Principles

Safety by Design Principles for Consumer Goods and Services

National Consumer Federation

@NCFvoice
nationalconsumer.org.uk

Safety by Design Principles for Consumer Goods and Services with automated control features that affect physical safety (i.e. software controlled functionality)

Introduction – Why Safety by Design for 'Digital'

The safe design of consumer products is the 'front line' in consumer protection. Traditional product safety standards depend on about 4,500 specific product type British Standards to bring about safe product design. However these standards are not built for the world of digital product control by software and algorithms.

Practically there are four ways in which software may be incorporated into a consumer 'product' (goods or services) that have the potential to introduce physical safety concerns additional (or significantly different) to the concerns applying to products without software or complex algorithms being involved:

A) *Enabling remote control*
For network connected products whether the control is exercised by the consumer, another human or an automatic system. Remote control loss due to connections and the inability to remotely sense unsafe hazardous conditions.

B) *Ever-changing software and hence product functionality and performance*
Involving software in a consumer device, or a remote control service, that is capable of being re-programmed during the lifetime of the product. Software change may be by download or physical replacement of the media on which the control software is stored.

C) *Control involving use of algorithms for control in complex situations*
Ranging from complex algorithmic designs by humans through to involving or determined by artificial intelligence learning during use of the product by consumer(s). This would include most systems that allow a consumer to control a product by voice command

D) *Interactions between humans and automated control as control passes between them or requires joint actions.*
Involving products where safe operation requires the automated control to pass control back to humans or for constant human supervision and intervention.

In the digital world there are a very few standards like IEC 61508 for the Functional safety of electrical/electronic/ programmable electronic safety-related systems. IEC 61508 etc. are good practice process standards to address the processes for embedding good design and maintaining that safe design over a product's lifecycle. BS EN 60335; a domestic appliances safety standard has started to appreciate some of the implications of software providing product functionality. Such standards currently do not however address the fundamental

principles of what constitutes 'safe operation' when automated control is part of a product's capabilities, taking into account user behaviour, user capability and vulnerability.
Note: The Product lifecycle impact needs to be taken into account too as design is upgraded during its lifecycle and has consequential effects from software or component change. Addressing the product lifecycle issues is essential to ensuring ongoing safety of users.

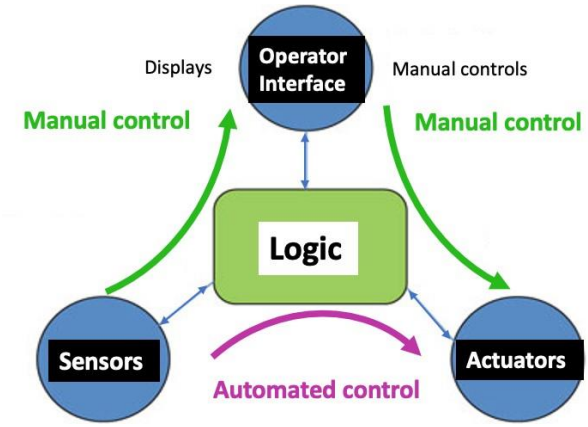
So a small number of consumer digital and safety experts have been brought together by the NCF and ESF to map out a preliminary view of what those safe functionality design principles should be. To do that we have looked at some use cases where even large capable organisations like Boeing, Tesla and the US Navy have made design mistakes or not taken account of the user interface leading to the cause of real accidents and deaths. We have tried to learn from those mistakes in setting out the straw principles outlined below.

In this exercise it is important to remember that security of processing is fundamental to safety of a product's functionality so that the control exercised is not maliciously altered throughout the lifecycle of a product.

The security implications for safe operation have been included with the functional performance principles.

Functions of automated product control.

The key functionality that is likely to be incorporated into software controlled products consists of :



Sensors of (variations in) physical conditions in an environment or the condition of Users

Actuators that allow digital signals to activate or vary the delivery of forces, power to machines, heating or lighting systems, or physical matter (liquids, gases, doses of medicines) or instructions/information to users.

Control functions realised in software

Human user physical control/input means (hands-on, present, line of sight or remote)

Human interface systems (e.g. displays, speakers)

Security features restricting access to control (and/or privacy) to specific user(s)

Principle 1: Safe Sensing

When a product has the ability to change its physical operation with actuators that are controlled digitally with algorithms and software.

For safe sensing design it is essential that :

- For safety critical functions sensor redundancy is applied, Safety critical operation shall not depend on the reliability of a single sensor
- Sensing design is capable of sensing hazardous conditions including those from reasonably foreseeable use
- Sensing capability is compatible with control and actuator ability to react to hazards
- Interoperability of sensors does not create hazardous condition(s).

