APEC Asia-Pacific Economic Cooperation · Universiti Kebangsaan Malaysia (National University of Malaysia) · SIRIM · NMIM National Metrology Institute of Malaysia

Daniel Peters

WELMEC 7.2

Software Quality Assurance

APEC Asia-Pacific Economic Cooperation

Capacity Building Workshop On Understanding Conformity Requirements For Software Controlled Weight And Measuring Instruments For Sustainable Trade 2022

APEC

Software Quality Problem

Consequences of incorrect software

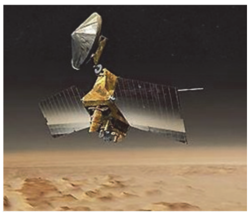
Butler Group (2007): In German industry, incorrect software applications cause a damage of €4.7 billion p.a.

(incorrect) **Software**

Declining user confidence

- Specific features of software
  - immaterial, digital product
  - faulty
  - distributed
  - fast moving
  - easily changeable
  - quickly transferable
  - minimal changes cause large-scale consequences (side effects)
  - missing transparency

Severe software bugs related to measurements



- Complete loss of *Mars Climate Orbiter* at NASA Mission 2000
- Damage: 125 Million US Dollar for Orbiter, …
- Reason: Mix-up between metric und English measures

- Thunderstorm ***„Lothar“:*** More than 60 dead person
- 25.12.99: Forecasting predicted a thunderstorm, error in interpretation: measurement error
- 26.12.99: Weather prediction failed because of ignored outlier data, wind speed 90 km/h instead of 215 km/h

APEC Asia-Pacific Economic Cooperation
Capacity Building Workshop On Understanding Conformity Requirements For Software Controlled Weight And Measuring Instruments For Sustainable Trade 2022
APEC

Reasons for Insufficient Software Quality

- Organisation and management:

  □ Insufficient sensitivity to software problems on behalf of the management,

  □ no support for the software development departments in companies,

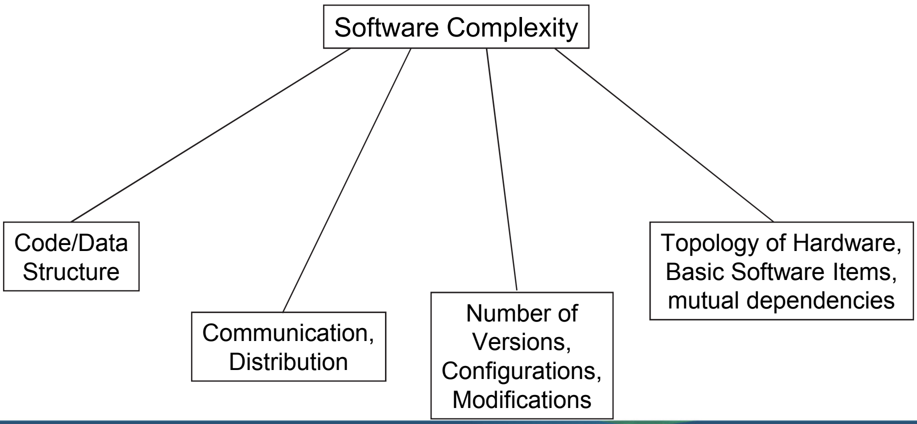
  □ no strategic plans

  □ Process models are not used for the development of a software

APEC Asia-Pacific Economic Cooperation

Capacity Building Workshop On Understanding Conformity Requirements For Software Controlled Weight And Measuring Instruments For Sustainable Trade 2022

Complexity of Embedded Software



APEC Asia-Pacific Economic Cooperation

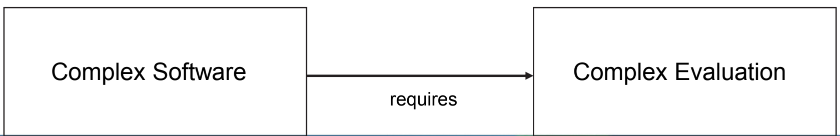
Capacity Building Workshop On Understanding Conformity Requirements For Software Controlled Weight And Measuring Instruments For Sustainable Trade 2022

