# Semantic Annotation of Product Safety Information

Erik A. Gilsdorf
Department of Computer Integrated Design (DiK)
Technische Universität Darmstadt
Darmstadt, Germany
Email: gilsdorf@dik.tu-darmstadt.de

***Abstract*—Due to an increasing number of regulatory restrictions and a rising product complexity, compliance and safety management have become key issues for enterprises today. Besides the requirements to build safe products, documentation of safety compliance and in-use restrictions have to be archived and published by law. Some research projects have already tackled the problem of visually identifying hazards zones within virtual environments. Other approaches deal with the formal analysis of safety issues in expert systems for conformity checks. What is still missing is the bridge between visual representation and documentation. The virtual reality (VR) approaches do not support storage and processing of identified hazards, furthermore 3D models have to be prepared and converted to VR formats, which does not allow "online" analysis. Expert systems only cover an abstract, textual definition of hazard zones, which separates the safety domain from design. This paper describes a framework for "product safety information" to identify, track and document hazards and protective measures throughout the product life cycle. The underlying data model supports integration of geometric references into the safety information, similar to the use of product manufacturing information like GD&T.**

## I. Introduction

Compliance management has become a key issue for enterprises today. Regulatory restrictions, standards and company policies constrain the product development to a high level. Legal restrictions and standards concerning product safety demand the engineer's attention.
"Product safety" is often defined in a fuzzy manner, as the term is used synonymously with "product reliability". Safety concentrates on the preservation of human health and prevention of damage to goods. Reliability means the probability that under defined conditions a product will serve its purpose until its intended end-of-life [1]. If a product fails due to bad reliability causing hazards or even harm, this leads to poor safety as well.
International and national laws impose obligations on manufacturers and retailers to address product safety as an key issue of their business. These laws often refer to technical standards, which specify guidelines for specific products or categories of products. The overall aim of all these restrictions is to prevent any harm that could come along with a product's intended use or even predictable abuse. To support this, several tools and methods have been developed to support safety experts in identifying and solving safety issues. The weak point of these tools is the lacking ability to attach safety information directly to virtual product geometry and make it available for later reuse.

## II. Safety in the product life cycle

Product safety is one important, if not the most important requirement in product development. Yet, safety is not limited to the development of a product but is a key issues for all phases of a product's life, which are described by the "product life cycle".

There are several existing definitions of a generic product life cycle. In contrast to business definition, where a product's life cycle starts with sale and describes market situation and saturation, the engineering view includes product planning & design, manufacturing, sales, usage and disposal [2].
In order to reduce risk imposed by a product throughout its whole lifetime, tasks have to be planned and executed, which can be described as the "safety life cycle" [3]. In short it can be summarized into its main stages "analysis", "realization" and "operation" [4]. Any modification of a product results in a loop back.

### A. Analysis

Hazard analysis and risk assessment help to identify and rate intrinsic dangers arising from product properties as well as hazards caused by product failure. These two types of hazards are often referenced as *deterministic* and *stochastic* hazards [5]. Examples of product-intrinsic hazards are angular or live parts. A product failure on the other hand can lead to a hazard as well, when the product runs into a critical condition. Regarding the reliability of a product, three different kinds of designs can be distinguished, based on possible failure-modes [6]:

- **exclusion design**, which inhibits any fault at every (predictable) operation mode,
- **preventive design** to reduce the probability of a fault and
- **fail-safe design** to minimize the risk caused by a fault.

