Functional Safety

NSS'04 Session by CNC/IEC TFFS
Task Force on Functional Safety
Chairman: Bill Bryans
2004-11-15

Outside Operational parameters…

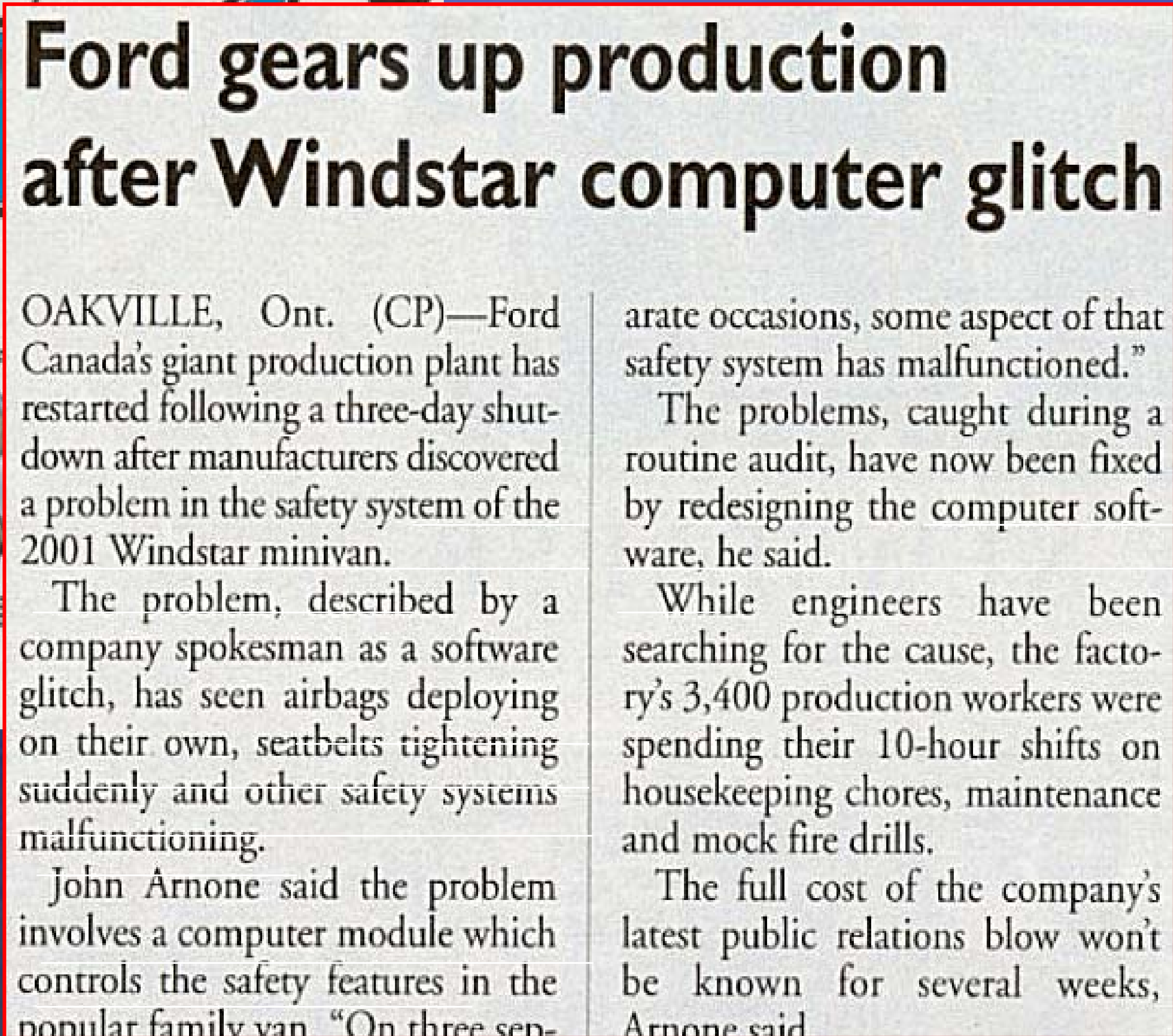
You think?

