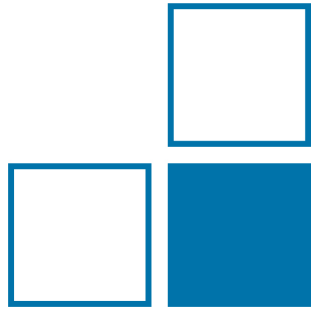
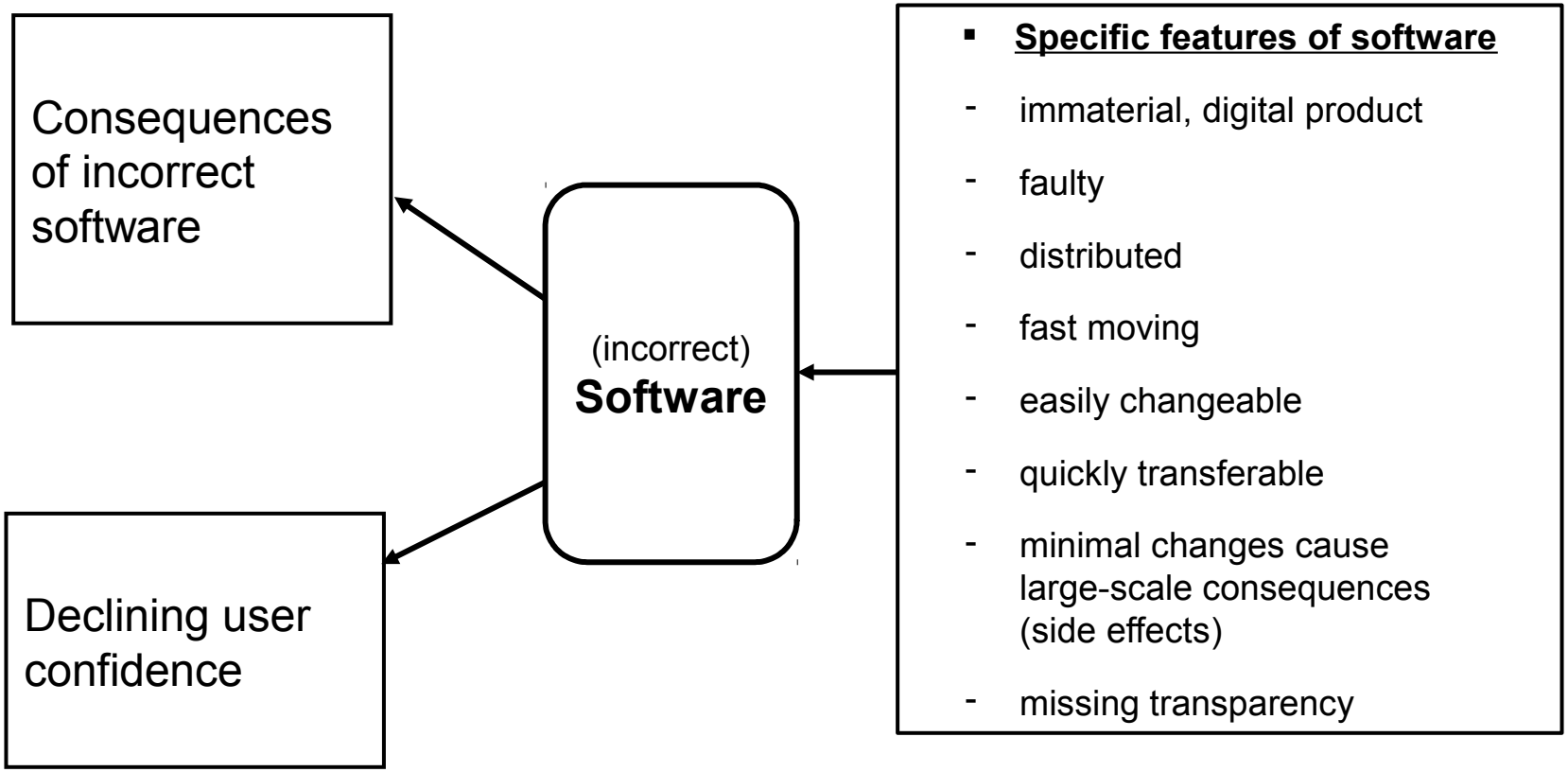
Physikalisch-Technische Bundesanstalt
Braunschweig und Berlin
Nationales Metrologieinstitut

