Integrating Safety and Mission Assurance into Systems Engineering Modeling Practices

Sean Beckman, CSEP

Scott Darpel, MSIE

NASA John H. Glenn Research Center

October, 2015

Abstract

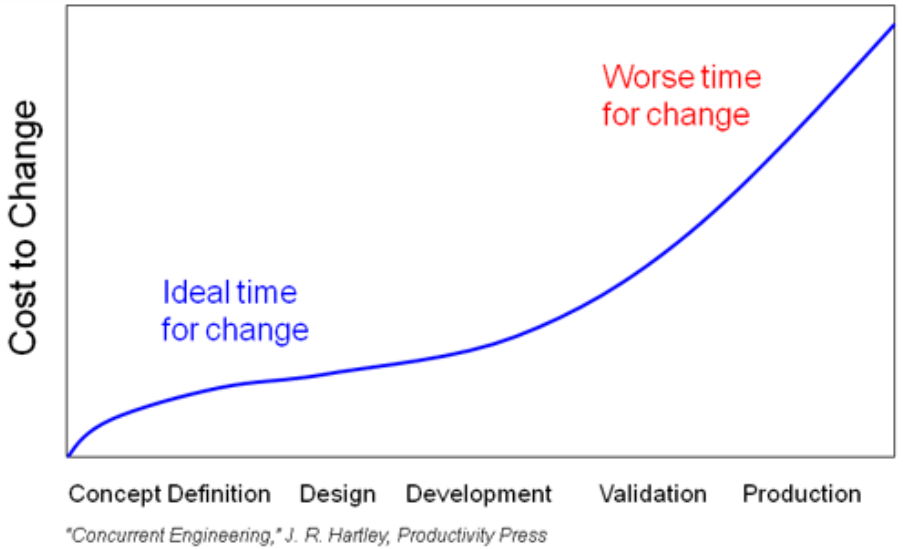
S. Beckman and S. Darpel

During the early development of products, flight, or experimental hardware, emphasis is often given to the identification of technical requirements, utilizing such tools as use case and activity diagrams. Designers and project teams focus on understanding physical and performance demands and challenges. It is typically only later, during the evaluation of preliminary designs that a first pass, if performed, is made to determine the process, safety, and mission/quality assurance requirements. Evaluation early in the life cycle, though, can yield requirements that force a fundamental change in design. This paper discusses an alternate paradigm for using the concepts of use case or activity diagrams to identify safety/hazard and mission/quality assurance risks and concerns using the same systems engineering modeling tools being used to identify technical requirements. It contains two examples of how this process might be used in the development of a space flight experiment, and the design of a Human Powered Pizza Delivery Vehicle, along with the potential benefits to decrease development time, and provide stronger budget estimates.

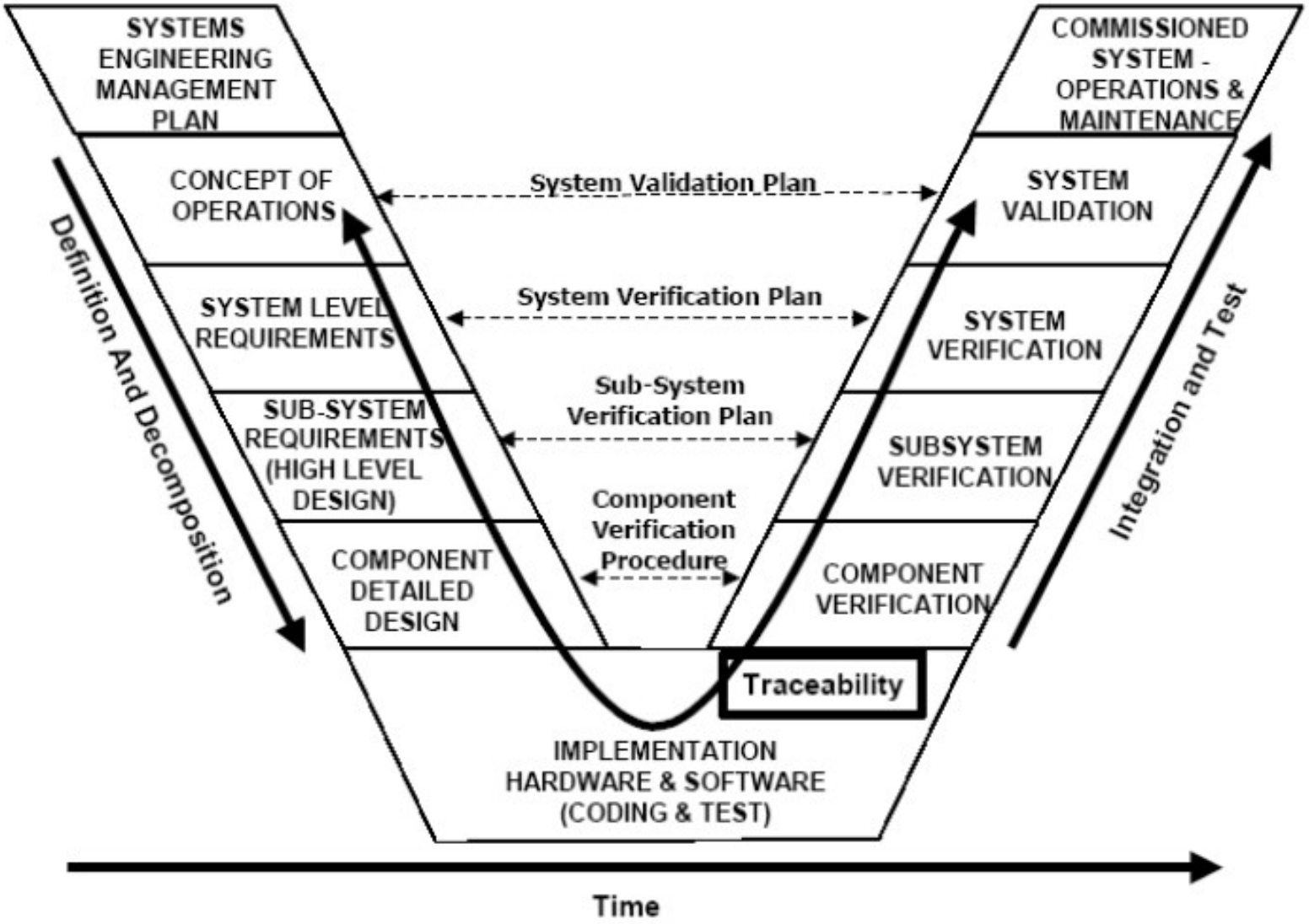
The Problem

- Systems Engineering and Project Management Professional universally agree with the notion that the later a change to a design occurs, the higher the cost
- Design changes are most often the result of a late identification of a requirement or a performance gap
- Requirements definition in the early concept and design phases focuses on technical and performance items
- Current paradigm ignores an entire grouping of requirements until well into the preliminary design phase, after decisions have been made about trades and architecture