### B. Realization

Improved safety can be achieved by **inherently safe design** or **protective measures** [7]. This means when a hazard is identified, the focus should be to permanently eliminate it by a design change [8], [9]. Whenever that is not possible, protective measures should be taken. This can be interlocking guards or sensitive protective equipment. Besides technical

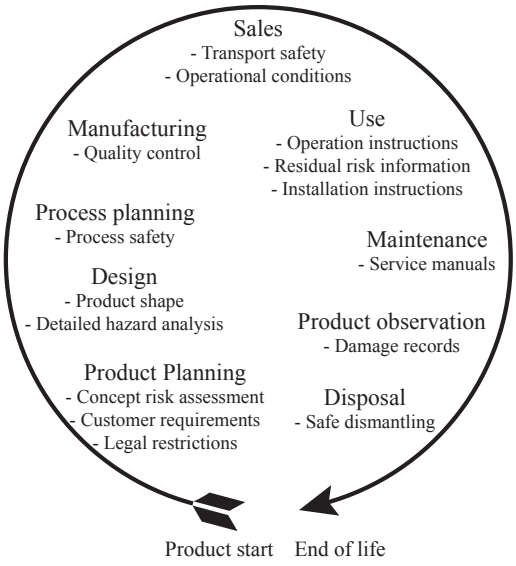



Fig. 1. Safety information in the product life cycle

measures, documentation of conducted risk assessments and residual risk is mandatory [8] . When a modification of the product arises at some point, a new hazard analysis has to be conducted.

### C. Operation

Once the product is realized, safety can be monitored in operating conditions and fed back to the manufacturer. Validation tests and maintenance reports are a valuable source of information.

## III. Safety information

During all stages of a product's life cycle, safety related information is generated [10] which has to be retrievable at later point in time at the same or even a different stage. Fig. 1 gives an incomplete overview about safety related information created at different points in product life.

### A. Internal and external safety information

Technical documentation in general can be distinguished into external and internal documentation, at which internal documentation resides inside the company, whereas external documentation is provided for sales, use, maintenance and disposal [10]. Safety information can be classified in the same way, i. e. risk assessments or design changes in development would typically not be published, while warning symbols or safety instructions are part of the user information. It can be assumed that internal documentation is more complex than external documentation, as the external information is processed from the internal one. Nevertheless there is a flow of information back to the manufacturer, for example as result of product observation and damage reports.

### B. Providers and receivers

Besides classification between internal and external information, the provider of the information as well as the intended receiver of the information are of interest for an effective filtering and responsibility management. This can be either achieved by a rough distinction of the information context, for example the product life cycle stage, or defined groups specified by criteria like organizational role, skills etc.
Internal safety information for example could be addressed to product designers or shopfloor workers, who are both interested in very different safety aspects. External safety information does not only address the product's user, but also can be valid for third-party safety experts, installation crew, maintenance personnel etc. [11].

## IV. Hazard identification - State of the Art

Many tools and methods have been developed for safety design, especially for hazard analysis. No matter which method is used, the outcome will be most likely a document listing the hazards with a description of reasons and possible consequences [3].
Besides traditional analysis tools like checklists and form sheets, computer applications have been developed that are supposed to support hazard analysis.
There are two main groups of applications that support safety design in product development. Knowledge-based systems incorporate checklists, rules and standards in a knowledge base. Their scope is to provide the correct set of applicable safety rules for a specific product depending on product properties, functions or field of operation and to assess safety compliance [12], [13].
The second group are the visual tools. These applications often use a virtual environment to support visual hazard analysis of digital prototypes by safety experts. Hazards can be flagged within the 3D environment and views saved for later review [14], [15].
The shortcoming of these two group is the missing link in between. While expert systems provide support at formal step-by-step hazard analysis and product certification by tracking and documenting safety issues, spatial information about hazards is at best limited to part identification numbers. Virtual environments perform well at visual identification of hazards, offering even motion or deformation simulation. Yet any hazards identified inside these systems are not really documented in a central repository, but just saved inside the application environment not offering any tracking along product modifications.

## V. Safety information linking to shape representation

The shortcoming of actual hazard analysis tools and methods is the rather abstract description of hazards zones. Spatial information is provided as textual description, which is fine for conceptual development, when a detailed design does not exist. As soon as the design gets a shape, visual annotation in a 3D environment is a more direct and accurate approach.