What happened?

Involve Functional Safety?

Stay tuned!

Functional safety application?



Ford gears up production after Windstar computer glitch

OAKVILLE, Ont. (CP)—Ford Canada's giant production plant has restarted following a three-day shutdown after manufacturers discovered a problem in the safety system of the 2001 Windstar minivan.

The problem, described by a company spokesman as a software glitch, has seen airbags deploying on their own, seatbelts tightening suddenly and other safety systems malfunctioning.

John Arnone said the problem involves a computer module which controls the safety features in the popular family van. "On three separate occasions, some aspect of that safety system has malfunctioned."

The problems, caught during a routine audit, have now been fixed by redesigning the computer software, he said.

While engineers have been searching for the cause, the factory's 3,400 production workers were spending their 10-hour shifts on housekeeping chores, maintenance and mock fire drills.

The full cost of the company's latest public relations blow won't be known for several weeks, Arnone said.

Objective and format for the session

- ***This session is to inform the audience on Functional Safety (FS) issues of concern to Canadian industry***
- ***Generate interest in new CDN committee memberships***
  - ***help position CDN industry in Global markets***
- ***The format is Q&A to encourage audience participation in the discussion***
- ***At the end of this session, the audience should gain basic knowledge on FS and the need for FS standardization***

TFFS activities to-date on FS standardization (background)

- *Preliminary study done by CNC/IEC TFFS on FS standards and requirements*
  - *Canadian, Regional and International*
  - *performed overlap and gap analysis*
- *Recommendations made in TFFS Roadmap report*
  - *initiated FS session for public information*
  - *identified the need for Canadian initiatives on FS standard to facilitate Canadian corporations and SME entry to global FS competitive markets*

Summary of our Discussion Topics

(Q1) What is Functional Safety (FS)?

(Q2) Why is FS important and requiring standardization?

(Q3) Why are FS standards needed in Canada?

(Q4) What benefits would FS standards bring to Canadian industry and business?

(Q5) What should be done to facilitate FS standardization in Canada?

(Q1) What is Functional Safety?

In the context of products and systems related to safe operation:

- ***What is a <u>function</u>?***
- ***What does <u>safe</u> mean to you?***
- ***What is <u>safety</u>?***
- ***What is <u>functional safety</u>?***
- ***What is <u>assurance</u>?***

(A1) <u>Possible</u> answers relating to FS

function

- *an expected activity or operation*
- *a design feature that meets the desired application*

functional

- *ability to perform a **function***

safe

- *free from harm or unacceptable risk*
- *secure from threat of danger, harm, or loss*

safety

- *condition of being **safe***

***functional safety** (FS) from IEC 61508-0 (TR)*

- *part of the overall safety that depends on a system or equipment operating correctly in response to its inputs*

Assurance

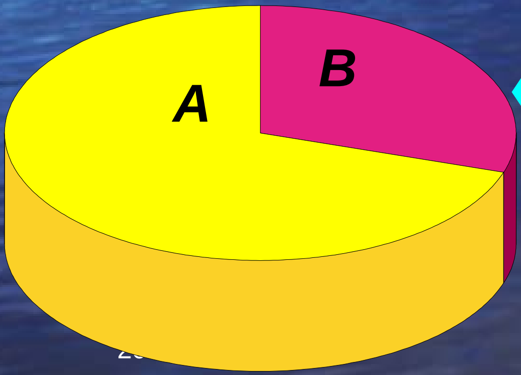
- *Ascertaining that the functions are present and will work when required*

Functional Safety

Another Definition

“<u>Part of the overall</u> safety relating to the equipment and its associated control system which depends on the correct functioning of electrical, electronic, programmable electronic (E/E/PE) safety-related systems………………………………….”.