Modularization Methods for Software

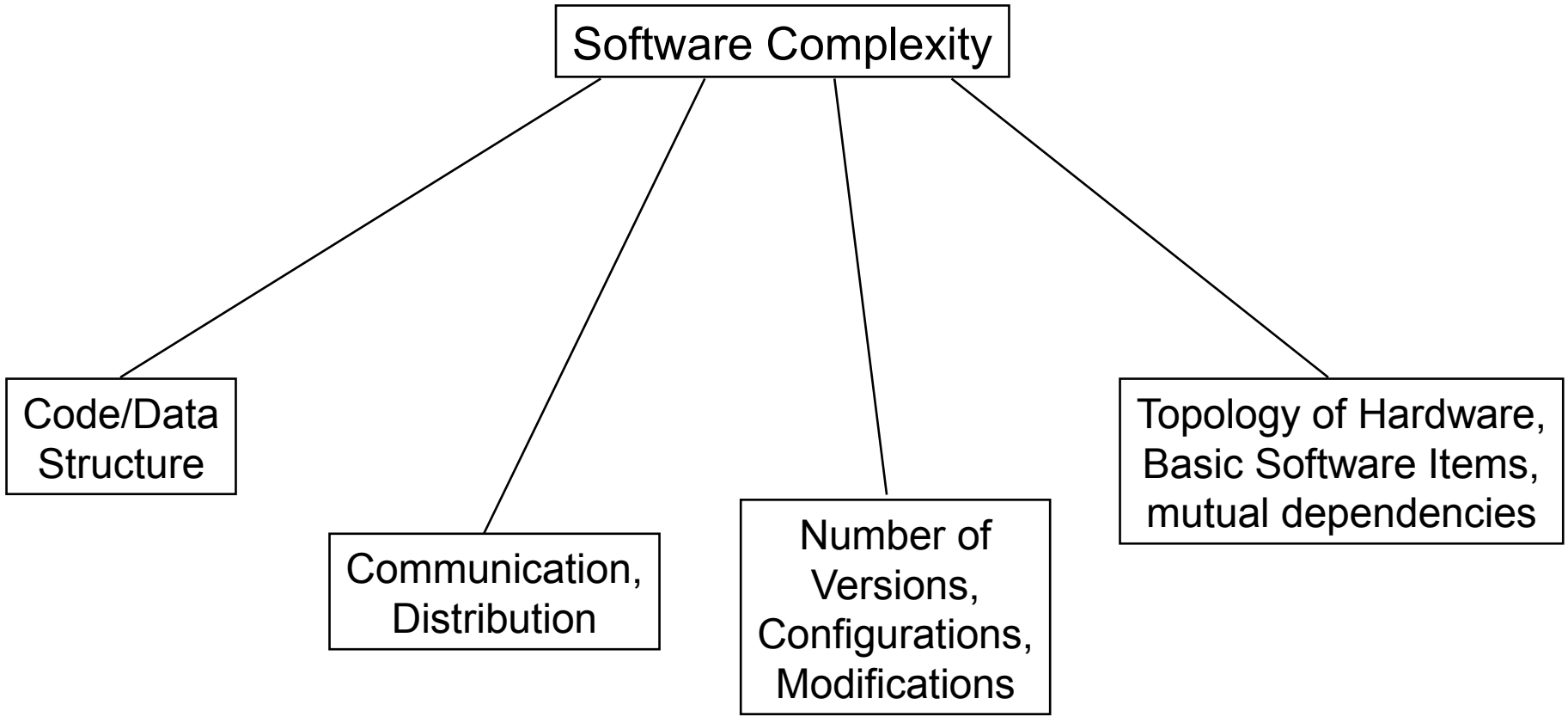
Daniel Peters



Software Quality Problems



Complexity of Embedded Software



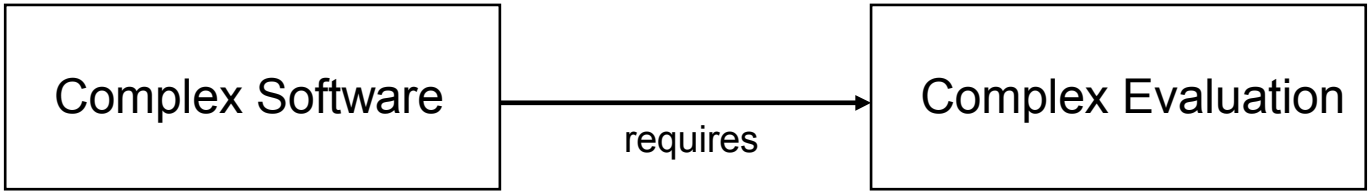
Complexity of Embedded Software

- Increasing complexity of software in embedded systems

BUT

There is no standardised software architecture

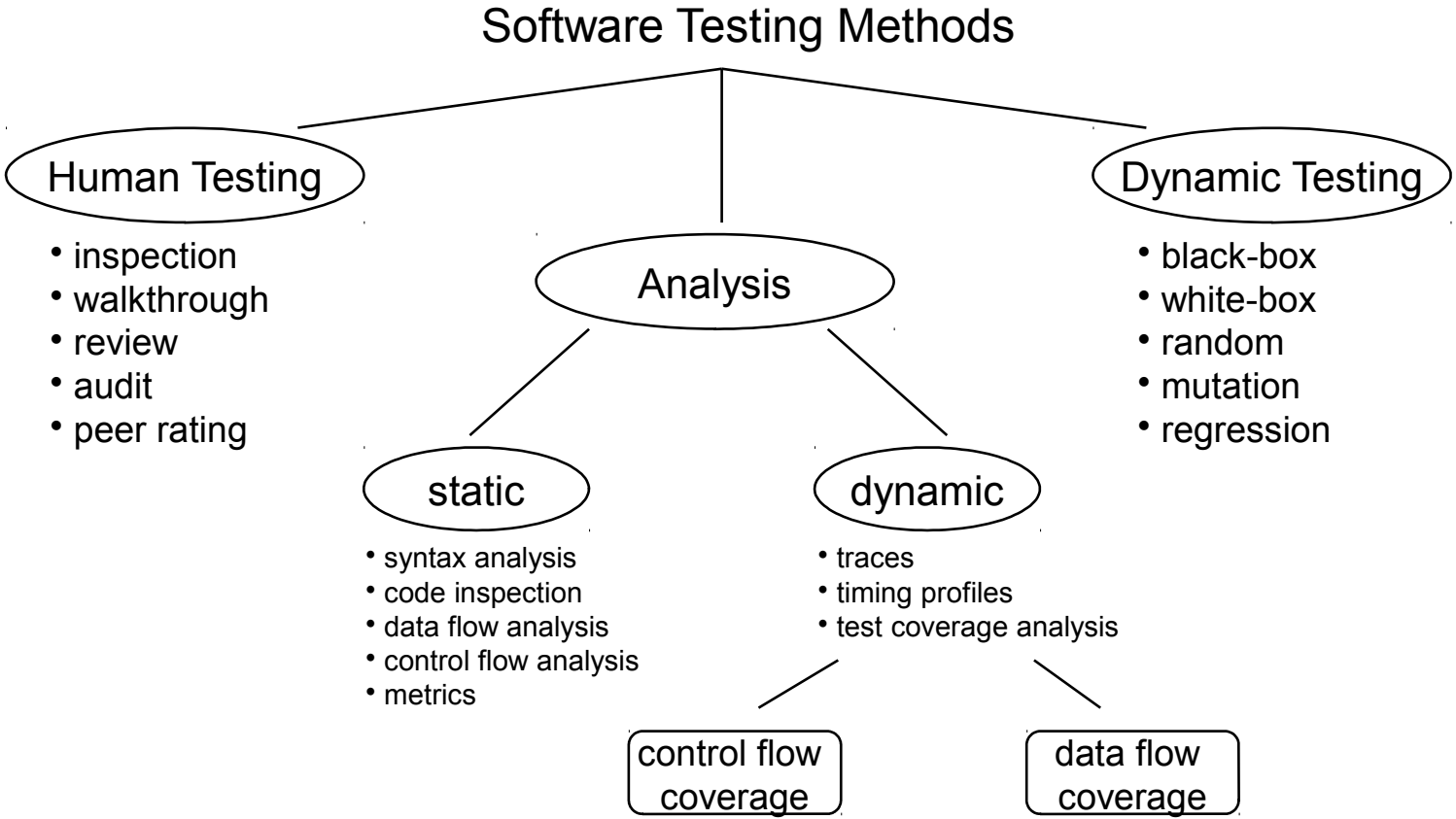
- There are no standardised software development methods
- There are no standardised software assessment methods



