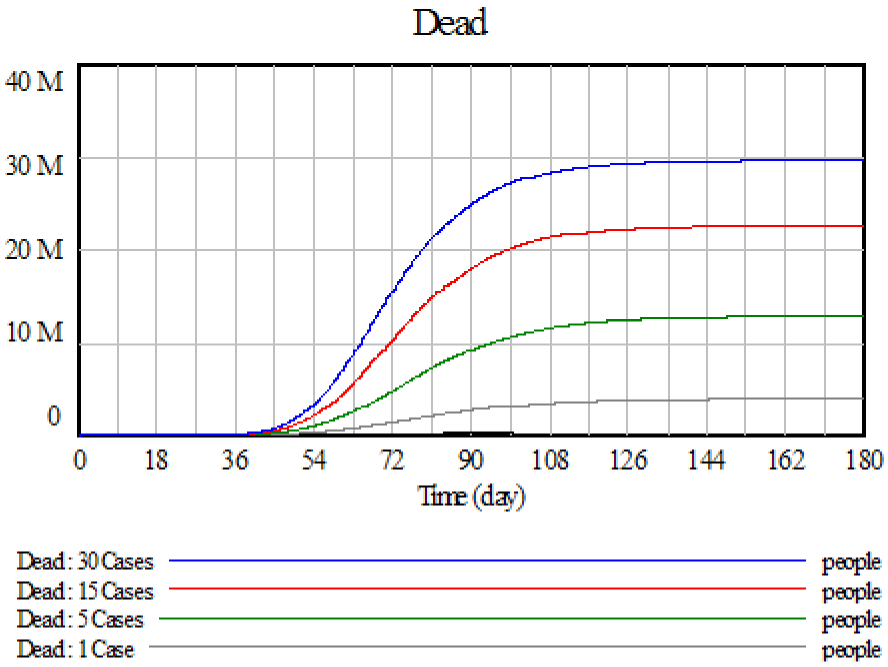
Note: System Dynamics modeling is typically not used to simply compute specific values, but rather to show relationships and trends. For example, my intent in one of the graphs below is not to predict exactly how many people will die but to show how a particular variable influences the number of total dead.



Simulations on the model produce graphs showing how variables change with time. Below is a graph which shows how the number of infected people with symptoms changes over the course of a year. This run was for a just-in-time (JIT) vaccination strategy that involved nationwide vaccination beginning after 10 confirmed cases of Smallpox.

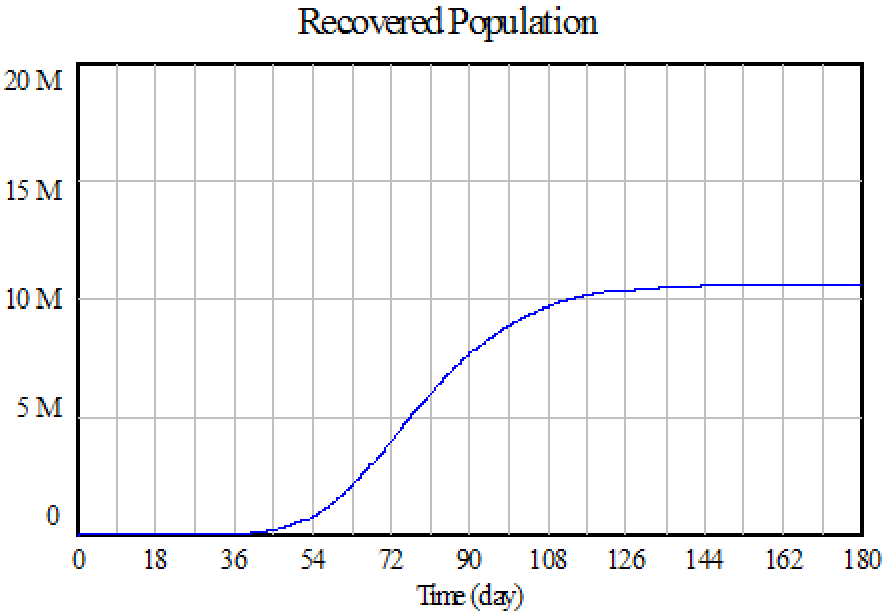


The next graph shows the difference in deaths resulting from a JIT policy where the government begins vaccinations after 1, 5, 15, or 30 people show symptoms.