Safety = A + B
Passive Safety = A
Functional Safety (active) = B



Required risk reduction achieved by means of E/E/PE safety-related systems

FS Examples

- *Control mechanism to turn off a microwave oven or a kitchen appliance using microwave energy to heat food (emission limits)*
- *A sensing device in an infusion machine to regulate blood flow to patients during surgery (flow detection)*
- *Automated control apparatus for control of equipment application functions (programmable control of application functions with pre-assigned operating limits)*
- *Air traffic control system using complex electronic subsystems with human-machine interactions to guide air traffic (multi-system functions designed for air traffic safety and set alarm for abnormal conditions)*
- *On-line banking or e-commerce engaging interactive information systems and security checks for control of user access to financial transactions*

Outside Operational parameters…

You think?

What happened?

Involve Functional Safety?

Stay tuned!

Functional safety application?

Ford gears up production after Windstar computer glitch

OAKVILLE, Ont. (CP)—Ford Canada's giant production plant has restarted following a three-day shutdown after manufacturers discovered a problem in the safety system of the 2001 Windstar minivan.

The problem, described by a company spokesman as a software glitch, has seen airbags deploying on their own, seatbelts tightening suddenly and other safety systems malfunctioning.

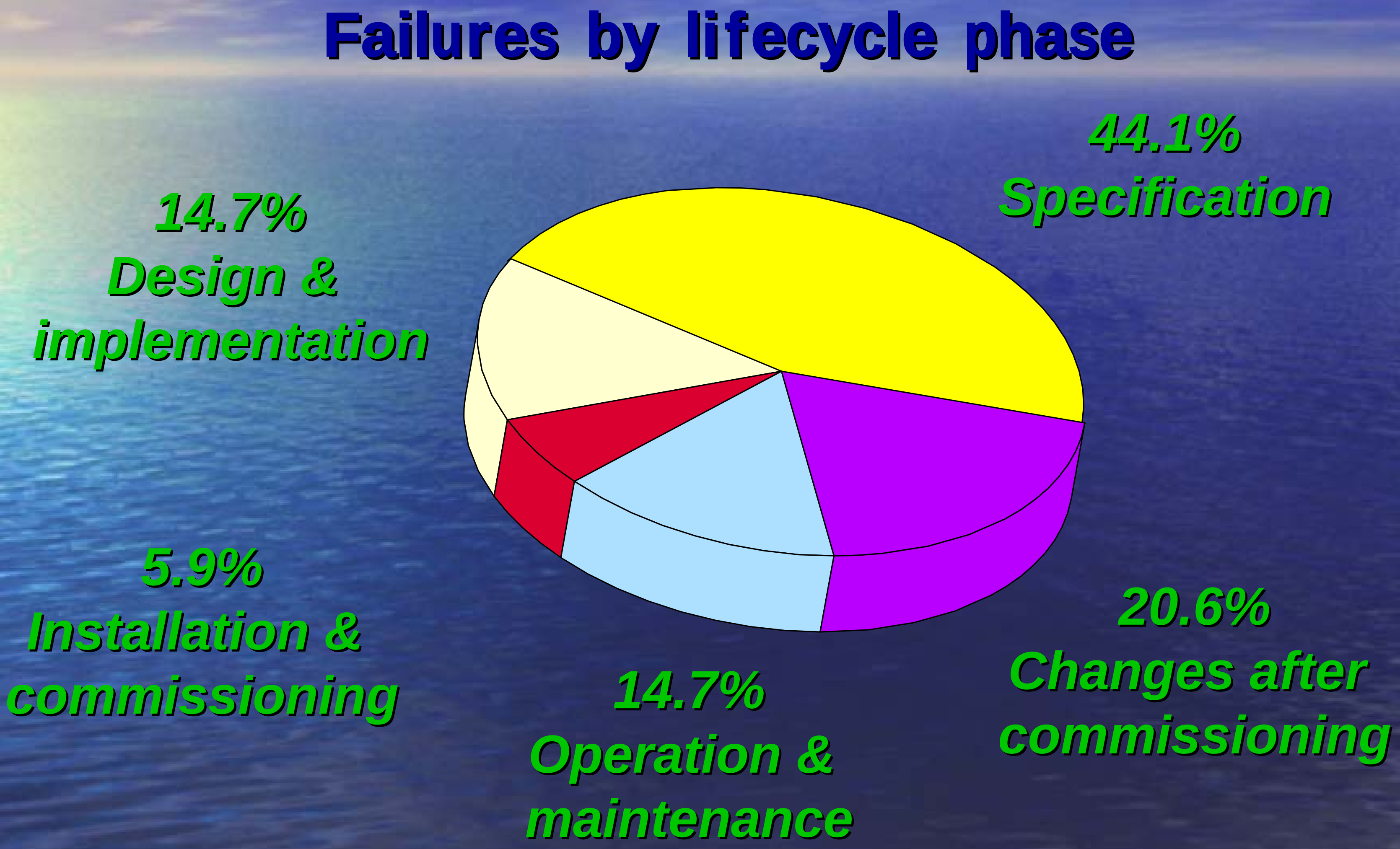
John Arnone said the problem involves a computer module which controls the safety features in the popular family van. "On three separate occasions, some aspect of that safety system has malfunctioned."

