Another EMC resource
from EMC Standards

The Safe Design of Electrical Equipment & LVD compliance - Updated Feb 2021

LVD09 2.0 v3.1

Helping you solve your EMC problems

1 Brassey Road, Old Potts Way, Shrewsbury, SY3 7FA T:+44 (0) 1785 660 247 E:info@emcstandards.co.uk

LVD09 2.0 v3.1

The Safe Design of Electrical Equipment, and compliance with the LVD or RED – or their equivalent UK Regulations

(2 days, includes IEC 62368-1)

Keith Armstrong CEng, FIEE/IET, Senior MIEEE, ACGI, EurIng (Gp1)
phone/fax: +44 (0)1785 660 247
keith.armstrong@cherryclough.com, www.cherryclough.com, www.emcstandards.co.uk
More training courses and textbooks on-line: https://www.emcstandards.co.uk/online-training
Keith's Blog: https://www.emcstandards.co.uk/blog
Linked In: https://www.linkedin.com/in/keith-armstrong-449801172/

LVD09 2.0 v3.1

Change Record: v2.4 – v3.1, Feb 2021

- **Material added on the UK Regulations replacing the LVD and RED, modifying the following slides: 62 (was 63), 77 (was 78), 85 (was 86), 132 (was 130), 155 (was 153), 171 (was 169).**
- **Material added on the 2020 version of IEC/EN 60335-1, has affected and/or created new the following slides:**
  171 (was 169), 174 (was 172), *new 184 and 187-190*, 197 (was 190), 205 (was 198), 206 (was 199), 223 (was 216), 227 (was 220), 233 (was 226), 241 (was 234), 243 (was 236), 264 (was 257), 267 (was 260), 281 (was 274), *new 283*, 284 (was 276), 300 (was 292), *new 302*, 303 (was 294), 306 (was 299), 321 (was 314), 344 (was 337), 370 (was 363), 372 (was 365), 375 (was 368), *new 384*, 385 (was 377), 407 (was 399), 412 (was 404), *new 412-413*, 423 (was 402), 438 (was 414), *new 439-440 and 495*.
- **Other new slides added: 8, 11, 125, 126, 386, 387, 407-411**
- **Slides that have been *substantially modified*:**
  52 (was 53), 56-57 (were 57-58), 113 (was 114), 133 (was 131), 502 (was 475)
- **Some other slides have been *slightly* modified (sorry: they are not listed)**
- **Other slides renumbered: 414-415 on 'Preventing Corrosion' (were 295-296)**
- **Other slides renumbered: 397-404 on 'Checking component data' and 'Counterfeiting', (were 380-387)**
- **Other slides renumbered: 441-494 (were 415-468) and 496-529 (were 469-502)**

LVD09 2.0 v3.1

CCC

Overall contents list

Throughout this course, the word 'earth' = 'ground' and vice-versa

LVD09 2.0 v3.1

CCC

Disclaimer

This course is only a *brief guide*

- **Responsibility for safety of your equipment, employees, customers and third parties…**
  - ***–is yours alone !!!!***
- **Each individual *must*, in their work, apply the latest safety knowledge, laws, standards, technology…**
  - **– and should act in accordance with accepted ethical standards of professional conduct…**
    - **e.g. see:** https://www.ieee.org/about/corporate/governance/p7-8.html
      and: https://www.theiet.org/about/governance/rules-of-conduct/

LVD09 2.0 v3.1

CCC

Directives and other legal regulations, and standards, all specify *minimum* requirements

- Many long-term successful companies aim to go beyond these minimum requirements…
  - because it helps make their products better in ways that their customers appreciate…
  - which means they can charge a price premium, *and* have a lower 'cost of sales', helping them make more profits and being more long-term successful
- This course is about complying with *minimum* safety requirements – you may wish to go further

Cherry Clough Consultants confidential training material

5 of 529

LVD09 2.0 v3.1

CCC

A. Basic Safety Principles

Note

Where an IEC or ISO standard is mentioned in this course, an EN of British Standard equivalent might now be available

Although an EN is usually identical to the IEC or ISO it comes from, sometimes there are differences, so for EU compliance it is best to follow the EN

Note

Safety standards are always being improved, amended and up-issued, so it is very important to apply the latest versions and amendments of the relevant standard(s), rather than rely on the text in this course

Cherry Clough Consultants confidential training material

6 of 529

LVD09 2.0 v3.1

CCC

Contents of the section on Basic Safety Principles

- What do we mean by 'safe'?
- Good practices in safety engineering
- Example of project safety flowchart
- The hierarchy of safety design techniques
- Hazards and risks assessments
- Doing hazard/risk assessments
- Overall safety documentation
- Qualifying and quantifying hazards and risks
- Keeping up to date with safety standards
- National safety laws
- Marketing and Sales and safety
- Making equipment for in-house use
- Competency
- Some examples of useless legal arguments
- It isn't enough to simply apply the more relevant published standard
- HALT and HASS

LVD09 2.0 v3.1

CCC

What do we mean by "Safe" ?