Complexity of Embedded Software

Availability	Data and programs must at any time be available to authorised users.
Confidentiality	Information shall be available to authorised users only (access protection).
Integrity	Data and programs must be protected from unintended or unauthorised modifications (including protection from complete loss).
Authenticity	Programs must clearly identify the communication partner (user, process) of protected transaction.

Complexity of Embedded Software



Challenges of GPOS

Verification

Stability

Encapsulation of legally relevant software

Malware

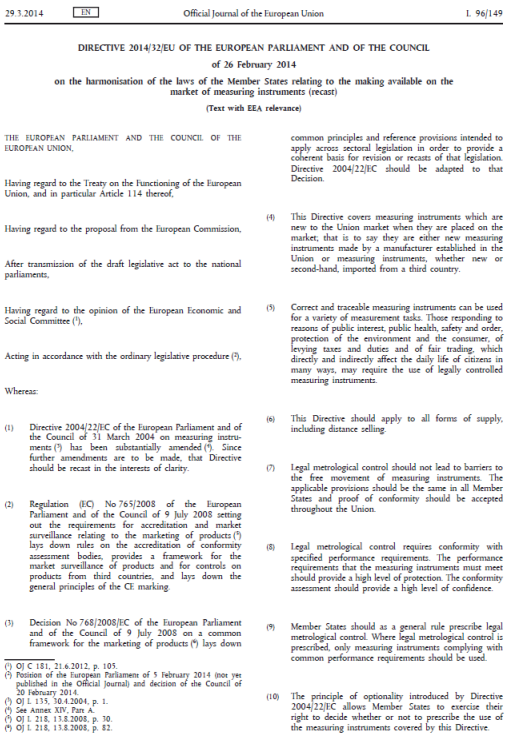
Updates

Real-time

Constructing Secure Systems

- Minimal implementation
- Component architecture
- Least privilege
- Secure development process
- Independent expert validation

MID and WELMEC 7.2



29.3.2014 EN Official Journal of the European Union L 96/149

DIRECTIVE 2014/32/EU OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL
of 26 February 2014
on the harmonisation of the laws of the Member States relating to the making available on the market of measuring instruments (recast)
(Text with EEA relevance)

THE EUROPEAN PARLIAMENT AND THE COUNCIL OF THE EUROPEAN UNION,

Having regard to the Treaty on the Functioning of the European Union, and in particular Article 114 thereof,

Having regard to the proposal from the European Commission,

After transmission of the draft legislative act to the national parliaments,

Having regard to the opinion of the European Economic and Social Committee (1),

Acting in accordance with the ordinary legislative procedure (2),

Whereas:

(1) Directive 2004/22/EC of the European Parliament and of the Council of 31 March 2004 on measuring instruments (3) has been substantially amended (4). Since further amendments are to be made, that Directive should be recast in the interests of clarity.

(2) Regulation (EC) No 765/2008 of the European Parliament and of the Council of 9 July 2008 setting out the requirements for accreditation and market surveillance relating to the marketing of products (5) lays down rules on the accreditation of conformity assessment bodies, provides a framework for the market surveillance of products and for controls on products from third countries, and lays down the general principles of the CE marking.

(3) Decision No 768/2008/EC of the European Parliament and of the Council of 9 July 2008 on a common framework for the marketing of products (6) lays down common principles and reference provisions intended to apply across sectoral legislation in order to provide a coherent basis for revision or recasts of that legislation. Directive 2004/22/EC should be adapted to that Decision.

(4) This Directive covers measuring instruments which are new to the Union market when they are placed on the market, that is to say they are either new measuring instruments made by a manufacturer established in the Union or measuring instruments, whether new or second-hand, imported from a third country.

(5) Correct and traceable measuring instruments can be used for a variety of measurement tasks. Those responding to reasons of public interest, public health, safety and order, protection of the environment and the consumer, of levying taxes and duties and of fair trading, which directly and indirectly affect the daily life of citizens in many ways, may require the use of legally controlled measuring instruments.

(6) This Directive should apply to all forms of supply, including distance selling.

(7) Legal metrological control should not lead to barriers to the free movement of measuring instruments. The applicable provisions should be the same in all Member States and proof of conformity should be accepted throughout the Union.

(8) Legal metrological control requires conformity with specified performance requirements. The performance requirements that the measuring instruments must meet should provide a high level of protection. The conformity assessment should provide a high level of confidence.