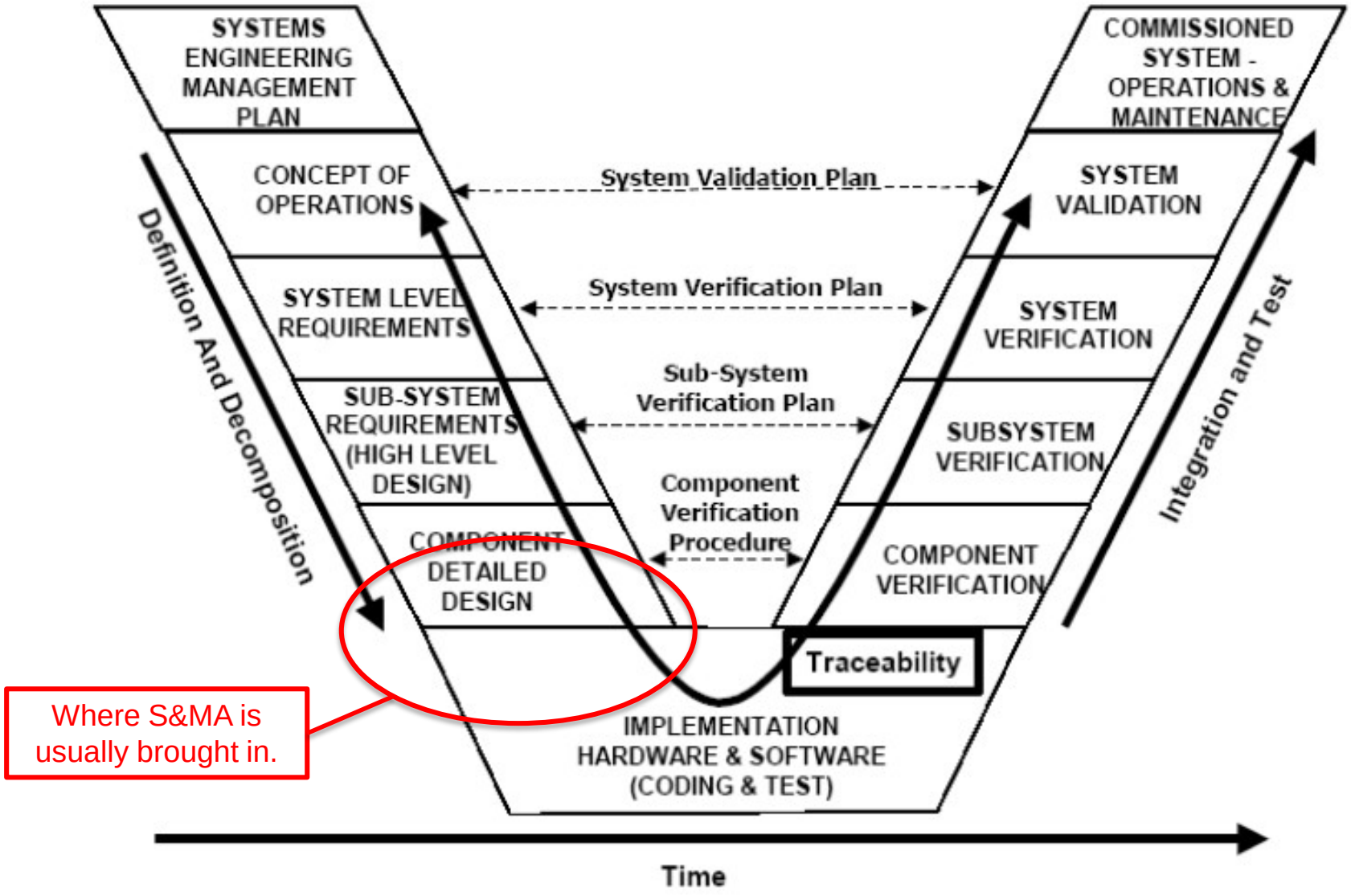
S&MA requirements not identified until the preliminary design phase yields additional redesign costs that could be avoided if done earlier



The Systems Engineering "V" Approach



The Systems Engineering "V" Approach



Where S&MA is usually brought in.