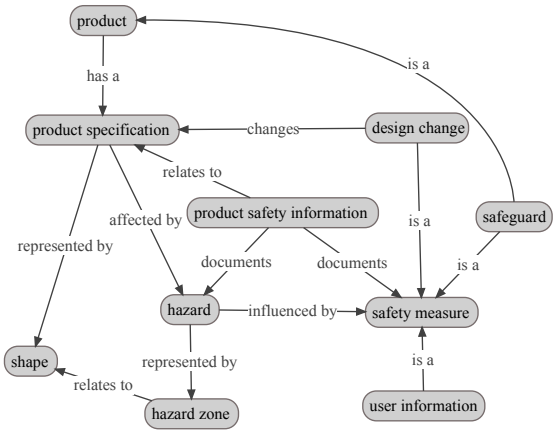



Fig. 2. Relations of product, hazard and safety measures

The concept presented in this papers supports storage of product safety information throughout the product's life cycle. Safety information can be attached to a shape representation of a product. Fig. 2 gives an simplified overview about the relationship between a product and its related safety relevant objects. A (physical) product is specified by a certain release version, which may change over time and development. This version is represented by a shape.

For a specific product release, hazards can be identified which may be result of the product release specification or the product category in general. As an example one might consider a combustion engine. While there might exist hazards like crushing or cutting, which are significant for the specific design, hazards arising from the use of combustibles are valid for all combustion engines. Spatial dimension of a hazard is defined by a hazard zone. This can either be a volumetric space, for example derived from the motion envelope of a machine's operating path or topological elements of the product's shape itself, like a sharp edge.

## VI. Protective measures

Once identified, hazards have to be addressed by protective measures described in section II-B. A design change will result in a new product specification, while safeguarding requires additional components. User information can generally be referred as a document. Combinations of protective measures for one hazard can occur, for example a safeguard combined with a warning sign.

The connecting element between product data, hazards and protective measures is identified as *product safety information (PSI)*. It gains in importance when versioning comes into play, as described in the following section.

## VII. Requirements for safety annotation

The annotation of safety information to product geometry requires a foundation that supports management of product safety information objects and fits together with common product data management. This foundation is defined by a data model.

### A. Data model

Requirements for a data model describing safety information in a product context have been defined as follows:

*1) Product identification:* Unambiguous product identification is a basic premise to any product data management. Product versioning has to be supported by the underlying data model, as well as different domain-specific views on a particular revision.

*2) Classification of safety information:* As described in section III-A, safety information can be classified as either internal (confidential) or external (public) to prevent unintended data leakage. The data model should provide a appropriate classification property, respectively support different views depending on life cycle stage.

*3) External reference:* A main objective of this work is linkage of safety information with shape representation in order to identify hazard zones. Therefore safety information should be able to target topological entities of external CAD files. Where safety information relies on pictorial content, binary image data like captures of product views or symbols should be stored and linked to safety information entities.

*4) Multiple views:* Safety information which has been stored together with other product data needs to be browseable and filterable according to criteria as related products, type, hazard type etc. Safety information needs to be independent of its representations, i.e. customized views for different users and tasks need to be supported.

### B. Visual annotation

When safety information like hazard warnings are linked to a product's shape or workspace, it seems natural that they are best described by attaching them directly to an existing visual representation of that object. Thus visual hazard analysis should be directly supported inside graphical applications used during product life.

The visualization of safety information should be as unambiguous and independent of cultural and linguistic preferences as possible to meet global product development demands.

## VIII. Data model

In general, a product is an assembly of parts or a single part. For better understanding, the following section does not make a difference between product, part and assembly.