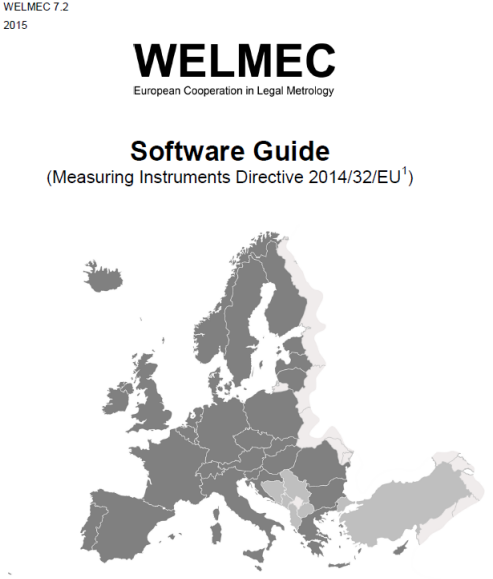
(9) Member States should as a general rule prescribe legal metrological control. Where legal metrological control is prescribed, only measuring instruments complying with common performance requirements should be used.

(10) The principle of optionality introduced by Directive 2004/22/EC allows Member States to exercise their right to decide whether or not to prescribe the use of the measuring instruments covered by this Directive.

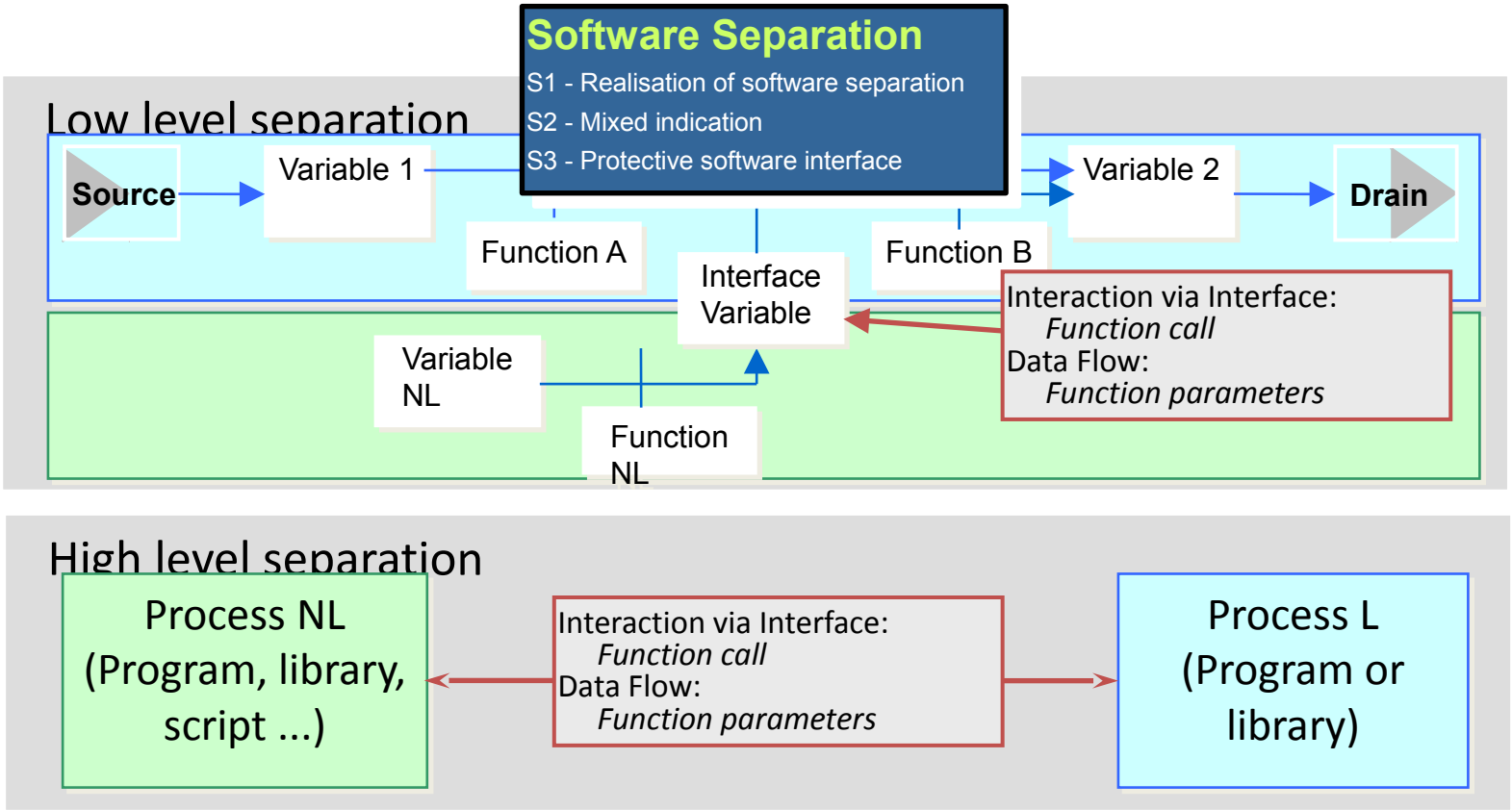
(1) OJ C 181, 21.6.2012, p. 105.
(2) Position of the European Parliament of 5 February 2014 (not yet published in the Official Journal) and decision of the Council of 20 February 2014.
(3) OJ L 135, 30.4.2004, p. 1.
(4) See Annex XIV, Part A.
(5) OJ L 218, 13.8.2008, p. 30.
(6) OJ L 218, 13.8.2008, p. 82.

