BAE SYSTEMS

Principles of Product Safety: Depiction of a Product Safety Management System using STPA

Mike Hurley
Head of Product Safety,
Electronic Systems Sector Defense Segment
BAE Systems

3/19/13




BAE SYSTEMS

Introduction

- BAE Systems is a global company with a wide variety of Businesses, Products, and Customers. The range of Products includes everything from communications and signal processing systems to vehicles and weapons systems.
- A unifying theme across our enterprise is an abiding concern for Product Safety, which represents a common commitment throughout our company.
- To meet this commitment, we have established Principles of Product Safety that provide guidance during the performance of our individual roles.
- This presentation will discuss the Principles of Product Safety in the context of their application to a Product Safety Management System in a primarily Defense-related Products organization and attempt to present same in Systems Theoretic Process Analysis (STPA) notation

BAE SYSTEMS

STPA: The Basic Model

- Identify the hazard of concern
- Draw the control structure
- Identify unsafe control actions that could result in mishap/accident due to the hazard
- Identify safety constraints for the design that will prevent/reduce likelihood of the unsafe control actions
  - Include consideration of causal factors

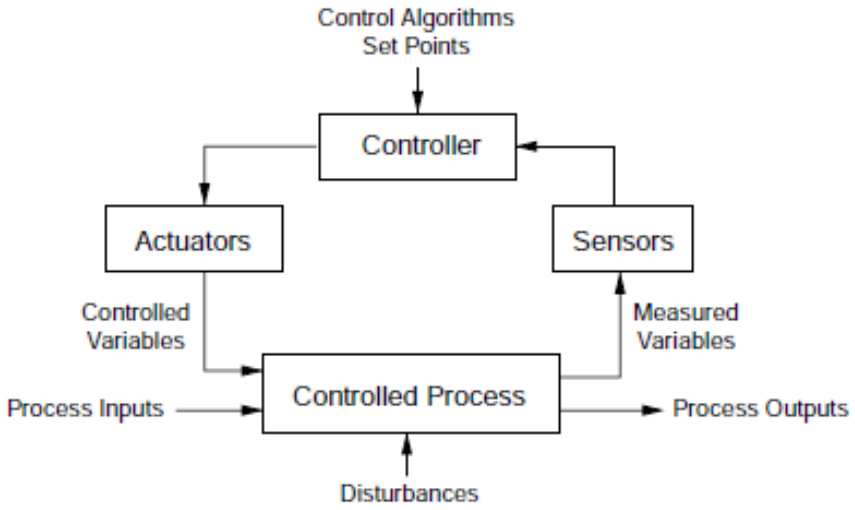


Figure 3.2
A standard control loop.

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

The First Step Is Depicting Systems And Processes
In Terms Of The Control Structure With Control & Feedback Loops

BAE SYSTEMS

Why A Product Safety Management System (PSMS)?

- The PSMS serves multiple purposes, and must address the several phases of the Product Life Cycle
  - Ensure the Product Development process includes both implicit and derived requirements for the Product (reflecting how it is used, maintained, and disposed of)
  - Ensure the Product Development process can be applied safely (as regards physical activities of manufacture, integration, test, disposal)
  - Ensure that what is built is what was intended
  - Contribute to maintaining the intended Level of Safety for the delivered Product
- The PSMS must provide the means to address and resolve
  - Cultural and organizational issues,
  - Hierarchies of governance & influence both internal and external to the organization, and
  - The tendency of all systems to move towards a less safe state

BAE SYSTEMS

BAE Systems Principles of Product Safety

- Vision: All of our Products are conceived, designed, built, supplied, maintained and replaced with the level of safety that is agreed to with our customers
- The Product Safety Principles are:
  - Accountability
  - Level of Safety
  - Conforming Product
  - Learning and Sharing Information
- From an STPA perspective, these Principles can be seen to act as an Actuator, or a Sensor, or both

We say what our Products are and what they do; and
We deliver Products that are and do what we say.

BAE SYSTEMS

Principle 1: Accountability

- We shall work with our customers and others to ensure that there is, at all times through the life of every Product, accountability for its unintended effects on the safety of people
  - we are and remain accountable for those aspects of our Products that are under our control or for which we are legally responsible;
  - we shall make reasonable efforts to maintain accountability when we no longer have control of, or responsibility for, our Products; and
  - the Company's accountability will be delegated to individuals.

- Accountability – establishing accountability, including delegations of authority = **an Actuator**

The Engineering Management Framework identifies Accountability for Product Safety as it applies to various Roles at various Levels in the organization

BAE SYSTEMS

Principle 2: Level of Safety

- We shall work with each customer to agree the level of safety that is to be achieved by each Product through its life.
- We shall seek the highest level of safety of those who might be unintentionally harmed by the Product that is compatible with the Product's required performance, cost and schedule and the way that it will be used.
- Level of Safety – represents the identification of customer needs and required functionality (in terms of safety provisions and features) including derived requirements and requirements originating in other Controllers – **an Actuator**

The PSMS includes a Process for determining applicable requirements and associated tasks to ensure compliance (including incorporation of lessons learned and requirements that apply to all Products) in the organization

BAE SYSTEMS

Principle 3: Conforming Product

- We shall ensure that our Products conform to their definition:
- with internal and, where necessary external, approvals for the organization and Product;
- by deploying suitably qualified and experienced people; and
- by applying independent assurance.