The problems, caught during a routine audit, have now been fixed by redesigning the computer software, he said.

While engineers have been searching for the cause, the factory's 3,400 production workers were spending their 10-hour shifts on housekeeping chores, maintenance and mock fire drills.

The full cost of the company's latest public relations blow won't be known for several weeks, Arnone said.

Primary cause (by lifecycle phase) of control system failure *[based on 34 incidents]*



(Q2) Why is FS important requiring standardization?

- *What technologies are involved in FS products and systems?*
- *Does FS need to be designed into the product or system to realize its safe and reliable operation?*
- *Is FS important to Canadian manufacturing industry, suppliers and developers of safety-related products and systems?*
- *Do you know that there are published guidelines, tools and techniques available to help you in your purchase or selection of safety-related products and systems?*
- *Do you know or use any FS standards?*

(A2) Importance of FS standardization

- *FS has been around a long time for very complex Operations -*

  but there are new emerging technology & concepts applicable for safety, security protection, & dependability opportunities
- *FS is needed in design and operation lifecycle of dependable electronic and programmable electronic products and systems involving hardware, software and human elements*
- *IEC 61508 sets the FS framework requirements and is used as bases for safety-related regulations, now in Europe and may quickly spread to other countries, including Canada*
- *FS is important to Canadian manufacturing industry, & suppliers & developers of safety-related systems & products to meet FS requirements, both domestically & internationally*
- *Common guidelines, methodology and techniques can be used as tools to assure that criteria on safety, security, and dependability are met*

(Q3) Why are FS standards needed in Canada?