Essential Requirements

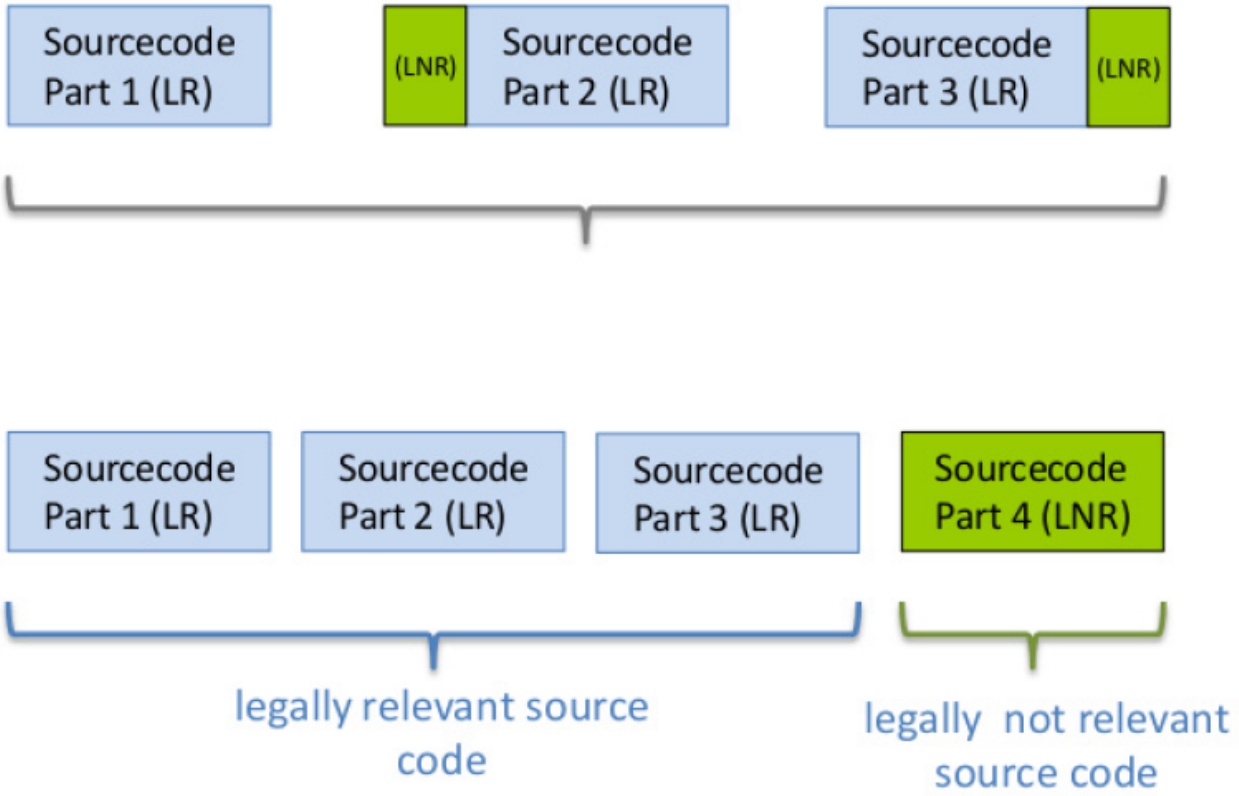
- **Security and software identification** (MID Annex I, 8.3)
- **Data transmission and data storage** (MID Annex I, 8.4)
- **Interfaces** (MID Annex I, 8.1)
- **Software separation** (MID Annex I, 7.6)



