CAST

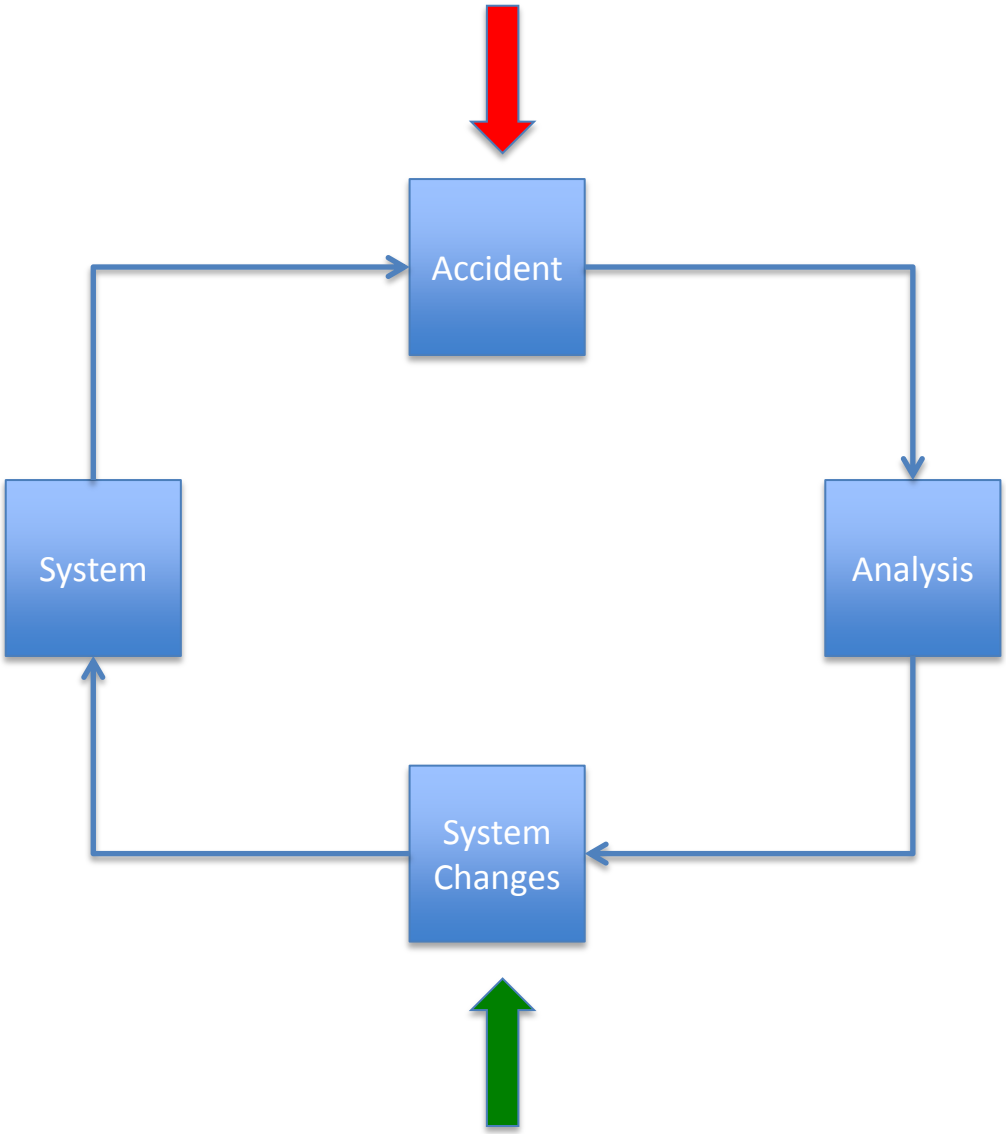
Causal Analysis using System Theory

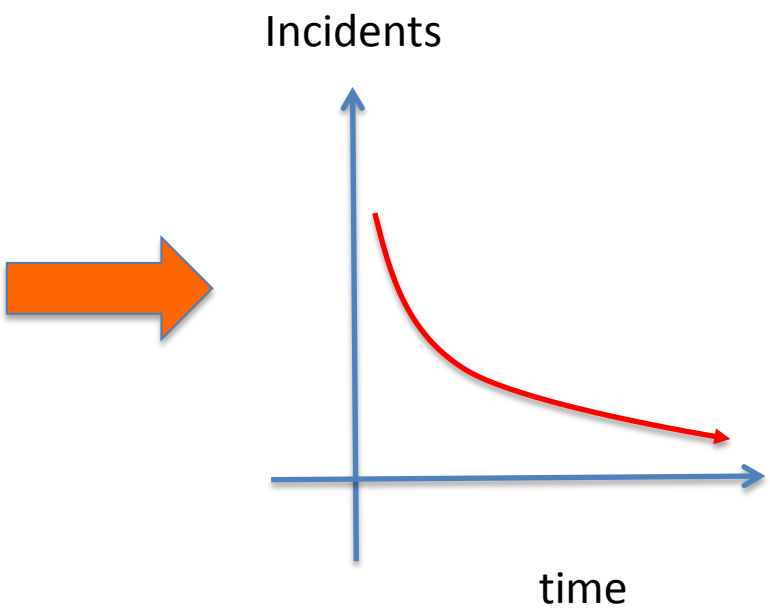
STAMP Workshop

Advanced Tutorial

April 17, 2012

Why do Accident Analysis?





Goals for an Accident Analysis Technique

- Provide a framework or process to assist in understanding entire accident process and identifying systemic factors
- Get away from blame (“who”) and shift focus to “why” and how to prevent in the future
- Goal is to determine
  - Why people behaved the way they did
  - Weaknesses in the safety control structure that allowed the loss to occur
- Minimize hindsight bias

Hindsight Bias

- After an incident
  - Easy to see where people went wrong, what they should have done or avoided
  - Easy to judge about missing a piece of information that turned out to be critical
  - Easy to see what people should have seen or avoided

"shoulda, coulda, woulda"

Overcoming Hindsight Bias

- Nobody comes to work to do a bad job.