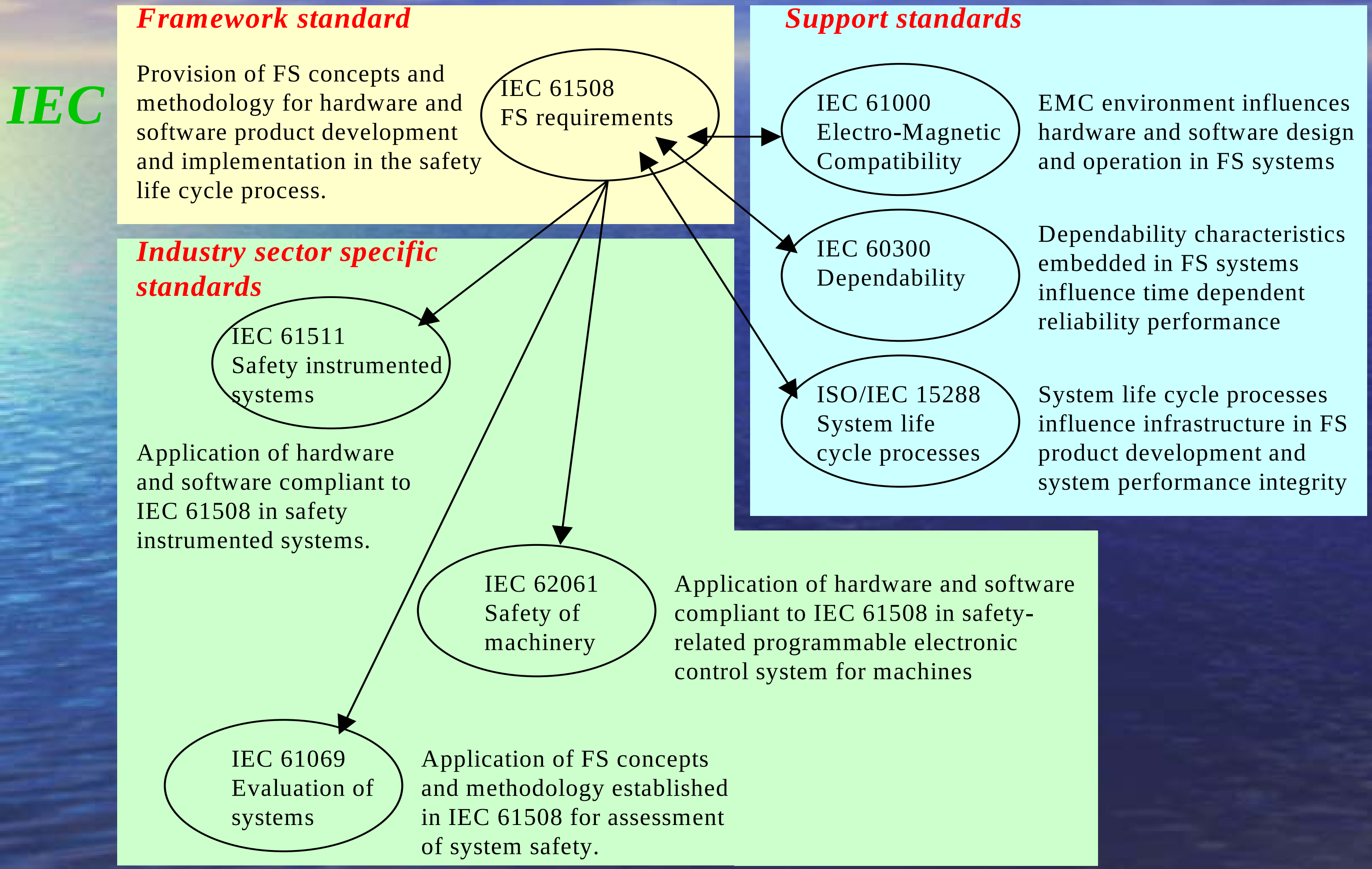
- *Have you heard of IEC 61508 standard?*
- *Do you know what FS standards are used in Canada, if so how?*
- *Have you heard of CSA C22.2 No. 0.8 standard?*
- *As a trading nation, do Canadian companies need to comply with FS standards to do business, nationally or internationally?*
- *Are there any FS regulations in Canada or elsewhere?*

(A3) IEC 61508 Standard

- *IEC 61508: Functional safety of electrical/electronic/programmable electronic (E/E/PE) safety-related systems*
- *The standard has 7 parts :*

  Part 1: General requirements
  Part 2: Requirements for E/E/PE safety-related systems
  Part 3: Software requirements
  Part 4: Definitions and abbreviations
  Part 5: Examples of methods for the determination of safety integrity levels
  Part 6: Guidelines on the application of Part 2 and Part 3
  Part 7: Overview of techniques and measures
- *IEC 61508 covers all safety-related systems that are electrotechnical in nature (i.e. electromechanical systems, solid-state electronic systems and computer-based systems).*
- *IEC 61508 provides a generic framework approach for all safety lifecycle activities for E/E/PE safety-related systems that are used to perform safety functions. It facilitates the development of standards and guides for application sectors and specific subsystems and components.*

IEC Standard Relationships



IEC

Framework standard

Provision of FS concepts and methodology for hardware and software product development and implementation in the safety life cycle process.