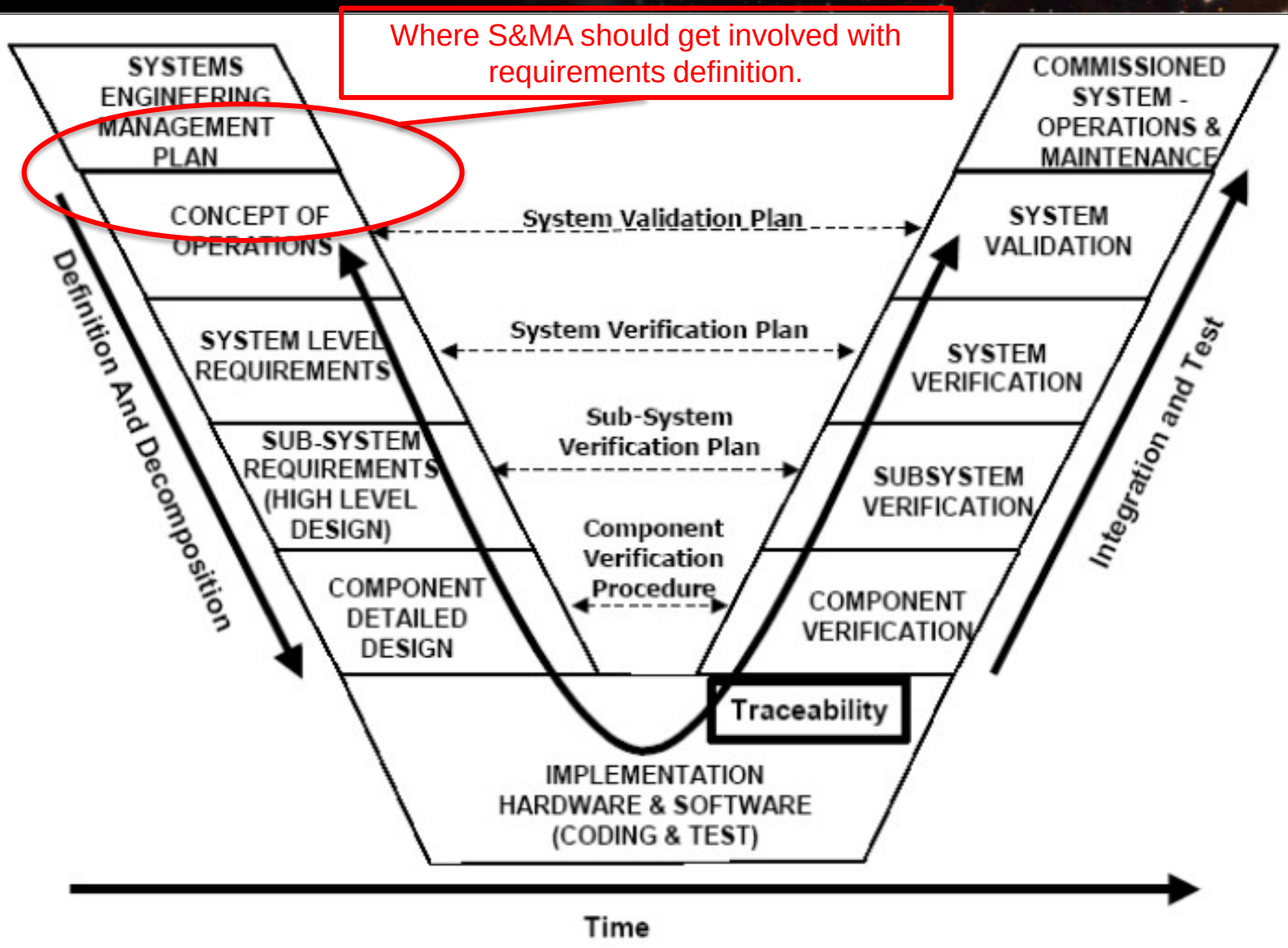
S&MA Typical Involvement

- **S&MA discipline support ramps up with focus on analyzing the preliminary design**
  - *Preliminary Hazards Assessment*
  - Environmental Testing
  - EEE Parts Plans & Searches
  - Required Margins
  - Identification of Standards
  - Materials Assessments
- **Requirements-based approach, leading a subtractive process that starts with a maximum set of items, tailoring down to an appropriate level**
  - Takes a lot of time, effort
  - S&MA disciplines thought of more as a burden, adding work to a project

Impacts of Current Paradigm

- **Identification of hazards after preliminary designs means redesign to accommodate the required controls, at best**
- **At worst, a complete redesign is required, when it cannot meet safety margins**

An Ehnacned Systems Engineering “V” Approach



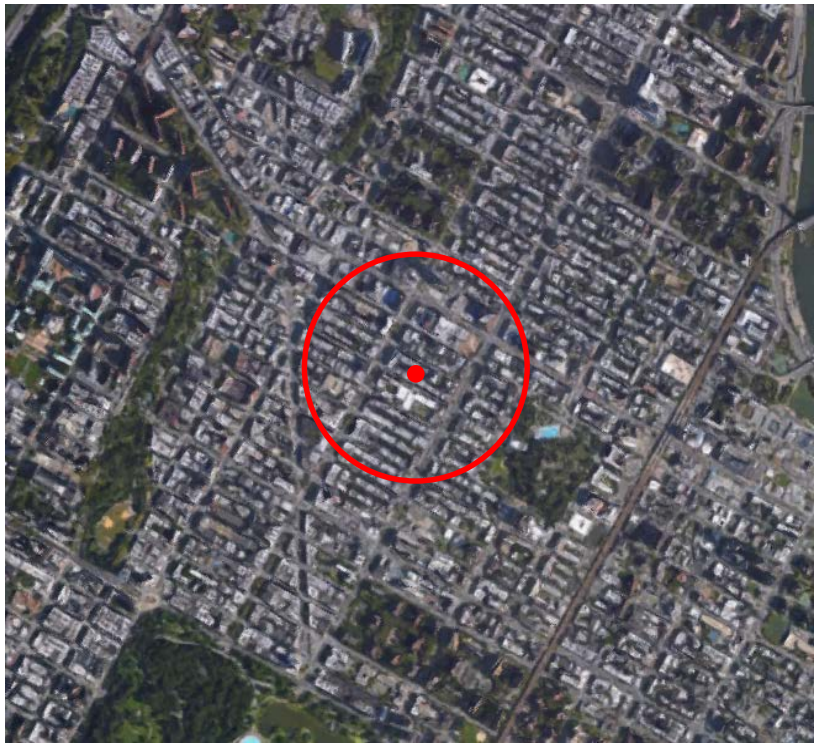
Redefining of S&MA Value

- **S&MA Disciplines are currently utilized to identify issues with a design**
- **Given that most hazards and QA requirements can be based on intended uses and activities, S&MA disciplines can help identify them during use case and concept of operations development**
- **Earlier involvement of S&MA can reduce redesign and cost**
- **S&MA discipline experts focused on risk**
  - Help the project identify what the risks are
  - Which risks might be associate with hazards?
  - What good practices or additional requirements can be used to mitigate?
  - NOT focused on applying a standard set of requirements, but adding in only those that add value through the mitigation of risk

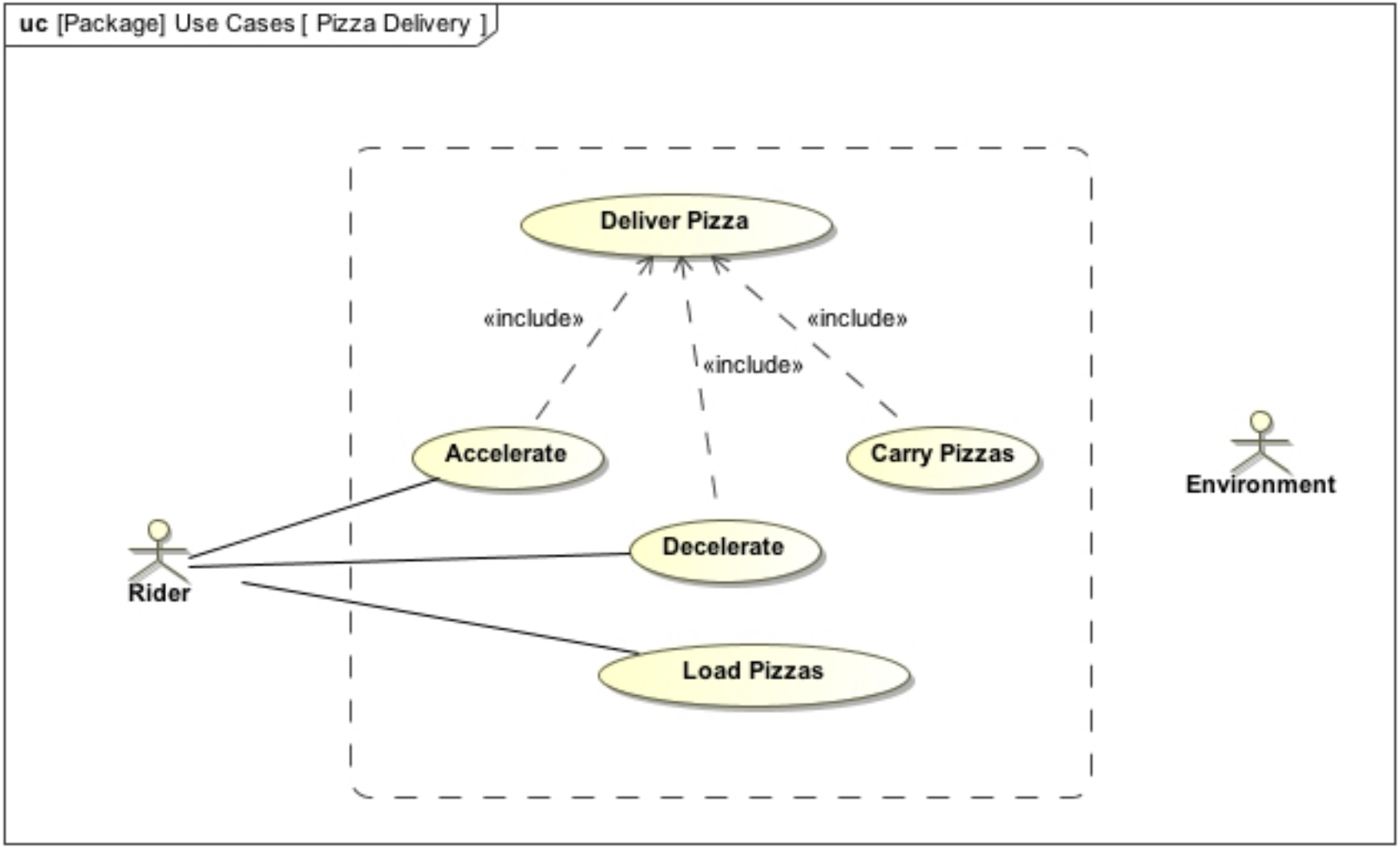
Example
Human Powered Pizza Delivery Vehicle