- A HAZARD is anything with potential to do HARM…
  - and we are interested in the severity of that harm
- A harm has a likelihood (probability) of occurrence
- The RISK is the product of the severity of the harm and its probability
- Nothing can ever be 100% safe….
  - whether it was *safe enough* is determined by the courts after a safety incident, using the relevant safety laws

LVD09 2.0 v3.1

CCC

What do we mean by Safe? continued...

- Safe design requires analysis of foreseeable hazards and their risks, to achieve…
  - functionality at a reasonable cost…
  - the degree of safety required
- The degree of safety required depends upon Directives and laws…
  - but also upon the application area…
  - the type and numbers of people exposed…
  - and whether national media involvement is likely

LVD09 2.0 v3.1

CCC

Two types of Safety (1)

1) *(what I am calling)* INHERENT SAFETY…

- i.e. shock, fire, burns, cuts, explosion, toxic fumes, etc…
  - this term is used by the chemical industry, but 'intrinsic' safety is used by the explosive atmospheres industry

- 2) FUNCTIONAL SAFETY…
  - i.e. safety risks caused by operation not as intended…
    - e.g. ABS failing to work; robots moving outside program parameters; process control allowing temperatures or pressures to rise too high; flight control errors, etc., etc…
  - a rapidly increasing problem because electronics is now being used to control *everything*

LVD09 2.0 v3.1

CCC

Two types of Safety (2)

- **Inherent Safety risks are traditionally dealt with by testing alone…**
  - **but Functional Safety risks cannot be proven safe enough by testing…**
  - **because modern digital systems (i.e. microprocessors, FPGAs, ASICs, etc., running software or firmware) have far too many digital states to *ever* test them all, even once!**
  - **and all digital systems are non-linear, so interpolation between measured states is not possible…**
    - **i.e. even if it *was* possible to prove by testing that 99.9% of all digital states were safe *(which it isn't!)* – we still could not assume that the untested 0.1% would also be safe**

LVD09 2.0 v3.1

CCC

Good practices in safety engineering

- **"Hazard identification and risk assessment" is well-known good engineering practice…**
  - **without this, it is difficult for an engineer to justify adding costs to improve safety**
- **Under many safety or liability laws it could prove difficult to make a good legal case for an equipment's safety….**
  - **if a hazard identification and risk assessment had not been done**

LVD09 2.0 v3.1

CCC

Two stages of Risk Assessment — the *Initial* Risk Assessment

- Before anything is designed, an '**Initial Risk Assessment**' is required, …
  - to determine the 'Safety Requirements' that guide the design, realisation, verification, validation, etc. and the rest of the project
- But since the hardware and software have not yet been designed…
  - detailed risk assessments like FMEA, Fault Tree, etc. cannot yet be applied

LVD09 2.0 v3.1

CCC

The Initial Risk Assessment continued…

- All of the hazards that could *possibly* occur, are identified…
  - and graded by severity of the harms they could cause
- The physical, climatic, biological, electromagnetic, user, etc., environments over the lifecycle are determined…
  - then a risk assessment determines the likelihood (i.e. probability) of each hazard occurring during the lifecycle, and these probabilities are then graded
- For <u>each</u> reasonably foreseeable hazard: Severity Grade x Probability Grade = the Risk