IEC 61508
FS requirements

Support standards

IEC 61000
Electro-Magnetic
Compatibility

EMC environment influences hardware and software design and operation in FS systems

IEC 60300
Dependability

Dependability characteristics embedded in FS systems influence time dependent reliability performance

ISO/IEC 15288
System life
cycle processes

System life cycle processes influence infrastructure in FS product development and system performance integrity

Industry sector specific standards

IEC 61511
Safety instrumented
systems

Application of hardware and software compliant to IEC 61508 in safety instrumented systems.

IEC 62061
Safety of
machinery

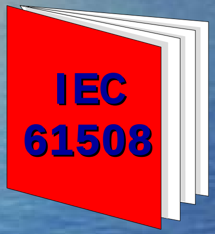
Application of hardware and software compliant to IEC 61508 in safety-related programmable electronic control system for machines

IEC 61069
Evaluation of
systems

Application of FS concepts and methodology established in IEC 61508 for assessment of system safety.

Standalone and sector/product standards

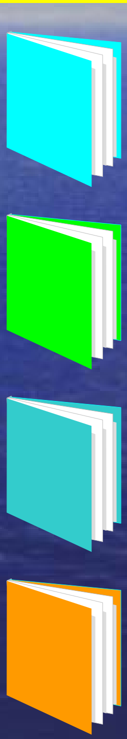
Standalone



Systems, components
& subsystems
to IEC 61508

Compliance
to IEC 61508

Sector & product implementations



IEC 62061: Machinery

IEC 61511: Process

IEC 61513: Nuclear

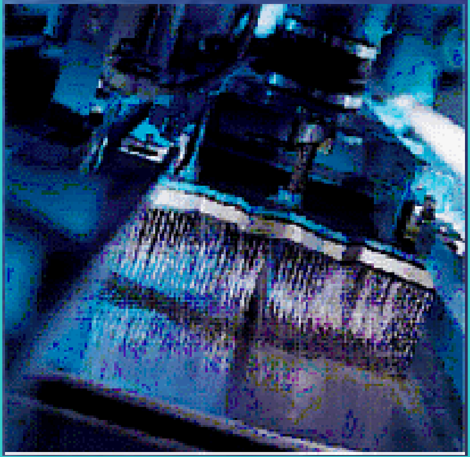
Product (e.g. PLCs)

Compliance
to IEC xxxxx

Safety related applications Sectors

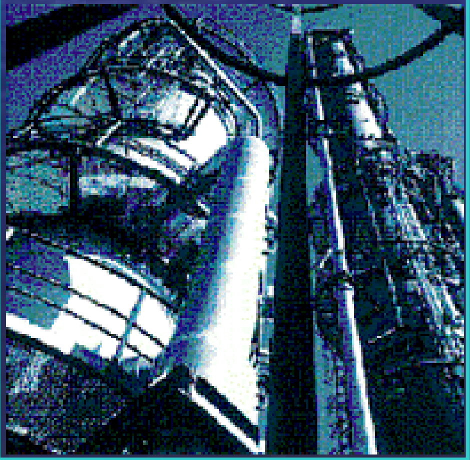
Machine protection

- Conveyor systems
- Presses
- Machining and processing equipment
- Machine tools
- ...



Process engineering

- Burner control
- Oil industry
- Chemicals
- ...