- A pizzeria owner in a large metropolitan area has his delivery person deliver pizzas one at a time on foot.
- Pizza needs to arrive at a minimum temperature.
- Radius of delivery is determined by speed of delivery person and time for pizza to cool to minimum temp.
- He needs a way to deliver more pizzas faster to increase radius of delivery and thus his customer base to increase profits.
- Since traffic congestion is an issue, a car is not a solution.

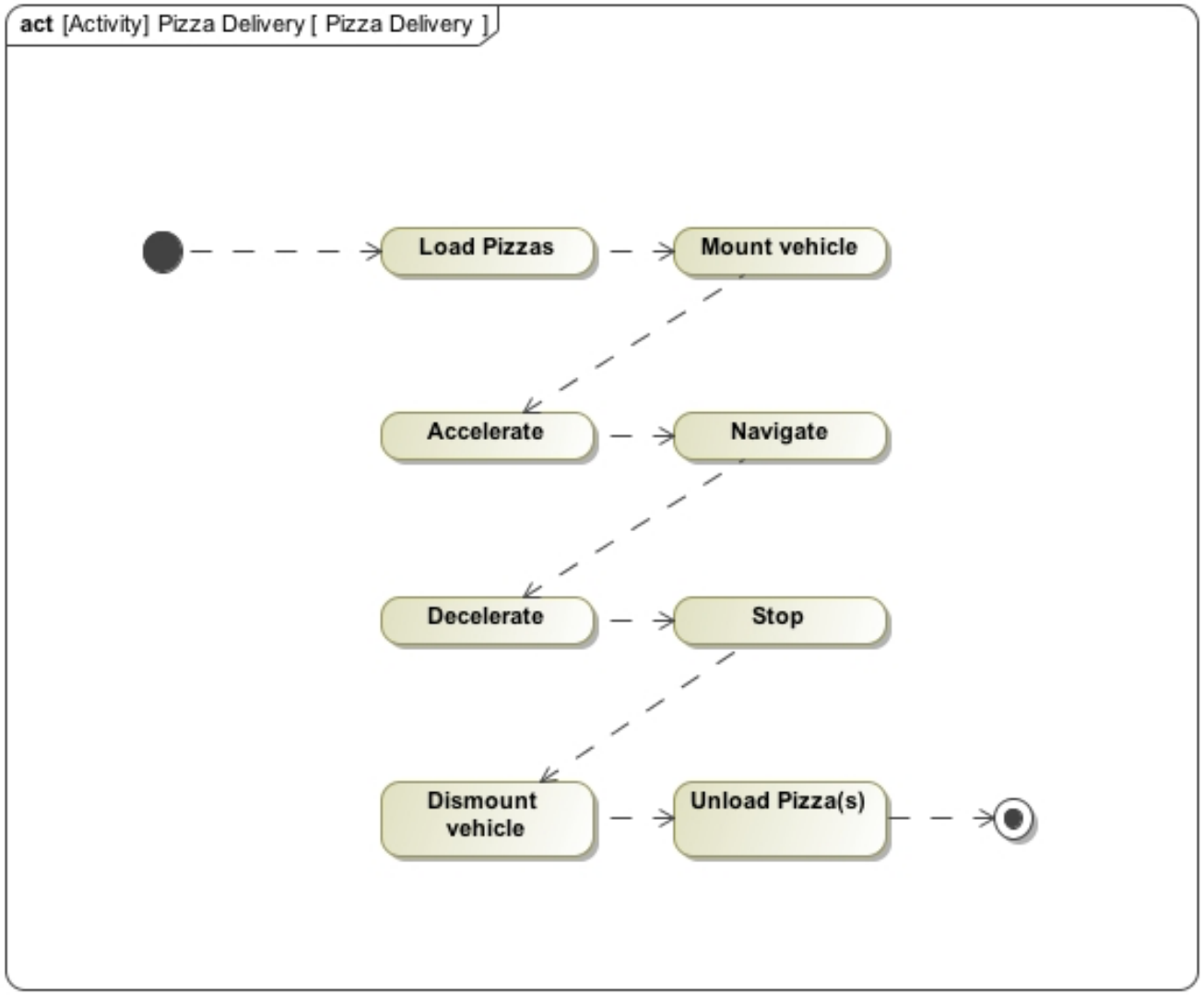
Example
Human Powered Pizza Delivery Vehicle



Use Case Diagram



Activity Diagram



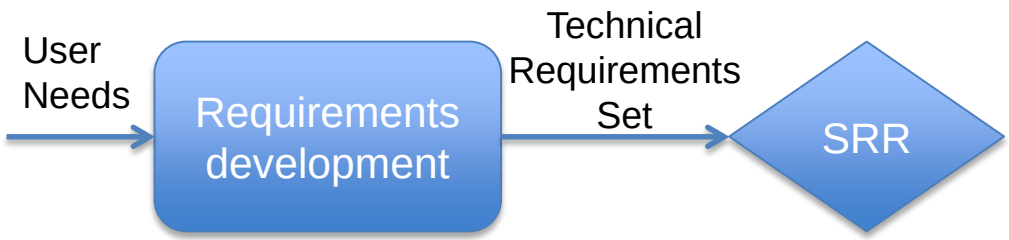
Partial Requirements Set

#	Id	Name	Text
1	HPPDV1	Carry Capacity	The HPPDV shall carry at least two pizzas.
2	HPPDV2	Speed	The HPPDV shall be capable of traveling at a speed of at least TBD kph.
3	HPPDV3	Acceleration	The HPPDV shall be capable of accelerating at a rate of TBD kph/sec.
4	HPPDV4	Deceleration	The HPPDV shall be capable of decelerating at a rate of TBD kph/sec.
5	HPPDV5	Maneuverability	The HPPDV shall be maneuverable.
6	HPPDV6	Mass	The HPPDV shall weigh no more than TBD kg.
7	HPPDV7	Size	The HPPDV shall fit in an envelope no larger than X m by Y m by Z m.