Principle 2: Consumer control

When a consumer chooses to exercise direct manual control of a product (i.e. not consumer remote) the overriding safety limitations must be ensured by hardwired/mechanical interlocks and cut-outs.

The consumer should always have the direct control option (overriding automatic software or remote control) to put the product into default safe mode indefinitely and (ultimately) to shut the product down (in a safe way).

For manual control safe design it is essential that :

- consumer users always have overriding control when present with the product (ie overriding any remote control functionality)
- Externally sourced 3rd party requests for control are designed into products in a manner that consumers retain overriding control.
- Notification of a 3rd party control request is provided and authorisation given by the consumer. (see also principle 8 Security)
- Instructions for manual override are not needed and manual controls for override should be clear and accessible

Exception to the above is permitted where consumer inaction is likely to result in serious risk of harm, such as to facilitate a product recall.

Principle 3: Safe product actuation

When a product has automated actuation of its physical behaviour it should operate safely.

For safe automated actuator design it is essential that :

- Actuators and their control are capable of reacting to hazardous conditions detected by sensors/control logic or humans so as to reduce risks to a tolerable level.

- Automated actuator control is unable to cause injury to the user or create more a hazardous situation or risk of greater injury to others than the risk events themselves.

Principle 4: Safe remote control

When remote control is applied to a product without a human presence to overview the product's safe operation.

For safe remote control design it is essential that :

- Remote control is only be applied when monitoring of a product's safe operation is possible and enabled
- Product sensing for remote control for hazards include the internal functioning of the product and its external environment.
- Remote control is applied within consumer's (and the product's) safe use parameters e.g. temperature not permitted to fall below X°C – and not rely on tripping/hitting hard-wired or physical limiters. (i.e. these remain a second line of protection)
- Control conflicts are not permitted or if they arise be referred to the consumer
- Consumer awareness of risk identification is considered – for example, use of non-smart products used with smart socket interface.

Principle 5: Design for real consumer abilities and behaviours

Theoretical behavioural design or design based on un-evidenced assumptions can lead to unsafe control logic. It is unsafe to assume that instructions will be followed by all users in all cases.

For safe design for consumers it is essential that:

- Design is based on target users' real capabilities, behaviours, vulnerabilities and use.
- Design provides use that is ideally intuitive, but is at least familiar, simple and easy to understand

Principle 6: Safe operation with digital unavailability of data or functionality

Software and or control algorithms may not always be available or functioning during use of a product, for example if software is being updated online, the product is re-booting, the product is hacked or remote functionality is temporarily unavailable such as loss of WiFi connection, loss of external product functionality support system or under fault conditions.

For safe automated control design for consumers it is essential that :

- Products are designed to revert to a default safe mode when control software is not operational or available. This must be a shutdown or standby condition or a sustained

operation that will be indefinitely safe for the product, current users and any persons or property in the vicinity.

- If a product depends for safe operation on time critical functionality or data supply when these are not available or interrupted the product continues to function safely under the control of the consumer or to the default safe mode
- The return of automated functionality must not create unsafe operation of the product – or it requires authorisation and oversight by a user.

Principle 7: Safe user interfaces

In addition to the safe design principle 5 for user controls, consumer products may include displays showing product performance and/or alarm indicators. Complex presentation of information confuses and can lead to unsafe decisions by users.

For safe user interface design and operation for consumers it is essential that :

- Product performance data provided to users is simple and easy to understand, taking account of user behaviour and physical impairment, as appropriate.
- Clear indications to the consumer is provided to alert when local or remote product functionality is in use
- Clear indications to the consumer be provided when the product is operating in default safe mode while data is being input remotely for the product. Users should be warned if updates may cause noticeable changes to the product's operation or to aspects of the interface (e.g. messages/ user control features).

Principle 8 - Security and product safety

When a product is connected to a network the product must be designed with security that protects the consumer's safety under reasonably foreseeable use :

- It must have secure access and authentication controls to ensure only actors authorised by the consumer can have control.
- Must hold any confidential information securely (e.g. Encryption)
- Data flow to and from the product must be protected from being interfered with.
- Must be protect from unauthorised access or unauthorised remote modification throughout the life of product with protection updates.
  Must have software written to existing industry security or protection standards.

Principle 9 – Installation

For safe operation products must be designed to allow installation by the consumer through plug and play or they must be installed by a competent person(s), in accordance with the manufacturers instructions.

- End -