### A. Product structure related to STEP PDM

STEP PDM Schema is a subset of several ISO 10303 application protocols for the management and exchange of product data. Fig. 3 shows a data model, whose structure closely follows STEP PDM Schema regarding the product package. A *product* (or part, STEP PDM does not make a difference here) usually runs through several development cycles or can exist in several specifications, which are represented by *product revisions*. Different views on the product revision, depending on task, life cycle stage or engineering domain, are subordinated as *product definitions*. Some product definitions do have shape definitions which again can be

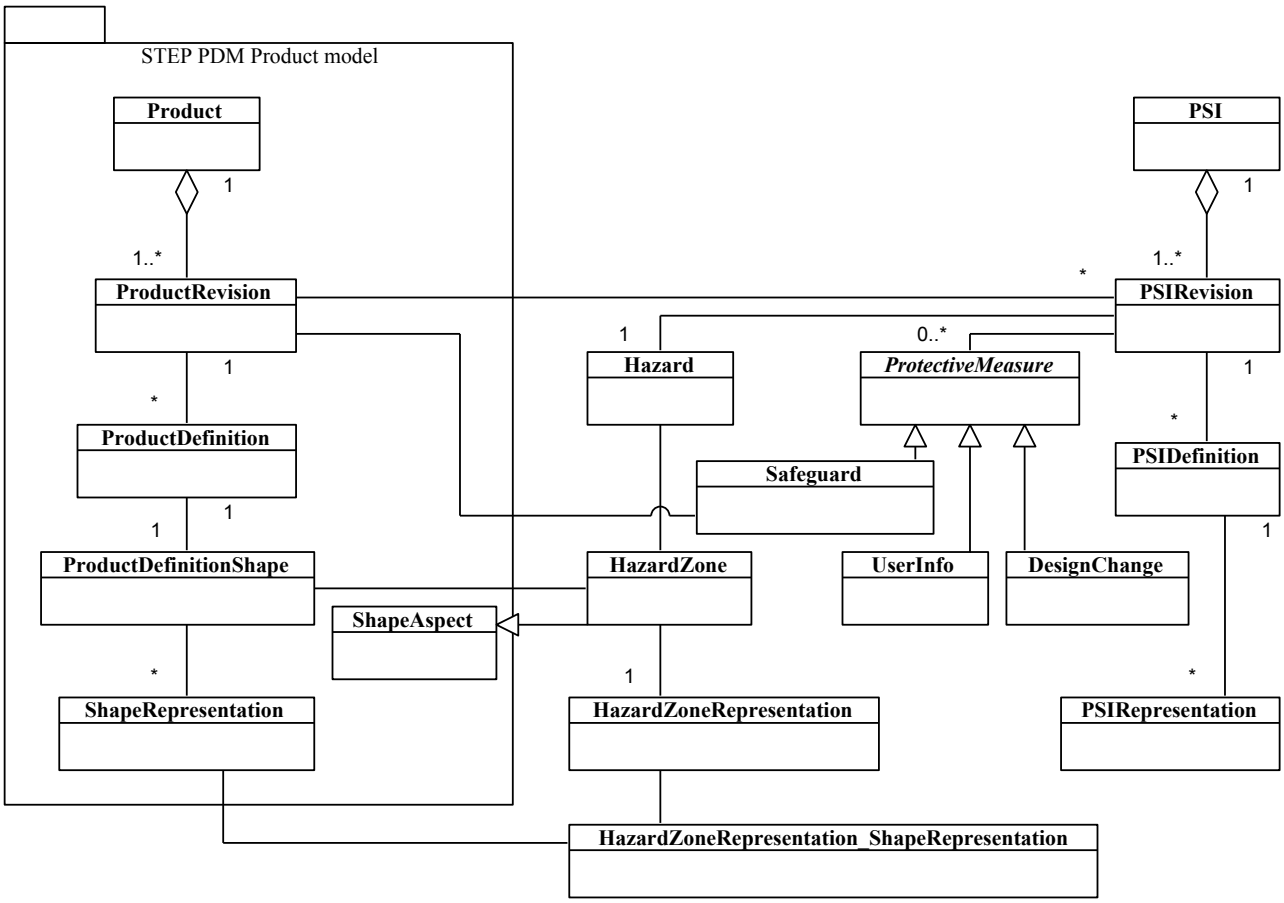



Fig. 3. UML data model

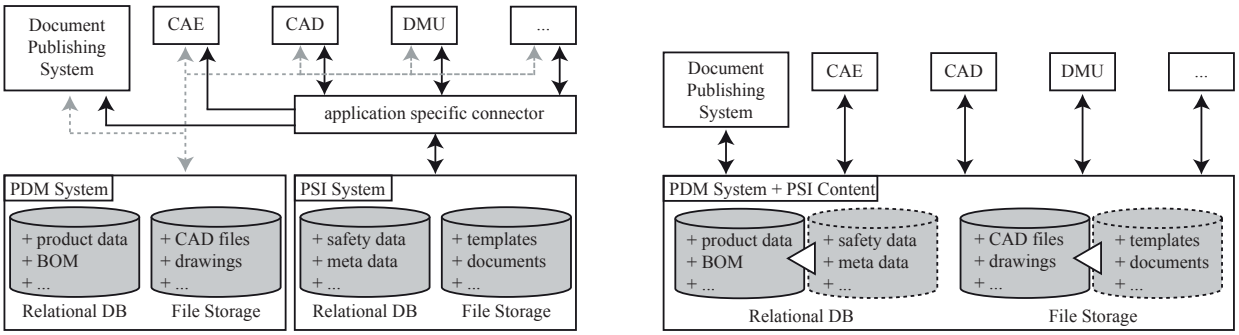
linked to geometric *shape representations*, externally defined by CAD files. According to STEP PDM Schema, documents are managed similarly, providing tracking of revision and multiple definitions [16].

### B. Product safety information model

Like a product, *product safety information* is specified by a revision. This is necessary to keep track of safety issues along the product life cycle or rather across product revisions.
A *PSI revision* always points to a specific product revision. However, several PSI revisions can be linked to the same product revision.
For different stakeholders of the safety life cycle, different views are specified by *PSI definitions*, this allows for example dedicated views for external usage, which will be generated by an expert. This views are then visualized by *PSI representations*
Protective measures inherit revisioning from their base classes. *Design changes* are a special case of protective measure, as they immediately influence product design. Implementing a design change means changing the product and by that creating a new product revision. A *safeguard* is a part itself. Thus, all relations and definitions for products are also valid for safeguards. This supports the idea of having modular designs reusing existing safeguard solutions, as the same safeguard revision can be referenced by several products. Depending on design strategy, the safeguard becomes a component of the product (assembly), which means it will be included in a new product revision.