Current Product Development Flow*

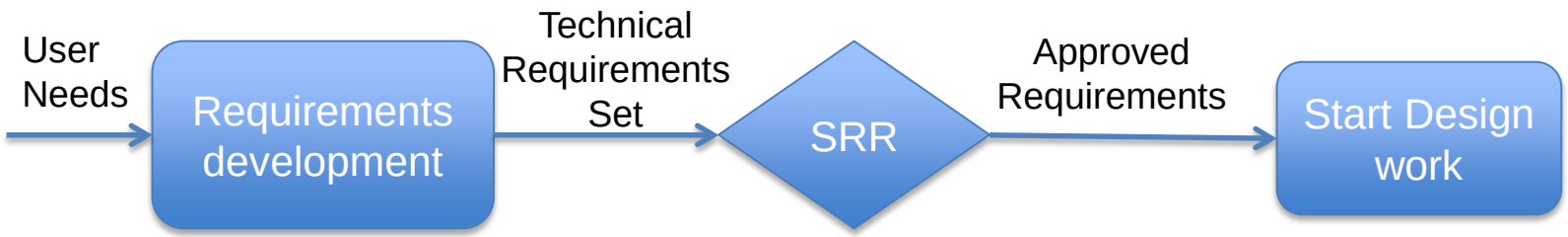
*Based on NASA NPR 7123.1A NASA Systems Engineering Processes and Requirements

Current Product Development Flow*



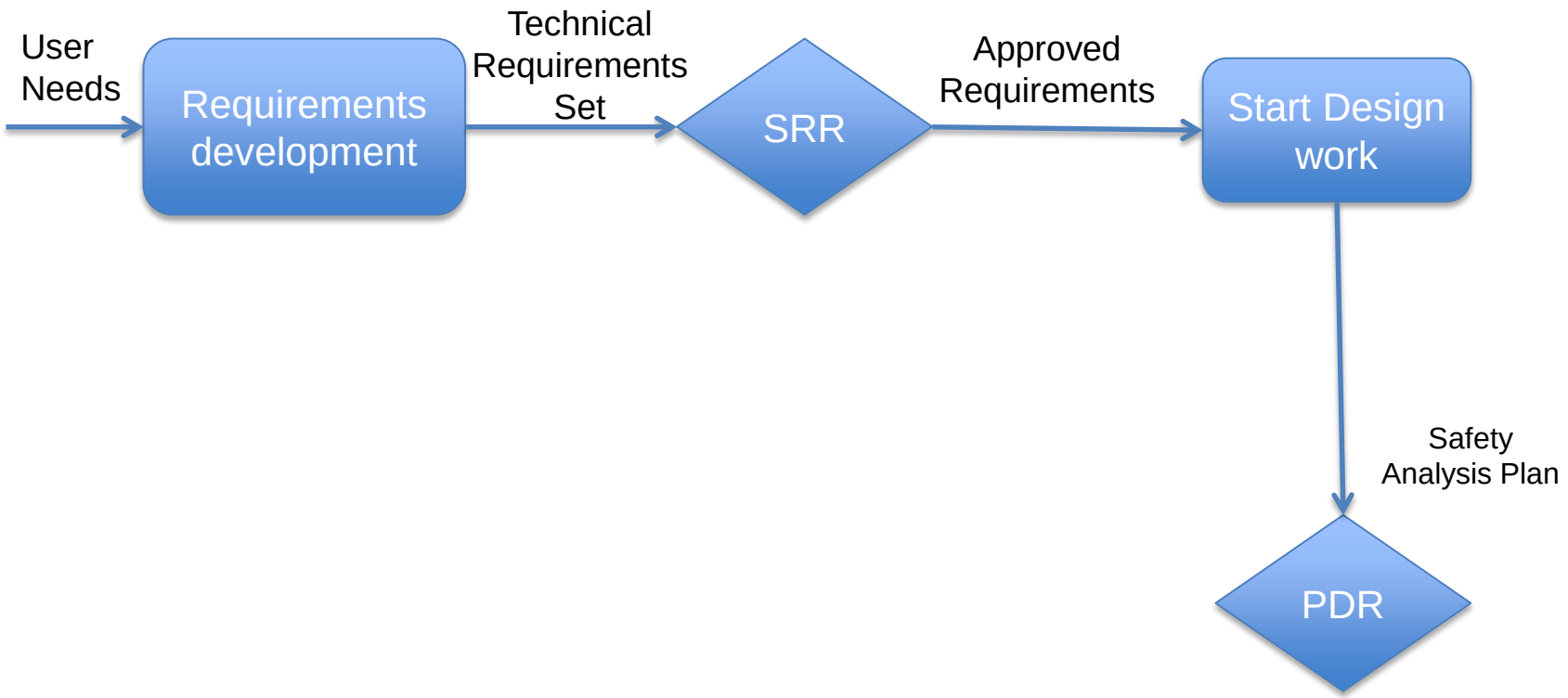
*Based on NASA NPR 7123.1A NASA Systems Engineering Processes and Requirements

Current Product Development Flow*



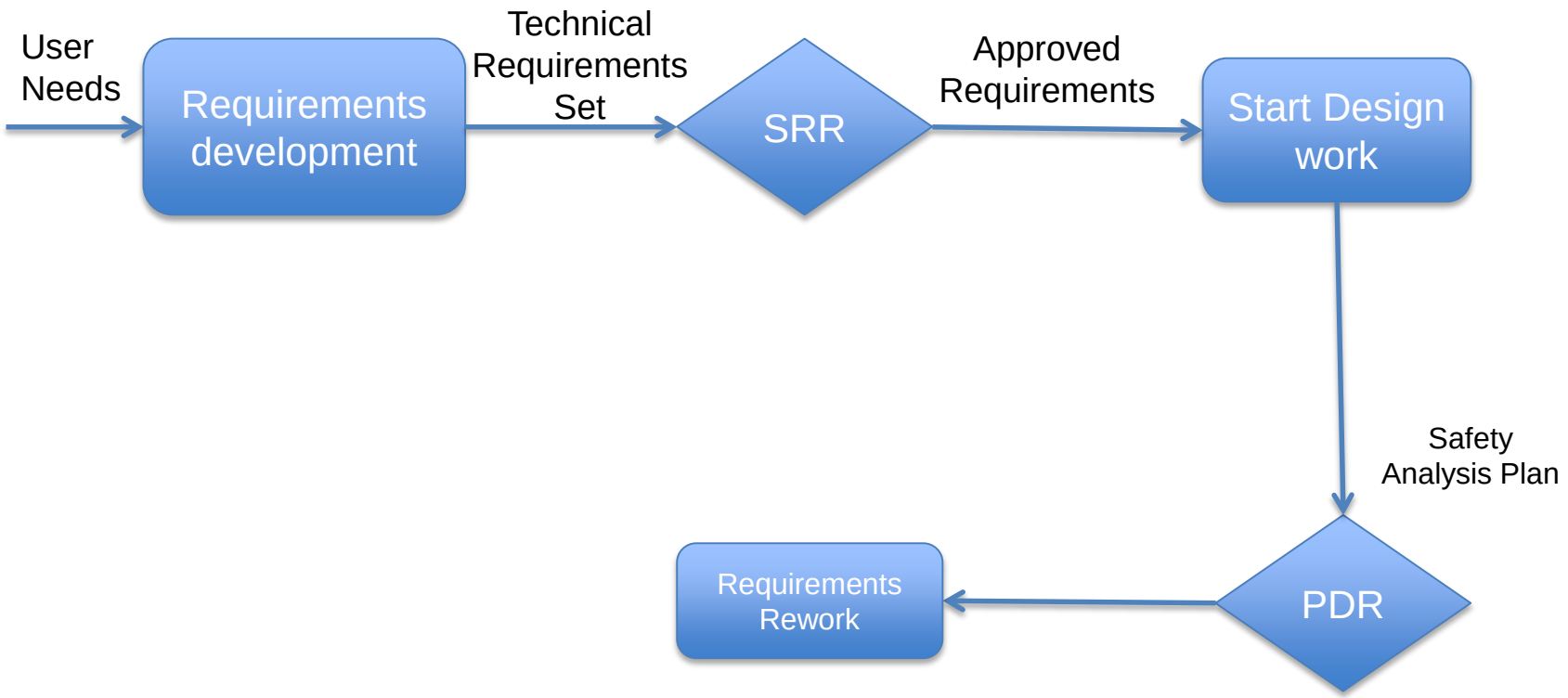
*Based on NASA NPR 7123.1A NASA Systems Engineering Processes and Requirements