One can see given *"unconstrained"* growth (no quarantine or other basic control policies) a few sick people wandering around can lead to the death of millions.

It is also important for policy makers to be aware of the dynamics of disease. Humans tend to simplify problems by assuming direct, linear relationships. This is often not the case. For example, one can expect the plot of recovered population versus time to follow an S-curve (see below). Recent work by Stephen Friedenthal in the area of management "flight simulators" and games brings the power of System Dynamics modeling in an accessible format to senior decision makers.[17] There are great opportunities for future work in this area, especially in the public health and safety area.



Conclusion

The results of a STAMP based analysis on the US Public Health System are a set of policies and a control structure necessary to achieve the policies. Such a result is eminently useful to policy makers and professionals involved in strategy development. By utilizing the tools of control theory and dynamical systems, policy makers and other officials can gain an understanding of the dynamics of disease, modify their organizational structure and planning to prevent bioterrorism, and finally respond quickly and effectively to attacks.

[1] McKenzie, F. Ellis. "Smallpox Models as Policy Tools." http://www.cdc.gov/ncidod/EID/vol10no11/04-0455.htm

2 Toroczkai, Zoltán. "Agent-Based Modeling as a Decision Making Tool." http://www.nae.edu/nae/naefoe.nsf/weblinks/VBAN-6J2PAD/$FILE/Toroczkai_ppt.pdf?OpenElement

[3] Sterman, John D. *Business Dynamics: Systems Thinking and Modeling for a Complex World*. Boston: Irwin Mcgraw-Hill, 2000, pg 42.

[4] Leveson, Nancy. "A New Accident Model for Engineering Safer Systems." *Safety Science*, Vol. 42, No. 4, April 2004

[5] Levson, Nancy. "A New Approach to Hazard Analysis for Complex Systems." Int. Conference of the System Safety Society, Ottawa, August 2003.

[6] Leveson, Nancy, , Mirna Daouk, Nicolas Dulac, and Karen Marais. "Applying STAMP in Accident Analysis" Workshop on Investigation and Reporting of Incidents and Accidents (IRIA), September 2003

[7] Leveson, Nancy. "Model-Based Analysis of Socio-Technical Risk." Technical Report, Engineering Systems Division, Massachusetts Institute of Technology, June 2002

[8] Leveson, Nancy and Nicolas Dulac. "Risk Analysis of the NASA Independent Technical Authority." Technical Report for NASA, June 2005.

[9] Dark Winter Presentation, Andrews Air Force Base. http://www.mipt.org/video/dark-winter/dark-winter.ppt, June 2001.

[10] Leveson, Nancy. "A New Accident Model for Engineering Safer Systems." *Safety Science*, Vol. 42, No. 4, pg 21, April 2004.

[11] Sterman, John D. *Business Dynamics: Systems Thinking and Modeling for a Complex World*. Boston: Irwin Mcgraw-Hill, 2000, pg XX.

[12] Zipkin, David. Using STAMP to Understand Recent Increases in Malicious Software Activity. SM Thesis, MIT. pg 18. June, 2005.

[13] Leveson, Nancy and Nicolas Dulac. "Risk Analysis of the NASA Independent Technical Authority." Technical Report for NASA, pg 6, June 2005.

[14] Howard, J and K. Kelley. "A Notation Supporting a Systems-Theoretic Hazard Analysis Technique." Technical paper for the Safeware Corporation, June 2004.

[15] Leveson, Nancy, Mirna Daouk, Nicolas Dulac, and Karen Marais. "Applying STAMP in Accident Analysis by Nancy Leveson." Workshop on Investigation and Reporting of Incidents and Accidents (IRIA), September 2003.

[16] Sterman, John D. *Business Dynamics: Systems Thinking and Modeling for a Complex World*. Boston: Irwin Mcgraw-Hill, 2000, pg 303.

[17] Friedenthal, Stephen. *Developing a Risk Management "Flight Simulator" for Manned Space Programs: A User Interface to a Systems Dynamic Simulation of System Safety at NASA*. SM Thesis, MIT, January, 2006.