*User information* is any information relevant to persons in contact with the product throughout its life cycle.
A hazard does not have revisions, as it is not actively designed or maintained.

### C. Spatial product safety information

Product safety information is often related to a product's shape or other spatial characteristics like its workspace. It is evident that mechanical hazards are bound to physical objects, but also different hazard categories have a spatial dimension. These *hazard zones* define areas where a person is in risk of a harm. The presented data model supports a conceptual description of a hazard zone which can detailed in a *hazard zone representation*, referencing generic topological objects, for example an edge, a face or a body. The mapping onto a product shape representation and its specific topological elements is described by a separate class (*HazardZoneRepresentation_ShapeRepresentation*).




(a) Side-by-side implementation with existing PDM

(b) Integration with existing PDM

Fig. 4. Different approaches of safety information management

## IX. Integration into PLM environment

Especially complex products demand software support for the management of product lifecycle data. A huge amount of this data can be managed by PDM (Product Data Management)-Systems. Effective safety information management has to take care of this precondition and needs to be included within existing product lifecycle management environments.

### A. Interaction with engineering applications

Two strategies to integrate PSI with an existing PDM solution can be identified.

The first solution (Fig. 4(a)) is to store all safety information in a separate database. Due to performance reasons binary files should be kept in a file storage and just referenced by the database entries. Applications access safety information through special connectors. Product data and structures are conventionally stored in standard PDM systems. This variant does not require customization of the PDM system.