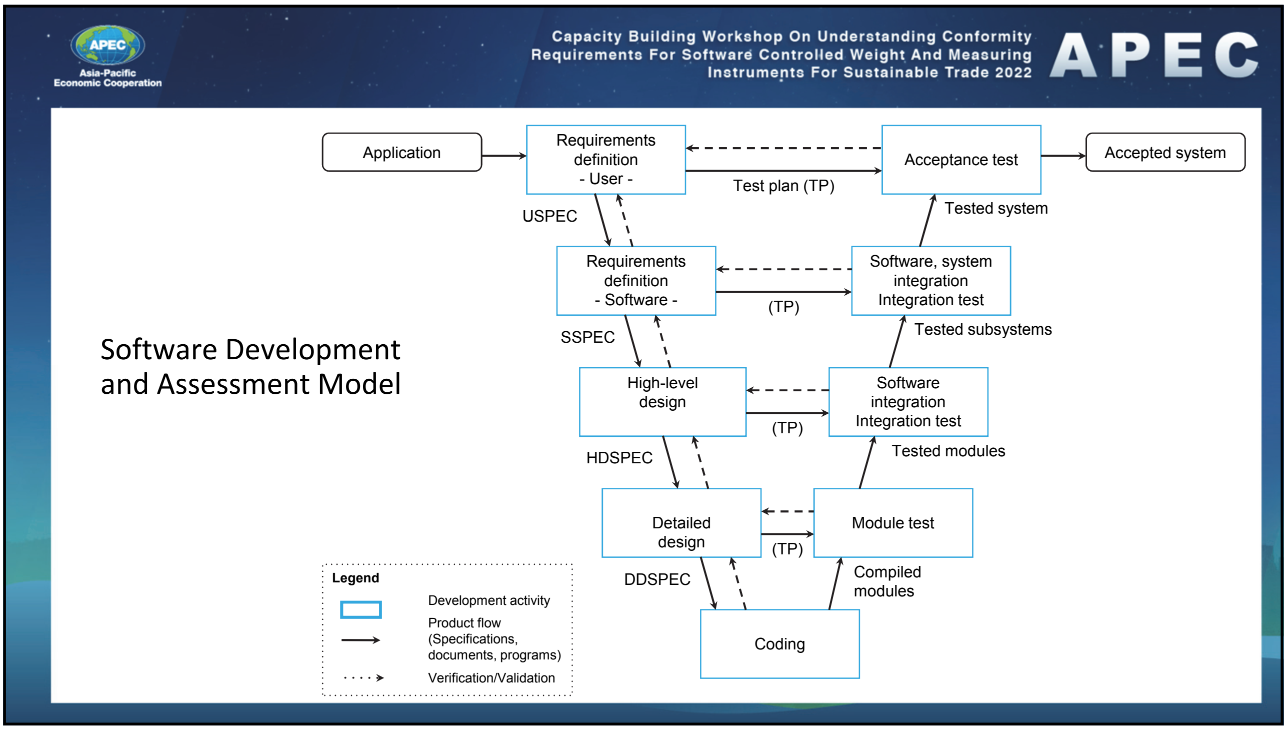
Current situation: Embedded software

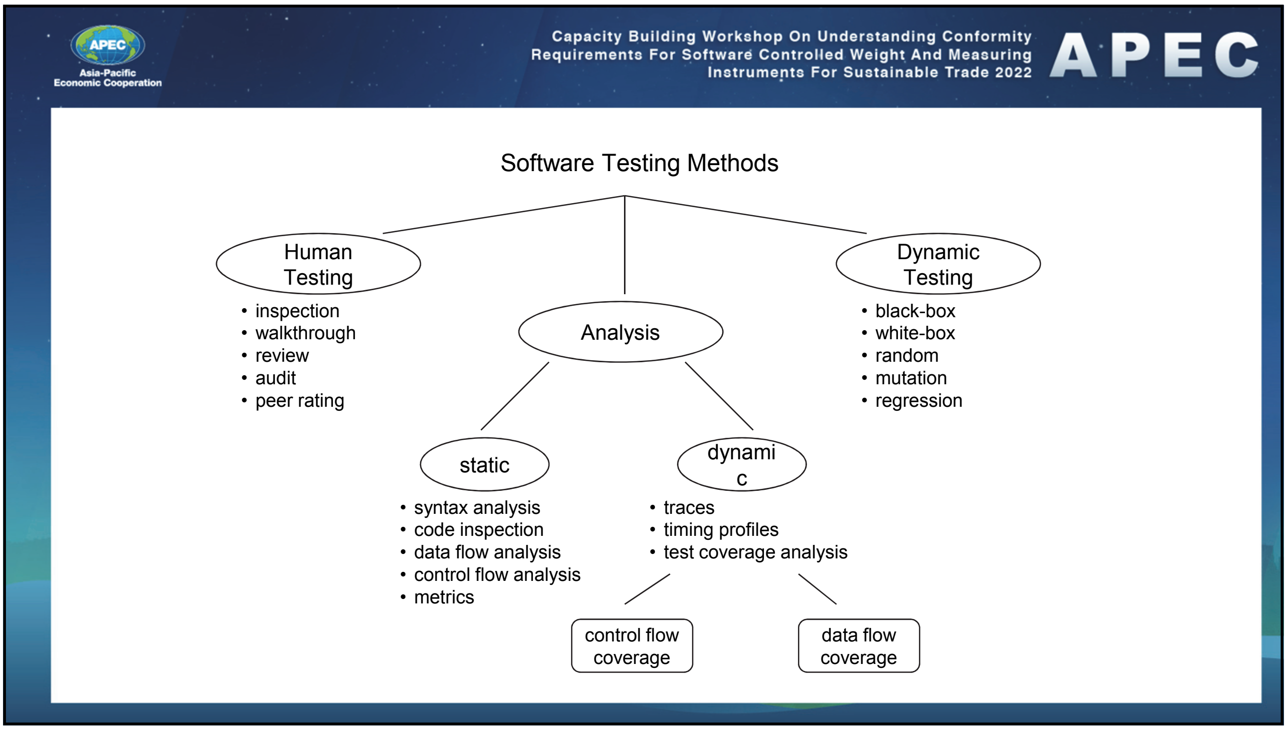
- Increasing complexity of software in embedded systems

BUT

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




APEC
Asia-Pacific Economic Cooperation
Capacity Building Workshop On Understanding Conformity Requirements For Software Controlled Weight And Measuring Instruments For Sustainable Trade 2022
APEC
Software Development and Assessment Model
Application
Requirements definition - User -
Acceptance test
Accepted system
Test plan (TP)
USPEC
Tested system
Requirements definition - Software -
Software, system integration Integration test
(TP)
SSPEC
Tested subsystems
High-level design
Software integration Integration test
(TP)
HDSPEC
Tested modules
Detailed design
Module test
(TP)
DDSPEC
Compiled modules
Coding
Legend
Development activity
Product flow (Specifications, documents, programs)
Verification/Validation


APEC
Asia-Pacific Economic Cooperation
Capacity Building Workshop On Understanding Conformity Requirements For Software Controlled Weight And Measuring Instruments For Sustainable Trade 2022
APEC
Software Testing Methods
Human Testing
• inspection
• walkthrough
• review
• audit
• peer rating
Analysis
Dynamic Testing
• black-box
• white-box
• random
• mutation
• regression
static
• syntax analysis
• code inspection
• data flow analysis
• control flow analysis
• metrics
dynami c
• traces
• timing profiles
• test coverage analysis
control flow coverage
data flow coverage

Capacity Building Workshop On Understanding Conformity Requirements For Software Controlled Weight And Measuring Instruments For Sustainable Trade 2022

Software Quality Assurance

Analytical Measures	Preventive Measures
Testing methods, techniques and tools to detect failures/defects, to evaluate software products and processes	Constructive methods, techniques and tools to avoid failures/defects in software development processes
• Dynamic testing • Static analysis • Inspections • Reviews • Usability testing • Performance testing • Auditing of processes	• Establishing compliance with standards and guidelines (evidence of conformity) • Systematic application of software life-cycle models/best practices • Testing/documenting at an early stage • Elaboration of harmonised documents

Capacity Building Workshop On Understanding Conformity Requirements For Software Controlled Weight And Measuring Instruments For Sustainable Trade 2022

Simple Methods of Software Validation

- Simple (informal) reviews of documents
- Manual conformity tests regarding guidelines, definitions, naming conventions, style guides, etc.
- Meetings/discussions with the software developer
- Systematic assessments of factors influencing the software results
- Comparison of software results with results achieved with other (software) methods
- Attestation of long-term correct operation
- Acceptance of certificates, test reports, process audit reports, self-declarations, etc.

Quality Characteristic: Security

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.