  - Assume were doing reasonable things given the complexities, dilemmas, tradeoffs, and uncertainty surrounding them.
  - Simply finding and highlighting people's mistakes explains nothing.
  - Saying what did not do or what should have done does not explain why they did what they did.
- Investigation reports should explain
  - Why it made sense for people to do what they did rather than judging them for what they allegedly did wrong and
  - What changes will reduce likelihood of happening again

CAST

1. Identify system hazard violated and the system safety design constraints
2. Construct the safety control structure as it was designed to work
    1. Component responsibilities (requirements)
    2. Control actions and feedback loops
3. For each component, determine if it fulfilled its responsibilities or provided inadequate control.
    1. Context
    2. Process Model Flaws

CAST (2)

4. Examine coordination and communication

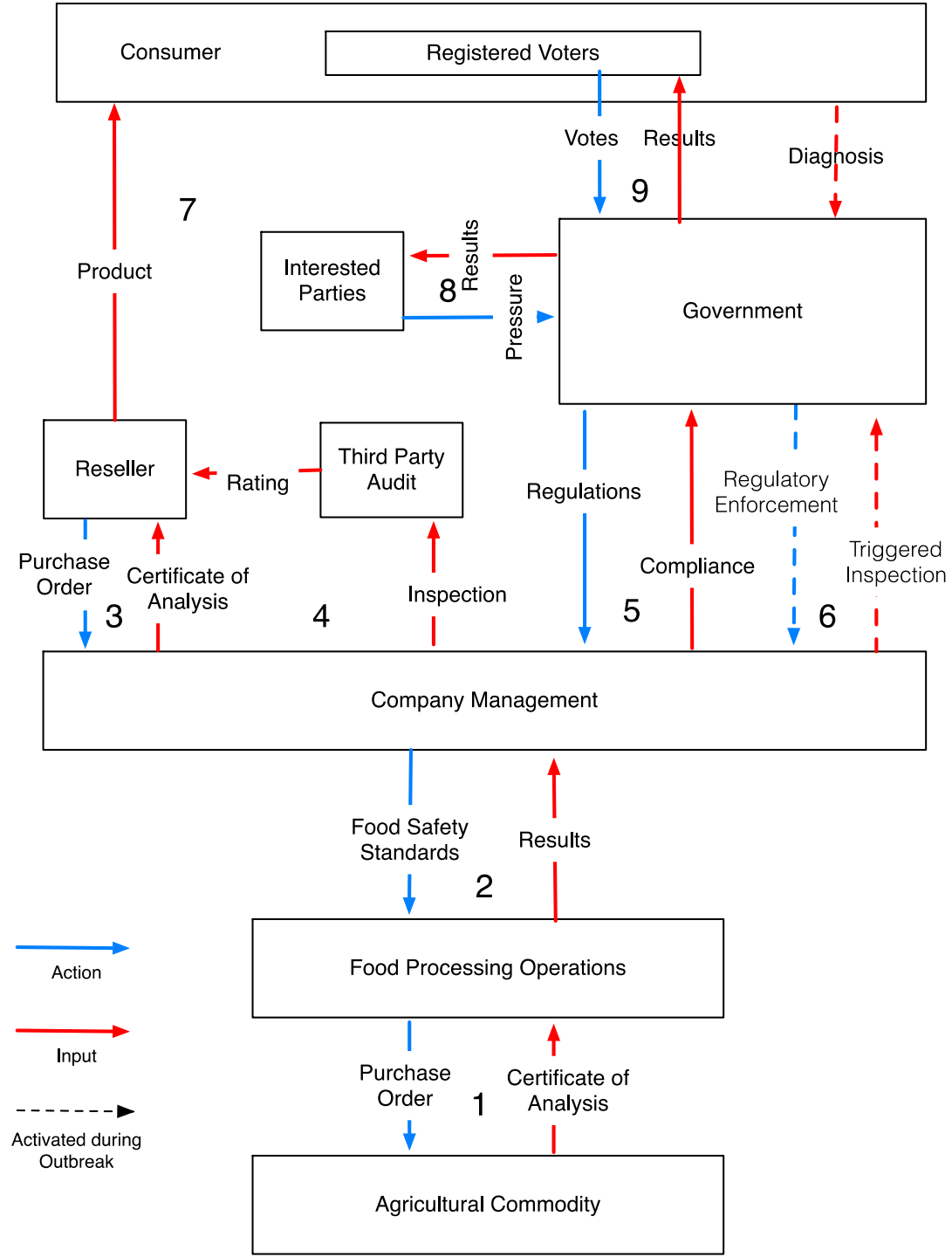
5. Consider dynamics and migration to higher risk