WELMEC 7.2 Software Separation



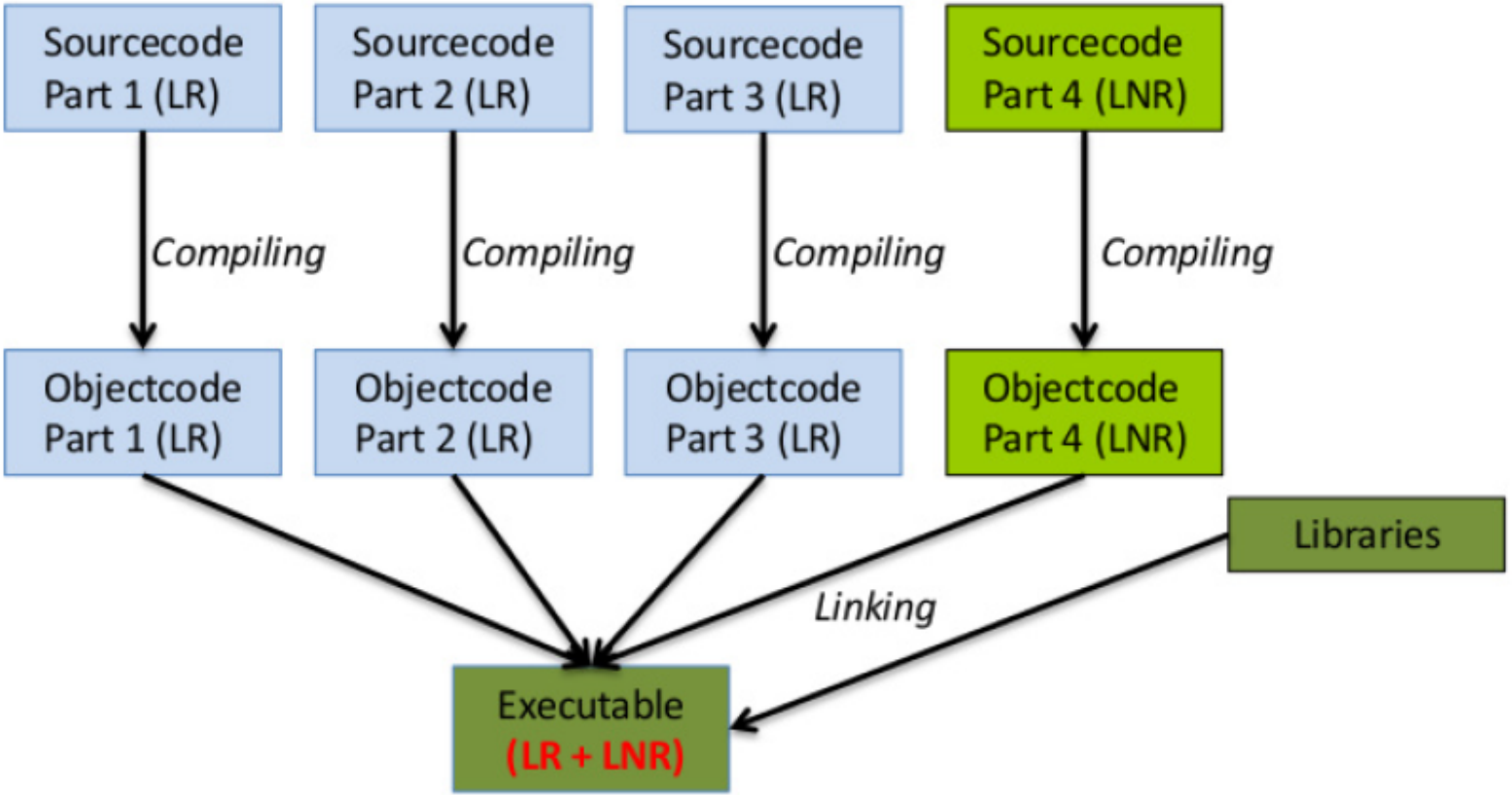
Low-Level Separation



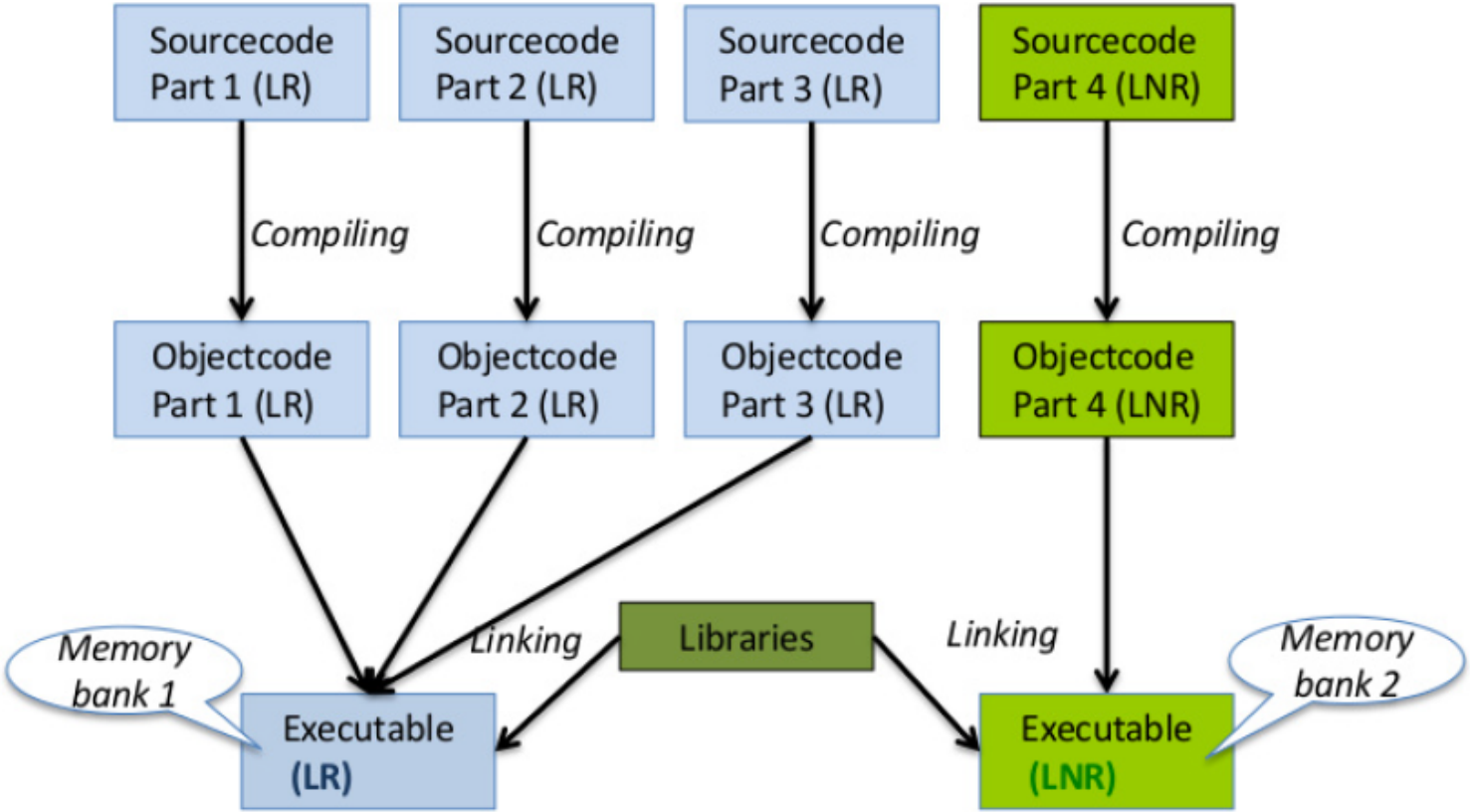
Low-Level Separation

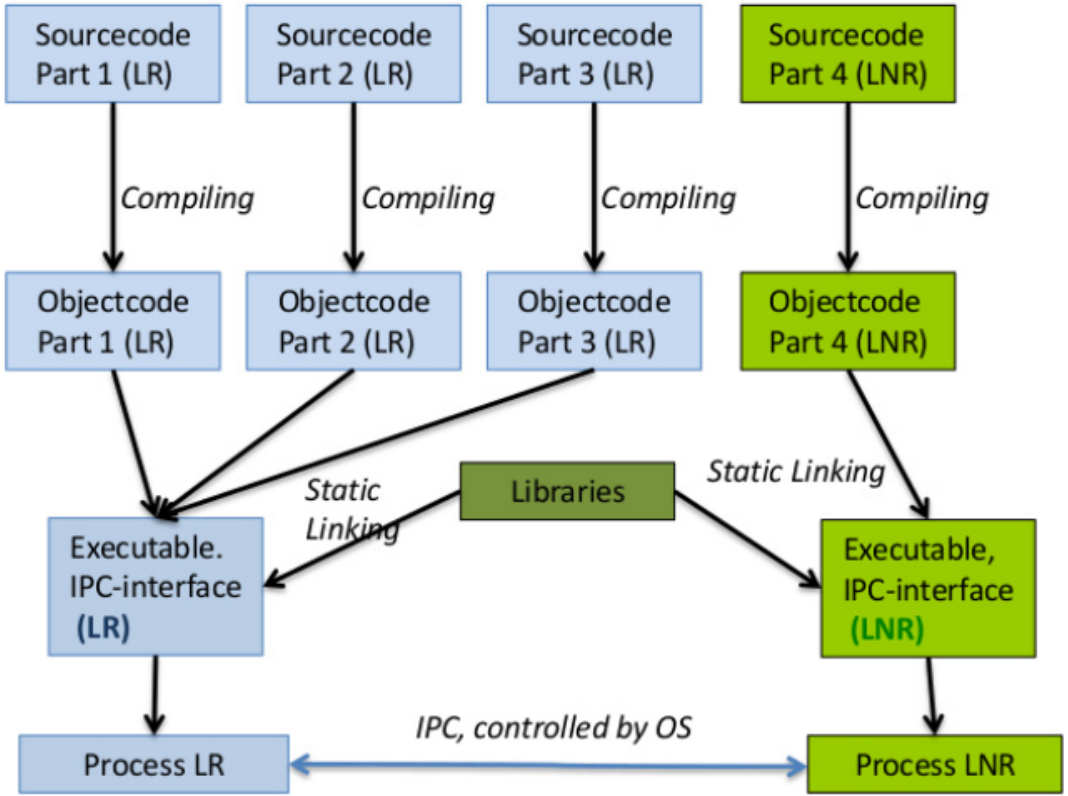
- **Is not enough!**
- **First step to achieve High-Level seperation**
- **Therefore, still a good way to achieve cleaner programming and security**