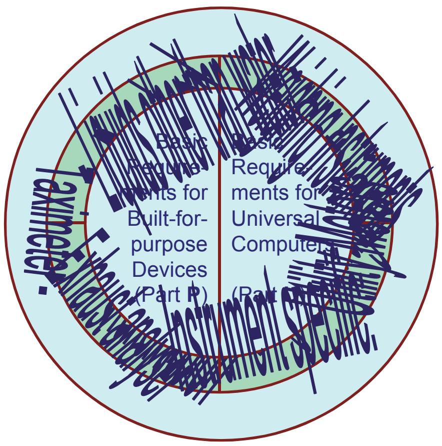
Capacity Building Workshop On Understanding Conformity Requirements For Software Controlled Weight And Measuring Instruments For Sustainable Trade 2022
APEC

Welmec 7.2 Software Guide

- Structure of the Guide

A
B
C
D
E
F

Risk Classes



Requirements Part P

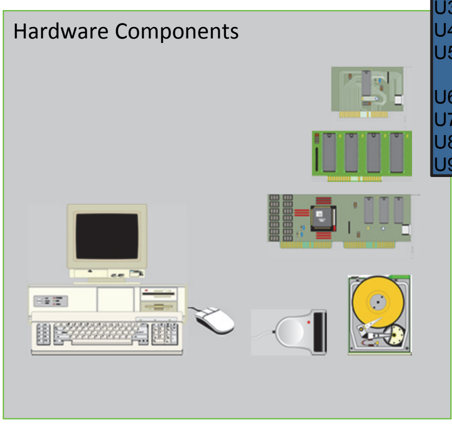
Built-for-Purpose Computer
P1 - Documentation
P2 - Software identification
P3 - Influence via user interfaces
P4 - Influence via communication interface
P5 - Protection against accidental or unintentional changes
P6 - Program protection against intentional changes
P7 - Parameter protection

- Devices designed for the measuring purpose
- IT components only realise functions for measuring, indication and supporting tasks
- No option of loading software, programming or starting of other software when instrument is in use

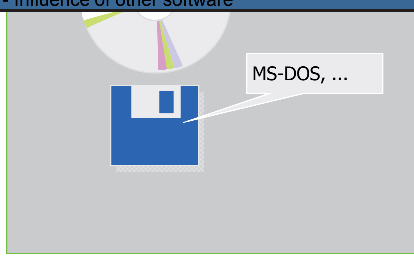
Capacity Building Workshop On Understanding Conformity Requirements For Software Controlled Weight And Measuring Instruments For Sustainable Trade 2022
APEC

Requirements Part U

Universal Computer



Universal Computer
U1 - Documentation
U2 - Software identification
U3 - Influence via user interfaces
U4 - Influence via Electronic interface
U5 - Protection against accidental or unintentional changes
U6 - Protection against intentional changes
U7 - Parameter protection
U8 - Software authenticity and presentation of results
U9 - Influence of other software



APEC Asia-Pacific Economic Cooperation
Capacity Building Workshop On Understanding Conformity Requirements For Software Controlled Weight And Measuring Instruments For Sustainable Trade 2022
APEC

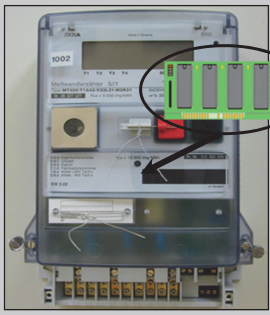
Requirements, Extension L

Long-term storages

Long-term Storage

- L1 - Completeness of stored data
- L2 - Protection against accidental or unintentional changes
- L3 - Integrity of data
- L4 - Authenticity of stored data
- L5 - Confidentiality of keys
- L6 - Retrieval of stored data
- L7 - Automatic storing
- L8 - Storage capacity and continuity

Integrated storage



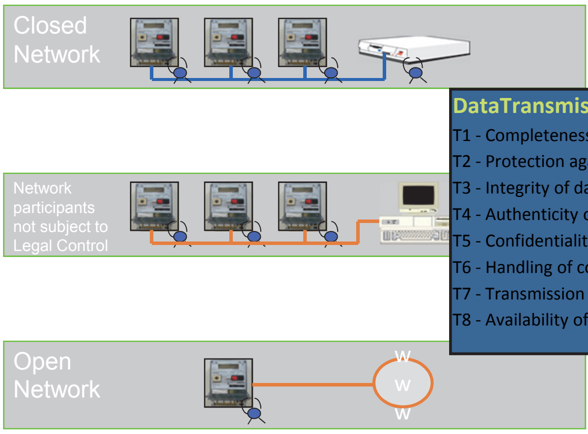
Storages in universal computers

Removable or remote storage

APEC Asia-Pacific Economic Cooperation
Capacity Building Workshop On Understanding Conformity Requirements For Software Controlled Weight And Measuring Instruments For Sustainable Trade 2022
APEC