Current Product Development Flow*



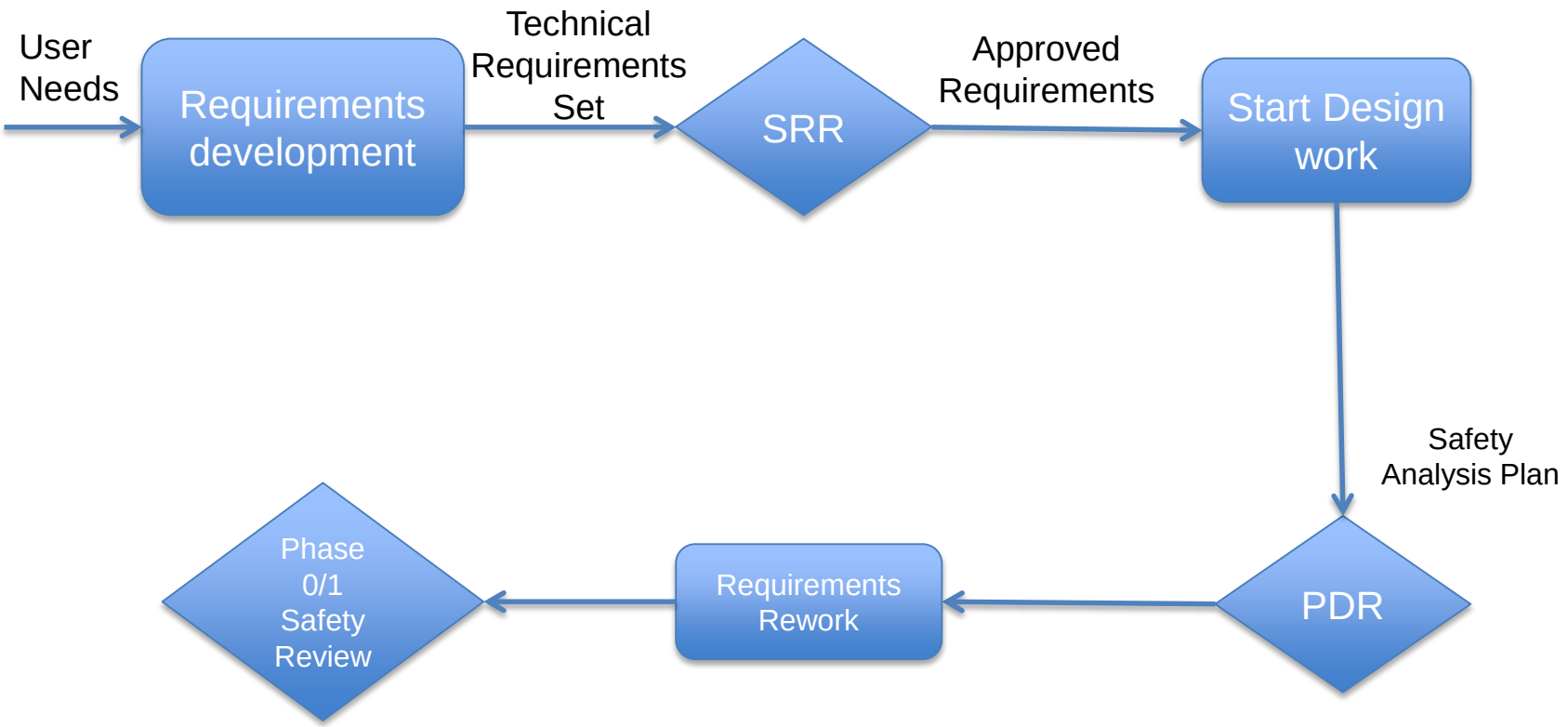
*Based on NASA NPR 7123.1A NASA Systems Engineering Processes and Requirements