A different strategy would be a PDM-centric approach (Fig.4(b)). All applications that have access to an existing PDM system do not need additional database connectors. On the downside, the PDM business model needs to be modified to handle additional information, which is always a risk regarding system updates. In the worst case, existing native application connectors cannot retrieve this information. Any application that does not connect to the PDM system will still need a connector, which then depends on the PDM system's interfaces.

### B. Prototype

A first prototype has been developed to demonstrate interoperability and validate the data model.

*1) Database:* The data model presented in Fig. 3 has been implemented in C#. Object-relational mapping to a SQL database is performed by Fluent NHibernate API.

*2) Hazard annotation:* Siemens NX 7.5 has been chosen as CAD front-end to annotate safety information to a 3D model. NX Open API supports .NET framework, which allows access to program functions and topological objects. As NX does not allow direct access to BREP (boundary representation) structure, all referenced NX-objects belonging to a hazard zone representation are stored in a custom container object. Hazards are annotated the same way product manufacturing information is annotated. They can be associated to any objects instantiated from subclasses of *DisplayableObject*, which are solid body, face, edge, point etc.. For the visualization, hazards symbols defined by ISO 7010 [17] and DIN 4844-2 [18] are used.

*3) Derived documents:* 3D annotations created inside NX are one possible view on the information content stored in the database for this PSI. Further representations can be created for different documentation purposes. Some can be directly derived inside NX: a drawing or a screenshot for example. Fig. 5(b) shows a drawing generated from 3D geometry. The hazard information has been selected to be included in that view. It is oriented automatically according to the generated view, no matter that the assembly has been flipped.

## X. Conclusion

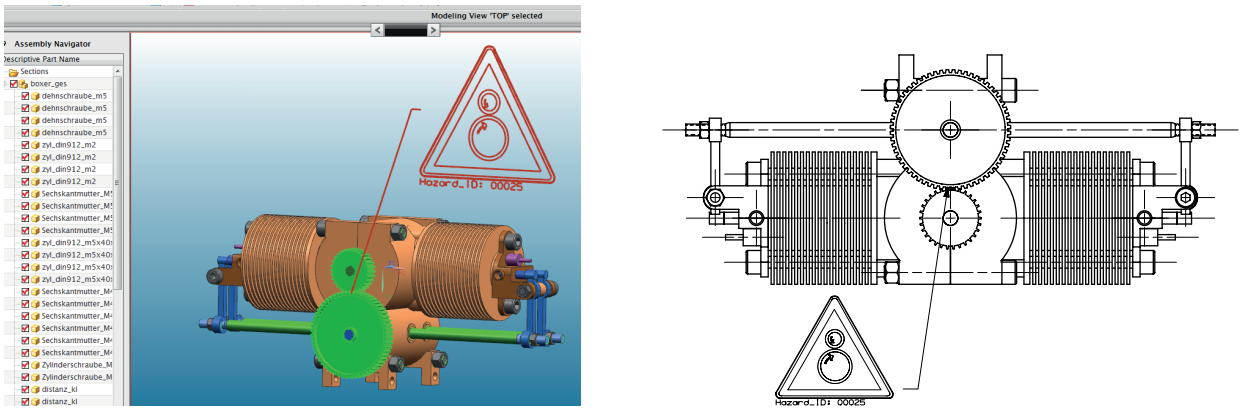
The presented approach has shown a possible way to link safety information to product geometry. A data model to support essential management of safety information has been developed. It takes into account that any safety related information is subject to change when modifications of the product are realized.

Integration with PDM systems has not been validated to its full extent, especially user rights management is still in need of investigation. Workflows provided by PDM systems promise better automation of hazard analysis and tracking of safety issues. A possible use case would be the triggering of an ECR workflow, whenever a protective measure requires a design change.