Requirements, Extension T

Data transmission

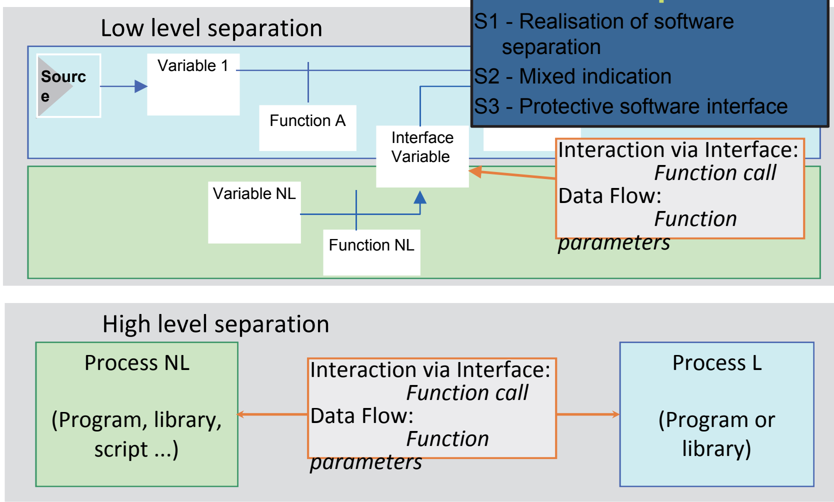


DataTransmission

- T1 - Completeness of transmitted data
- T2 - Protection against accidental or unintentional changes
- T3 - Integrity of data
- T4 - Authenticity of transmitted data
- T5 - Confidentiality of keys
- T6 - Handling of corrupted data
- T7 - Transmission delay
- T8 - Availability of transmission services

Requirements, Extension S

Software separation

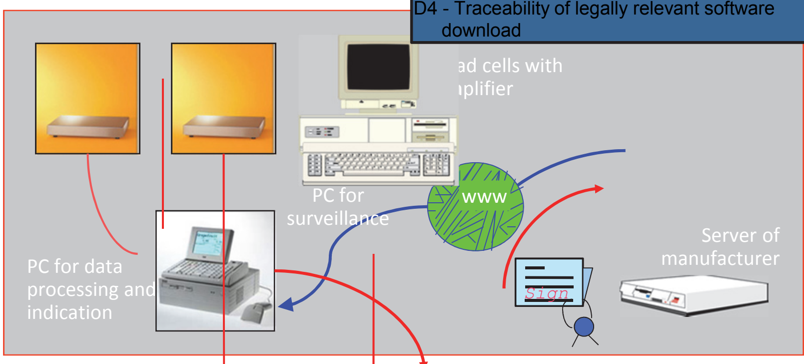


Software Separation
- S1 - Realisation of software separation
- S2 - Mixed indication
- S3 - Protective software interface

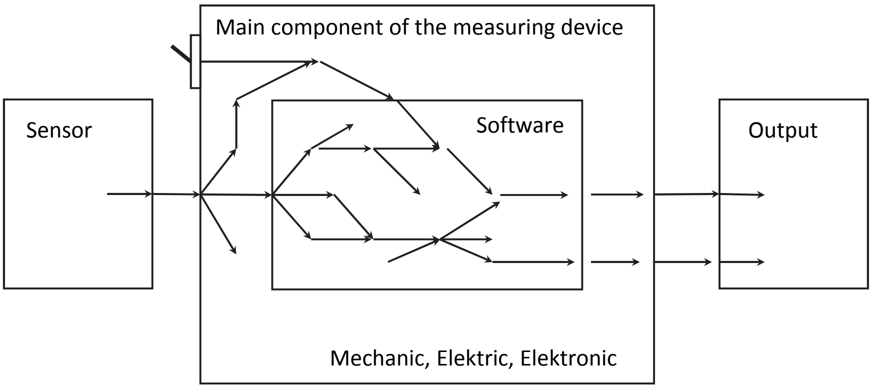
Requirements, Extension D

Measuring system with download via op

Download
- D1 - Download mechanism
- D2 - Authentication of downloaded software
- D3 - Integrity of downloaded software
- D4 - Traceability of legally relevant software download



Capacity Building Workshop On Understanding Conformity Requirements For Software Controlled Weight And Measuring Instruments For Sustainable Trade 2022



Dataflow analysis is the analysis of the transport of values and the usage of variables.