- **Other examples: Object-oriented, MISRA-C, Hungarian notation**

One executable



Separate executables





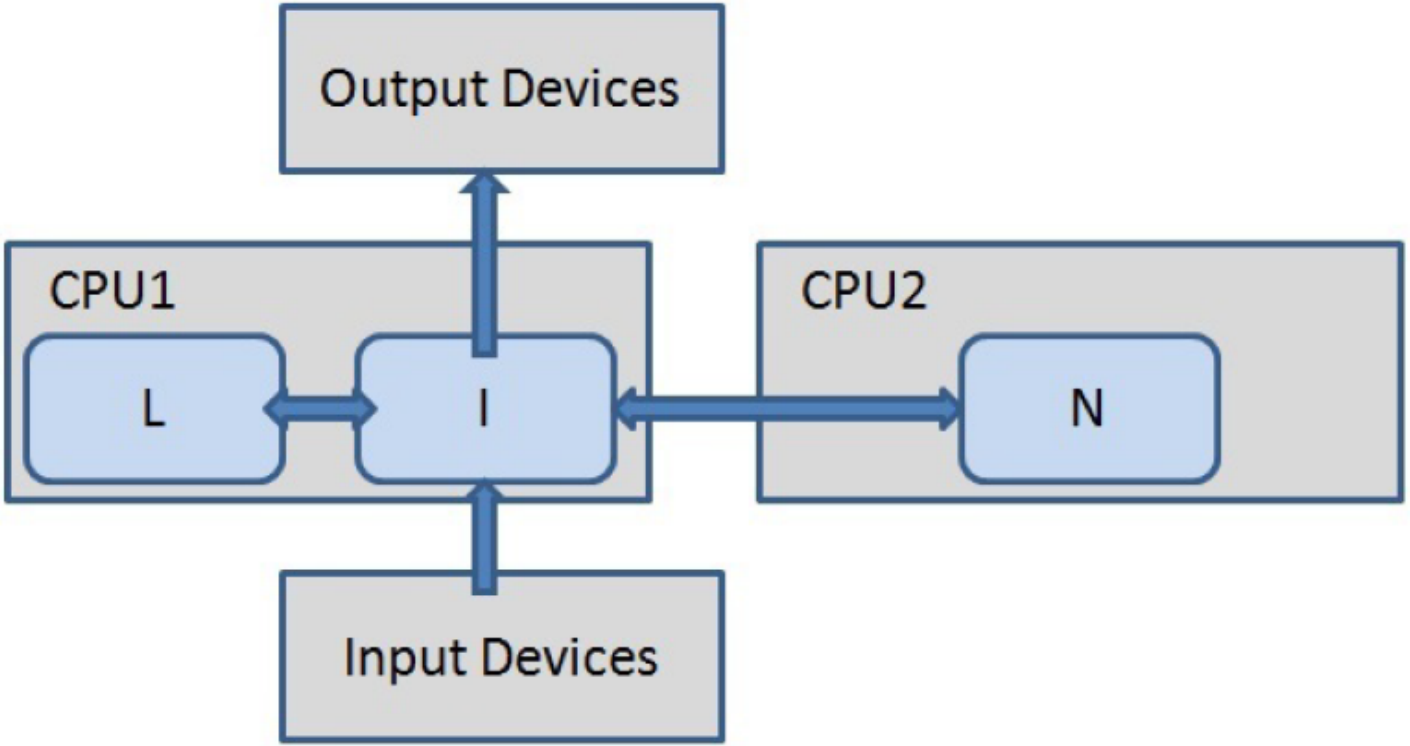
*Daniel Peters and Florian Thiel, Software in Measuring Instruments: Ways of Constructing Secure Systems, AMA, Nürnberg, 2016