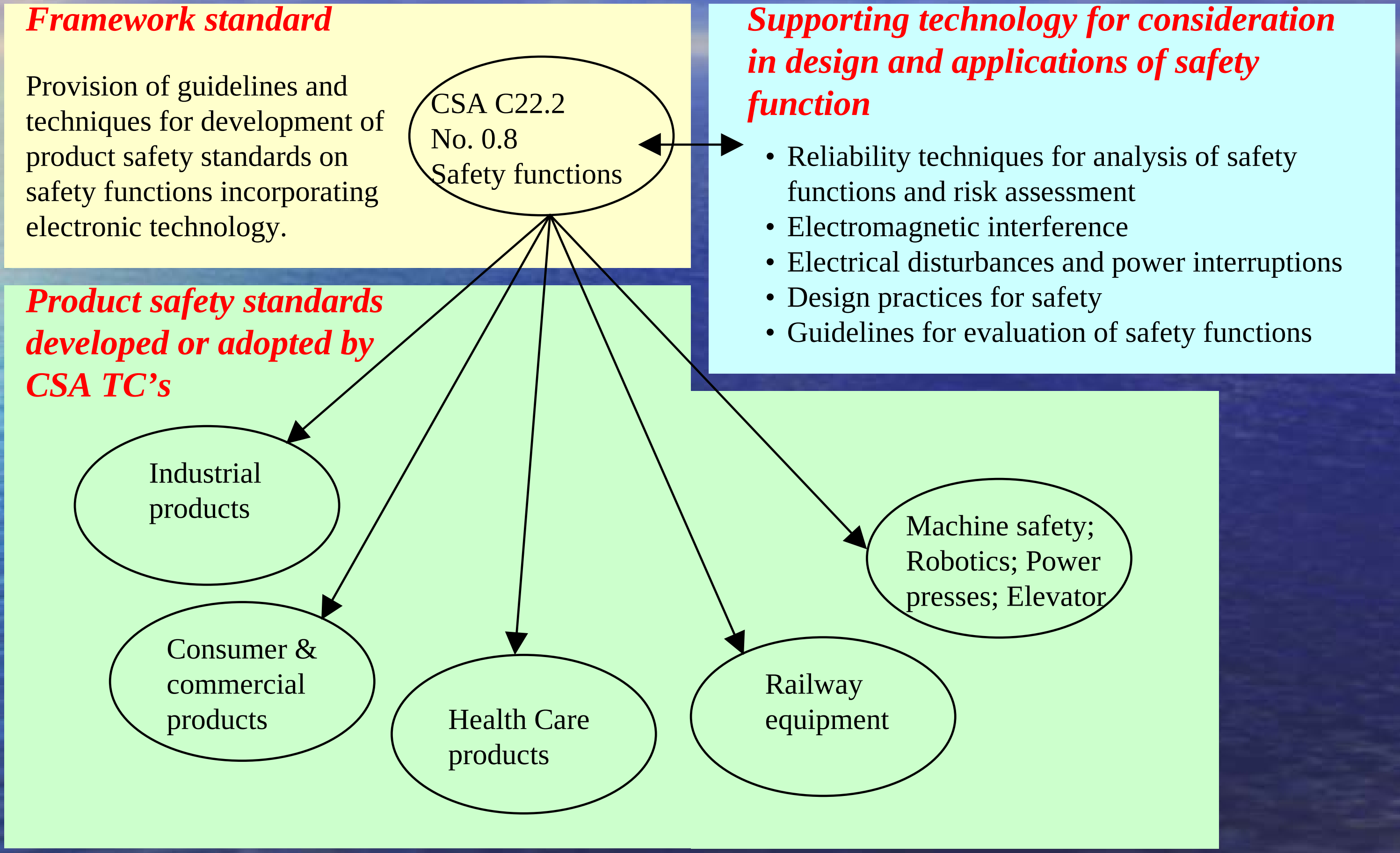
Passenger transport

- Cable railways
- Lifting platforms
- ...

(A3) CSA C22.2 No. 0.8 standard

- *CSA C22.2 No. 0.8: Safety functions incorporating electronic technology*
- *C22.2 No. 0.8 applies to devices, such as electronic components, assemblies, or systems including software and firmware that perform a safety function. A safety function means a mechanism that is incorporated into a device in order to minimize anticipated hazards.*
- *C22.2 No. 0.8 provides general guidelines for safety analysis in design, and evaluation and test of electronic safety functions. It applies to any product, depending on its complexity and the criticality of the safety function it performs as specified by the criteria in the individual standards of the Canadian Electrical Code, Part II.*

CSA Standard Relationships



CSA

Framework standard

Provision of guidelines and techniques for development of product safety standards on safety functions incorporating electronic technology.