Current Product Development Flow*



*Based on NASA NPR 7123.1A NASA Systems Engineering Processes and Requirements

Current Product Development Flow*

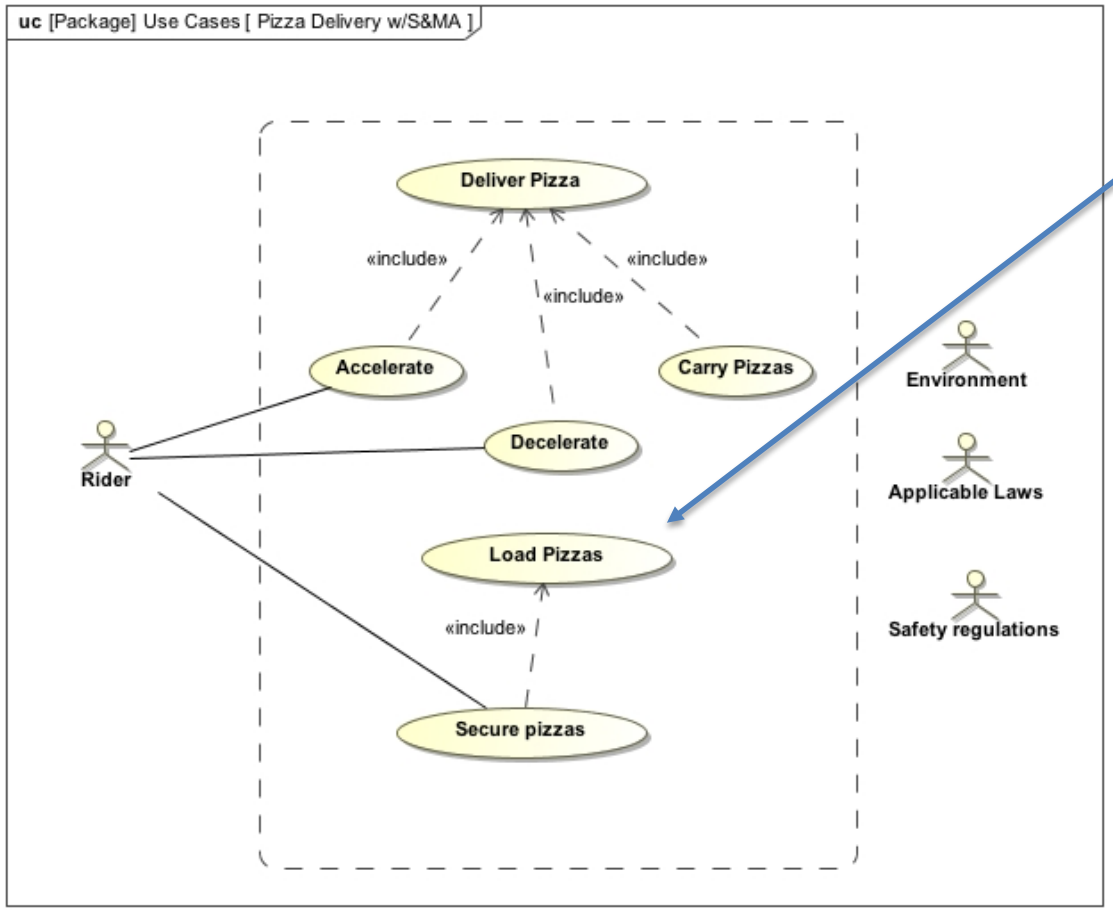


*Based on NASA NPR 7123.1A NASA Systems Engineering Processes and Requirements

Earlier Involvement Of S&MA

- **As use case or activity diagrams are developed, include S&MA disciplines**
- **Looking at each use or activity, ask the questions**
  - "Is there any way this can cause a hazard?"
  - "How can this go wrong?"
- **This early identification of risk can lead to additional technical, performance, and S&MA requirements**

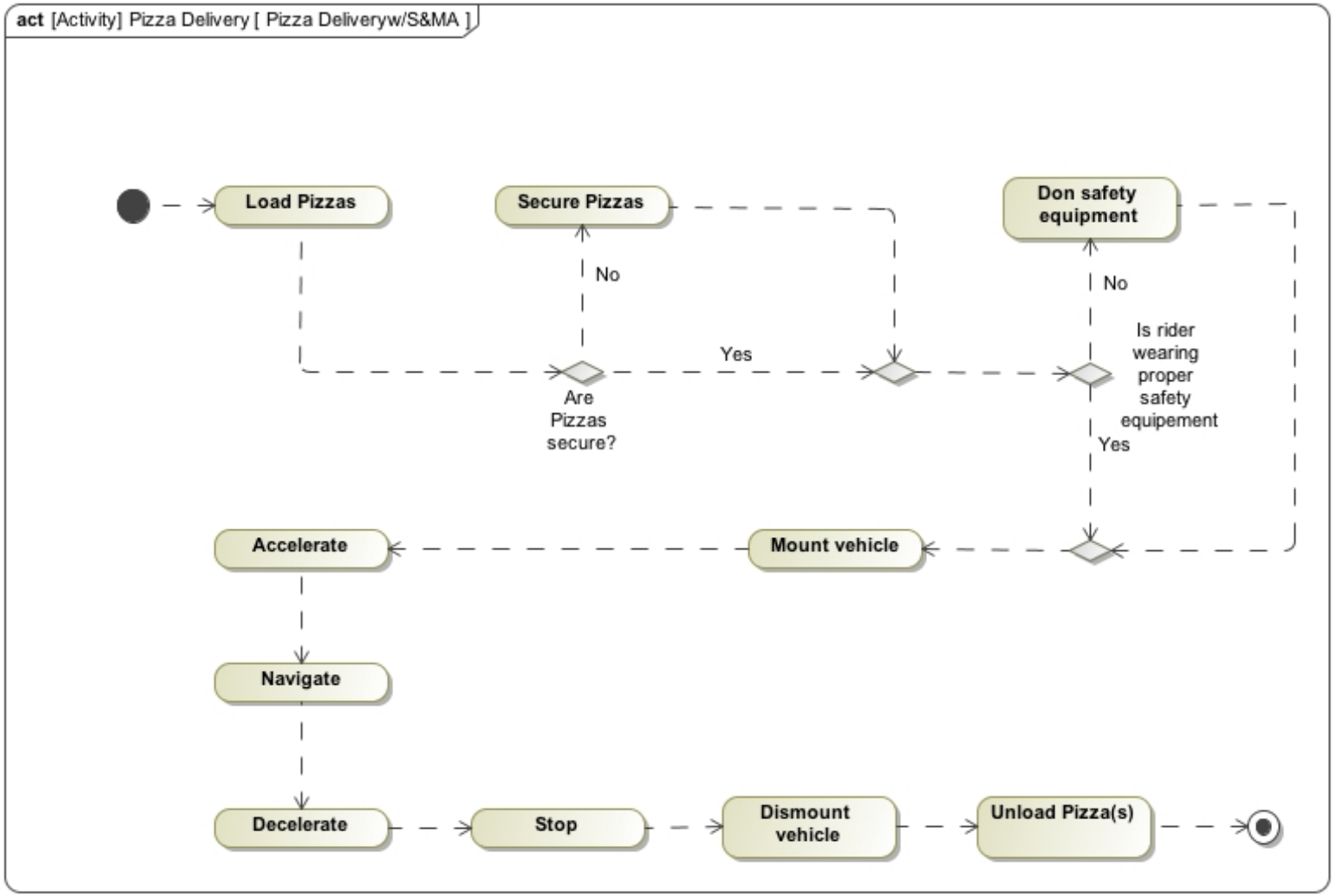
Use Case Diagram with S&MA input



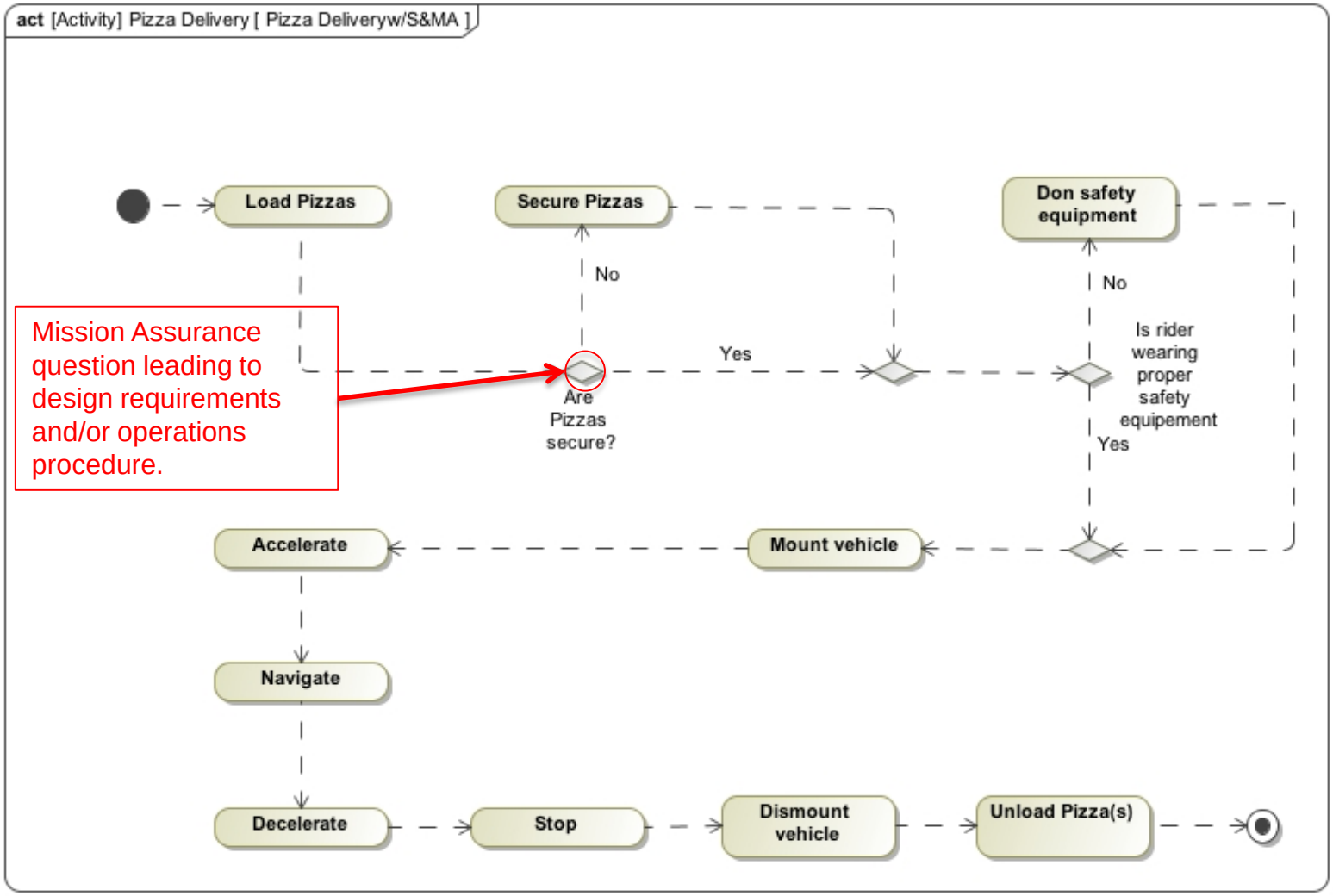
How can “Load Pizzas” go wrong? What are the risks associated with this interaction?