- Conforming Product – represents the assessment of the design/Product to “validate” that the required Level of Safety has been met via conformance to the established design requirements – **a Sensor**

Internal Policies require independent reviews of plans, designs, test results to ensure conformance at each stage of the Product Life Cycle
Product Safety related roles & levels of competency are defined, with ongoing competency assessment & development

BAE SYSTEMS

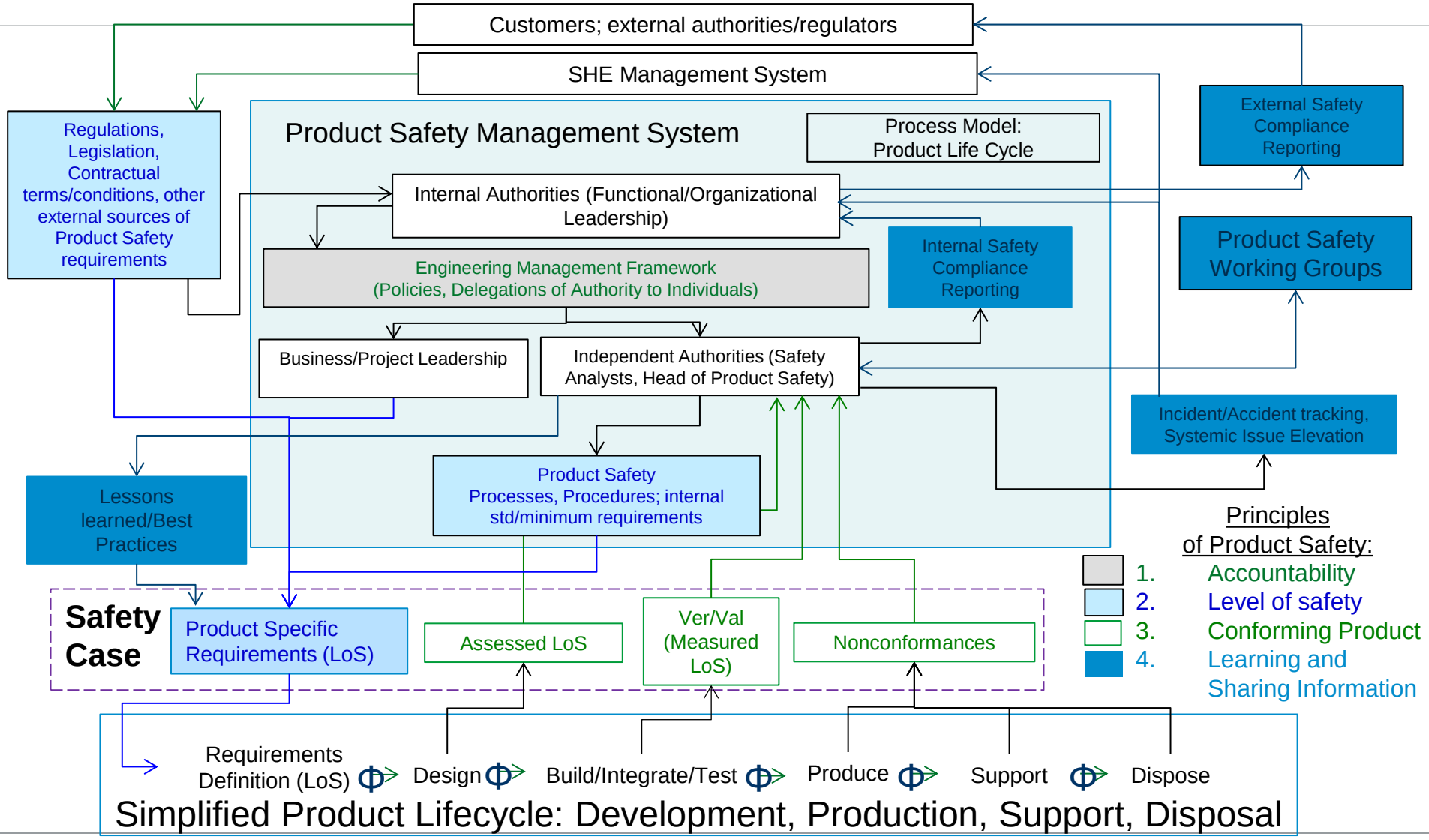
Principle 4: Learning and Sharing Information

- We shall work with our customers and suppliers through the life of each Product to:
  - provide topical information on safety so that each customer may determine how the Product is used, and obtain information on the use and performance of the Product to assess the consequences for safety;
  - understand the cause of significant accidents and incidents involving our Products, where appropriate with independent accident investigators, to reduce the probability of recurrence.
- We shall seek to learn from other parts of the company, organisations and domains.
- Learning and Sharing Information – since it is used for influencing Product Development and deriving knowledge during the development/deployment & use of existing Products = **Both Actuator & Sensor**

Incident & Accident tracking & reporting to Senior leadership;
Project/Customer Specific Safety Working Groups, and Safety Working groups at various levels internal to the Organization, for learning & sharing

BAE SYSTEMS

STPA Depiction of a PSMS ("simplified")



Questions?