LVD09 2.0 v3.1

CCC

The Initial Risk Assessment continued…

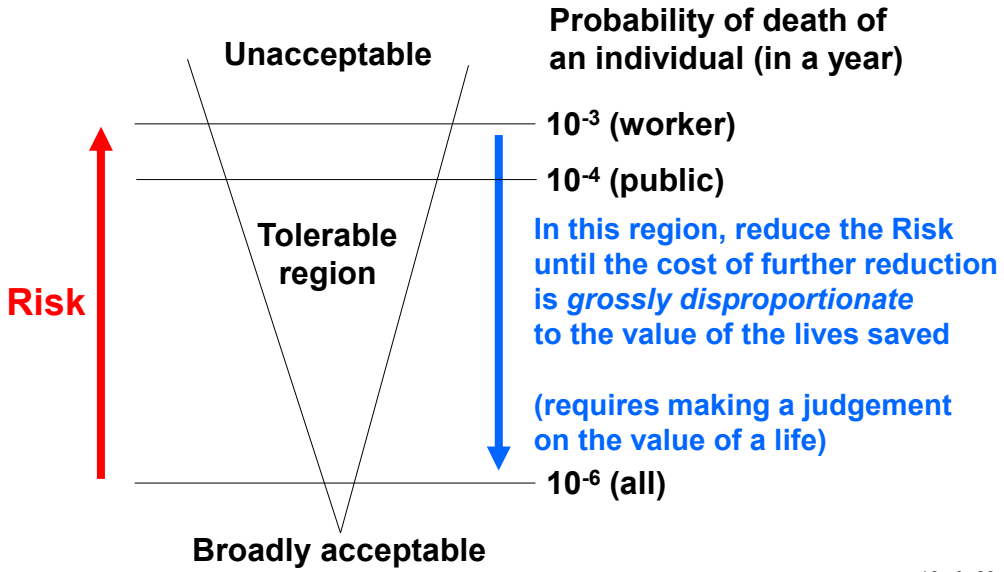
- ***For each hazard:***
  the Risk is compared with what is considered to be acceptable (some people say 'tolerable')…
  - **sometimes there are no fixed Risk levels to comply with, and Risks are required to be ALARP…**
    - **i.e. 'As Low As Reasonably Practical'**
- **Decisions are then made about how much risk reduction to apply, *to each hazard*…**
  - **and the project's 'Safety Requirements Specification' is written on that basis**

LVD09 2.0 v3.1

CCC

Guidance on acceptability of individual risks

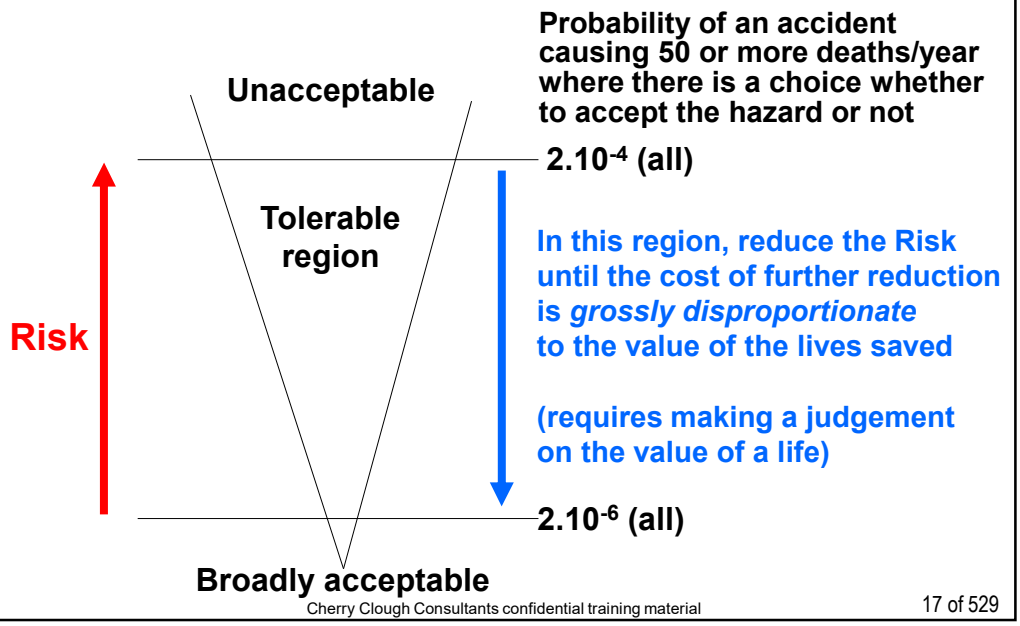
(From the HSE's 2001 publication: "Reducing Risks, Protecting People")



LVD09 2.0 v3.1

Guidance on acceptability of 'societal risks'

(from the HSE's 2001 publication: "Reducing Risks, Protecting People")



LVD09 2.0 v3.1

The Initial Risk Assessment continued…

- The Safety Requirements will eventually be used for the final validation of the project…
  - *after* its design, development and realisation (which includes manufacture, integration, installation, commissioning, etc., as appropriate to the type of project)
- Some of the methods listed at the end of these notes can help create the Initial Risk Assessment