CSA C22.2
No. 0.8
Safety functions

Supporting technology for consideration in design and applications of safety function

- Reliability techniques for analysis of safety functions and risk assessment
- Electromagnetic interference
- Electrical disturbances and power interruptions
- Design practices for safety
- Guidelines for evaluation of safety functions

Product safety standards developed or adopted by CSA TC's

Industrial products

Consumer & commercial products

Health Care products

Railway equipment

Machine safety; Robotics; Power presses; Elevator

(A3) Comparison of standards

- *CSA C22.2 No. 0.8-M1986 (Reaffirmed 1999): Safety functions incorporating electronic technology is out-of-date due to technology advancement*
- *IEC 61508 (1998): Functional safety of E/E/PE safety-related systems is a framework standard on FS requirements to guide development of sector-specific FS standards*
- *IEC 61508 is applicable to large scale systems with well established infrastructure and processes*
- *IEC 61508 requirements are complex and often require expert interpretations (e.g. Safety Integration Level - SIL)*
- *There are not too many large scale safety-related systems in the Canada starting development from the ground up*
- *Existing safety-related systems are legacy systems needing performance enhancement, capacity upgrade or service improvement*

(Q4) What benefits would FS standards bring to Canadian industry and business?

- *Is FS a possible new business opportunity for Canada?*
- *Does FS only apply to large process plants for safe operation?*
- *Is there something for the SME with FS expertise to develop new product and service applications?*
- *Where is our market for FS?*

(A4) Some benefits on FS applications

- *Challenges for Canada are on safe plant operation utilizing FS technology and provision of FS products and expert services to existing and new safety-related systems on a global basis*
- *Ideal market niche for Canadian corporations and SME with FS expertise to develop suitable platform technology for diverse product applications and service provisions*
- *New business opportunities include FS project management and engineering, FS design and applications of hardware/software integrity, dependability in networks and systems, safety and security assurance, and FS conformity assessment*

(Q5) What should be done to facilitate FS standardization in Canada?

- *How are the following sectors involved in FS standardization issues?*
  - *industry*
  - *government*
  - *science and technology institutions*
- *Do we need training to industry work force?*
- *Do we need to educate our students on FS in our academic institutions?*
- *Do we need to harmonize our Canadian FS standard and requirements with the international FS standards?*
- *Do we need to establish an industry forum on FS to deal with evolving technologies, and to update and share our knowledge?*

(A5) Actions needed for FS standard implementation

- *Need collaboration amongst industry-government-science and technology community*
- *Need grass-root approach to promote and share FS knowledge base*
- *Need to establish Canadian FS standard and requirements to harmonize with international standards*

Recommended steps for FS management within your Company

- *Know the FS standards involved*
- *Emphasize FS planning and evaluation*
  - *- make this part of Management System policy and procedure*
- *Establish criteria for FS product development and servicing of safety-related systems*
- *Educate users by warning, labeling, and communications to effect fitness-for-use and compliant to safety regulations*
- *Monitor new product introduction and user feedback*
- *Establish FS database on knowledge gained for continual improvement*
- *Contribute to FS knowledge base*
  - *- internally, your Supply Chain and national standards*
- *Get involved in the national and international efforts toward FS standard development and harmonization*

Recommended steps to achieve FS in product development

- *Understand FS requirements in product use environments*
- *Define product application scenario*
- *Establish FS criteria and determine potential risk exposures*
- *Incorporate fault tolerant designs to meet expected/intended applications*
- *Design for risk containment and mitigation*
- *Assess criticality of FS for acceptable risks in safety-related system realization*
- *Validate achievement of Integrity Levels*
- *Obtain certification if needed*
- *Gain user confidence in product applications*
- *Collect performance data for FS performance improvement*

Additional information

- *www.iec.ch/functionalsafety FS Zone*
  - *IEC introductory brochure on IEC 61508: Functional safety of electrical/electronic/programmable electronic safety-related systems*
  - *A basic guide on FS and IEC 61508*
- *Contact information:*
  - *CSA: David Mascarenhas:* david.mascarenhas@csa.ca
  - *SCC: Loise de Silva:* ldesilva@scc.ca