More research has to be done regarding the integration of end-user applications. Exchange of annotations between Adobe 3D PDF and CATIA has already been successfully validated by at the DiK by [19].

## Acknowledgment

The author would like to thank Daniel McKinley who contributed to the software prototype. Special thanks also go to Thomas Rollmann for his academic support.




(a) 3D model with safety annotation

(b) Derived drawing

Fig. 5. Visual hazard identification

## REFERENCES


[1] B. S. Dhillon, *Reliability, Quality, and Safety for Engineers*. CRC Press, 2005.

[2] J. Stark, *Product Lifecycle Management*, ser. Decision Engineering, R. Roy, Ed. Springer London, 2005.

[3] D. Macdonald, *Practical Machinery Safety*. Newnes, 2004.

[4] R. Ali, "How to implement a safety life-cycle," *Valve Magazine*, vol. 19, no. 3, pp. 1–6, 2007.

[5] A. Neudörfer, *Konstruieren sicherheitsgerechter Produkte: Methoden und systematische Lösungssammlungen zur EG-Maschinenrichtlinie*, 4th ed. Springer Berlin, 2011.

[6] M. S. Sanders and E. J. McCormick, *Human Factors in Engineering and Design*, 6th ed. McGraw-Hill Book Company New York, 1987.

[7] M. S. Wogalter, "Purposes and scope of warnings," in *Handbook of Warnings*, ser. Human Factors and Ergonomics, M. S. Wogalter, Ed. Lawrence Erlbaum Associates London, 2006, ch. 1, pp. 3–9.

[8] *ISO 12100: Safety of machinery – General principles for design – Risk assessment and risk reduction*, International Organization for Standardization Std., 2010.

[9] "Directive 2006/42/EC of they European Parliament and of they Council of 17 May 2006 on machinery, and amending Directive 95/16/EC (recast)," May 2006.

[10] *VDI 4500 Part 1: Technical documentation – Definitions and legal basics*, Verein Deutscher Ingenieure Std., Jun. 2006.

[11] E. P. Cox, III and M. S. Wogalter, "Warning source," in *Handbook of Warnings*, ser. Human Factors and Ergonomics, M. S. Wogalter, Ed. Lawrence Erlbaum Associates London, 2006, pp. 111–122.

[12] M. Elliott, "Computer-assisted fault-tree construction using a knowledge-based approach," *Reliability, IEEE Transactions on*, vol. 43, no. 1, pp. 112 –120, mar 1994.

[13] S. Dowlatshahi, "The role of product safety and liability in concurrent engineering," *Computers & Industrial Engineering*, vol. 41, no. 2, pp. 187–209, 2001.

[14] J. Järvinen, R. Kuivanen, and J. Viitaniemi, "Safety design by using three-dimensional simulation models," *International Journal of Industrial Ergonomics*, vol. 17, no. 4, pp. 343–350, Apr. 1996.

[15] T. Määttä, "Virtual environments in machinery safety analysis and participatory ergonomics," *Human Factors and Ergonomics in Manufacturing & Service Industries*, vol. 17, no. 5, pp. 435–443, 2007.

[16] M. Ungerer and K. Buchanan, "Usage guide for the STEP PDM Schema V1.2," ProSTEP iViP - PDM Implementor Forum, Tech. Rep., 2002.

[17] *ISO 7010: Graphical symbols - Safety colours and safety signs - Registered safety signs*, International Organization for Standardization Std., 2011.

[18] *DIN 4844-2: Graphical symbols - Safety colours and safety signs - Part 2: Registered safety signs*, Deutsches Institut für Normung e.V. prelim. Std. DIN 4844-2, Dec. 2010.

[19] D. Völz, A. Schüle, and R. Anderl, "An approach to use semantic annotations in global product development to bridge the gap in interdisciplinary and intercultural communication," in *Proceeding: WMSCI 2010*, vol. 3, Orland, Florida, USA, Jun. 2010.