6. Determine the changes that could eliminate the inadequate control (lack of enforcement of system safety constraints) in the future.

7. Generate recommendations

1. Identify system hazard violated and the system safety design constraints

Hazard	Safety Constraint	Safety Constraint Violated
Pathogenic Bacteria	No pathogenic bacteria in food at point of consumption	**35 *Salmonella enterica* serotype Typhimurium isolates were detected in 16 states by PulseNet**
Metal or other foreign object	No metal or other foreign objects > 1 mm in size	
Toxins	Aflatoxin < 20 ppb(FDA 2000)	



2. Construct the safety control structure as it was designed to work

- Component responsibilities (requirements)
- Control actions and feedback loops

3. For each component, determine if it fulfilled its responsibilities or provided inadequate control

Loop	Safety Resposibilities	Inadequate control action	Context in which decisions made	Process or Mental model flaws
2	Ensure building and equipment are maintained to prevent egress or growth of pathogens	Building had openings that allowed pests and rainwater to enter	No plant manager on site from April to Sep	?
3	Maintain adequate sanitation and pest control to prevent pathogens from entering the production environment	Pest control did not function, equipment not properly sanitized	No plant manager on site from April to Sep	?
7	No product is shipped to customers that contains pathogens	Product shipped that tested positive with a negative retest	Financial pressure Action had been taken before without negative consequences	OK to ship product on negative retest
8	No product is shipped to customers that contains pathogens	Certificate of analysis did not reflect positive salmonella test	Financial pressure Action had been taken before without negative consequences	OK to ship product on negative retest Cannot afford to scrap product when contamination is in question

CAST (2)

4. Examine coordination and communication

5. Consider dynamics and migration to higher risk

6. Determine the changes that could eliminate the inadequate control (lack of enforcement of system safety constraints) in the future.

7. Generate recommendations

CAST Exercise

1) Choose an accident you are familiar with to analyze using CAST
2) Determine the proximate events in the actual accident you chose
3) Identify the system hazard violated and the system-level safety constraints
4) Construct the safety control structure as it was designed to work
    a) Identify the major controllers and other components
    b) Identify the roles and responsibilities for each controller
    c) Draw the control structure
    d) Label the possible control actions for each controller
    e) Label the possible feedback information for each controller

Choose a controller to analyze further:

1) Identify inadequate control actions that violated safety-related responsibilities
2) Identify any process model flaws that contributed to inadequate control
3) Identify other contextual factors that contributed to inadequate control