New project requirement: *System shall have features to secure loaded pizzas to prevent loss during delivery*

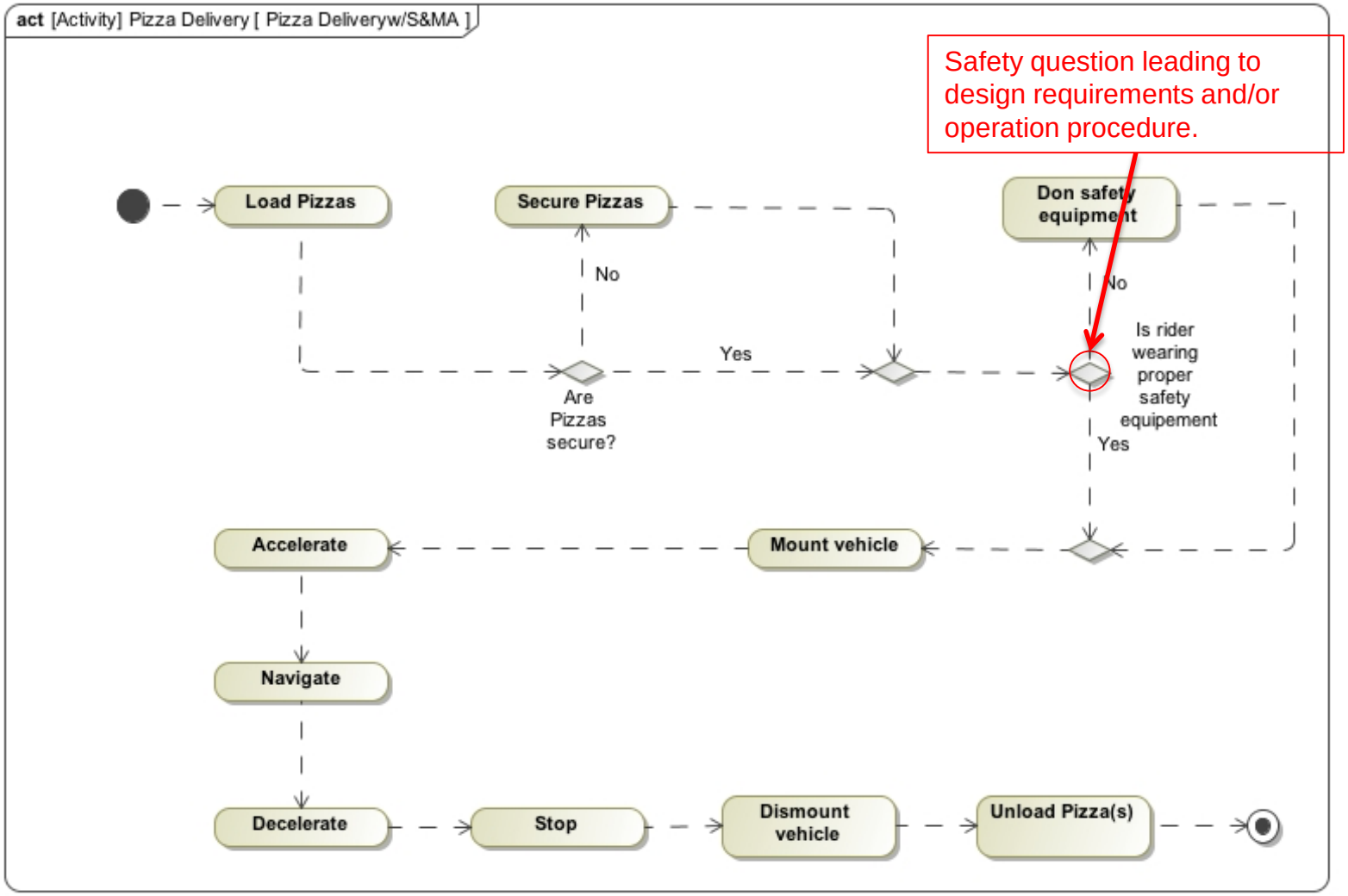
Activity Diagram with S&MA input



Activity Diagram with S&MA input



Activity Diagram with S&MA input



Benefits

- Earlier identification of hazards will yield fewer design iterations. (Safety risks)
- Earlier identification of assurance requirements will yield better understanding of testing needs.
- Earlier involvement of S&MA disciplines during use and activity model development will yield better understanding of the system use
  - More effective S&MA plans
  - More appropriate S&MA requirements sets
  - Risk-based, additive approach leads to appropriate requirements sets better in line with risk posture

Supplemental Reading

- **Integrating Failure Modes and Effects with the System Requirements Analysis** – R. Carson, INCOSE 2004 - 14th Annual International Symposium Proceedings
- **Using SysML to Automatically Generate of Failure Modes and Effects Analyses** – M. Hecht, E. Dimpfl, and J. Pinchak, INCOSE 2015 - 25th Annual International Symposium Proceedings
- **Integrating Systems Safety into Systems Engineering during Concept Development** – C. Fleming and N. Leveson, INCOSE 2015 - 25th Annual International Symposium Proceedings
- **An Integrated Model-Based Approach to System Safety and Aircraft System Architecture Development** – E. Villhauer and B. Jenkins, INCOSE 2015 - 25th Annual International Symposium Proceedings