Access Control Strategies

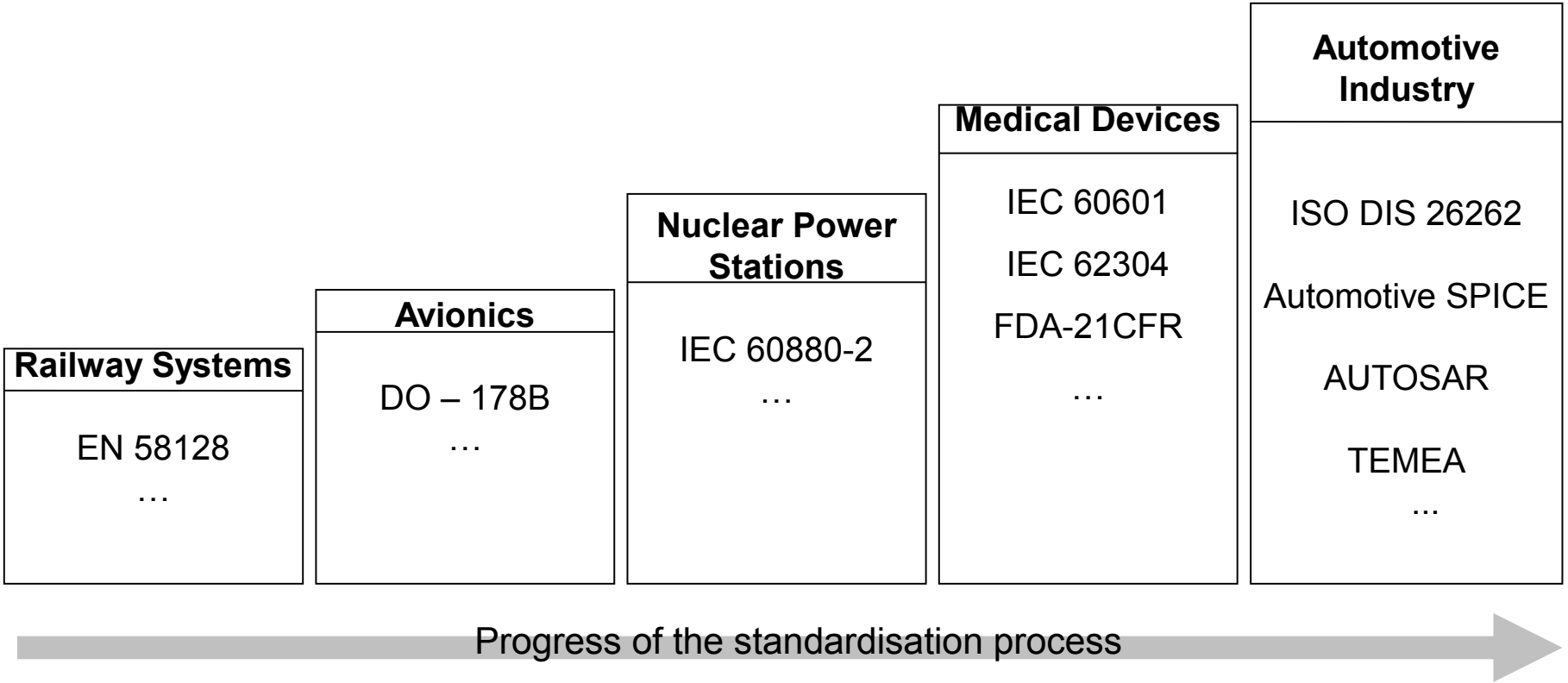
- **Access Control Strategies** determine which **access type** (e.g., read, write, or execute) a **subject** (e.g., user, process, or device) may have to an **object** (e.g., file, table, or subject).
- The **Discretionary Access Control** (DAC) is a strategy in which access rights are defined only by the **identity of a subject**.
- In the **Mandatory Access Control** (MAC) strategy an access decision is additionally determined by means of object properties and rules.

*Patrick Scholz, Daniel Peters and Florian Thiel, Security Concepts for Software in Measuring Instruments, IMEKO Budapest, 2017

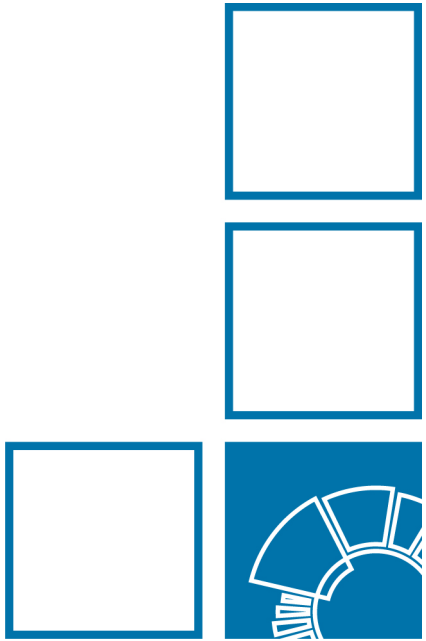
Hardware Separation



Standardisation Process



for software architecture, development and assessment methods



Physikalisch-Technische Bundesanstalt
Braunschweig und Berlin
Abbestraße 2 - 12
10587 Berlin

Daniel Peters
Telefon:030 3481-7916
E-Mail: daniel.peters@ptb.de
www.ptb.de

Stand: 06/17