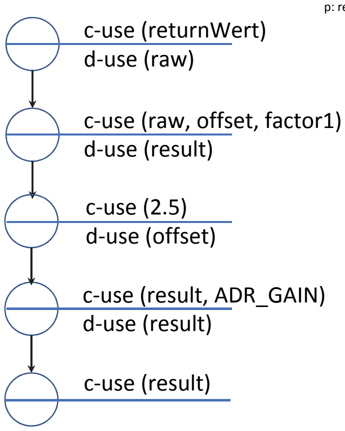
Capacity Building Workshop On Understanding Conformity Requirements For Software Controlled Weight And Measuring Instruments For Sustainable Trade 2022

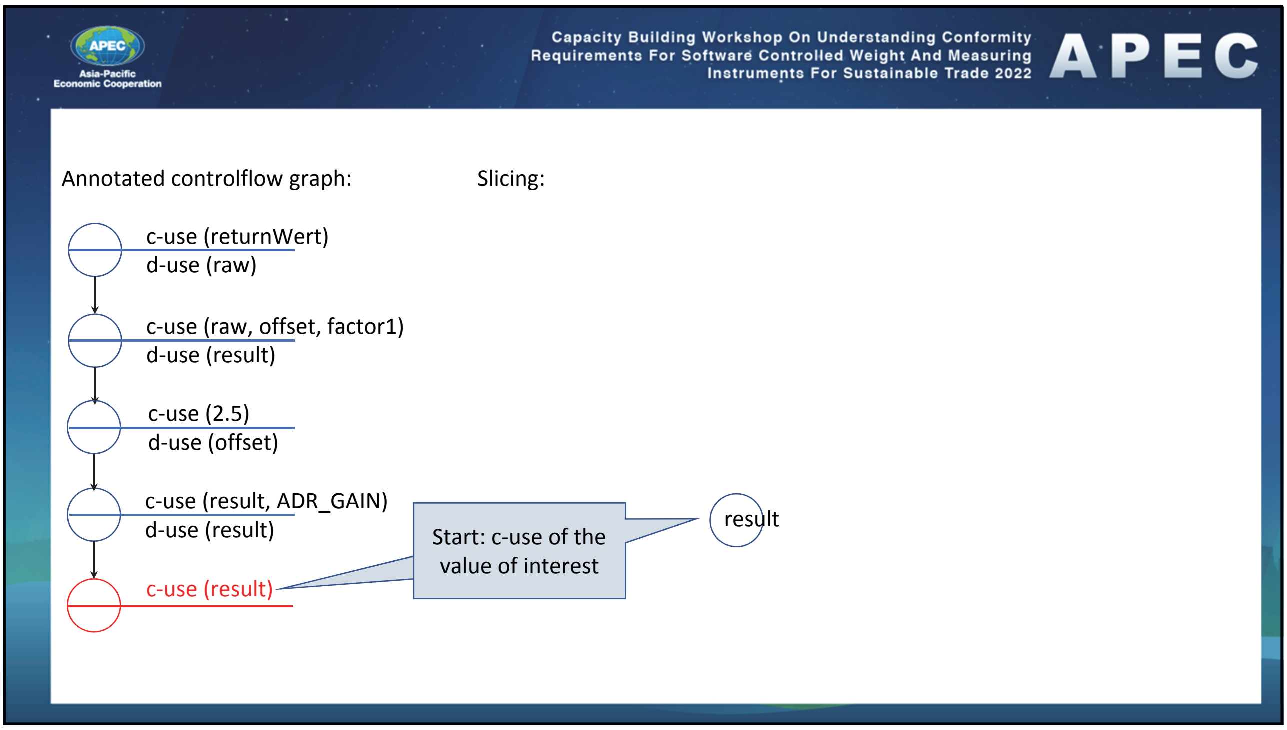
Code:

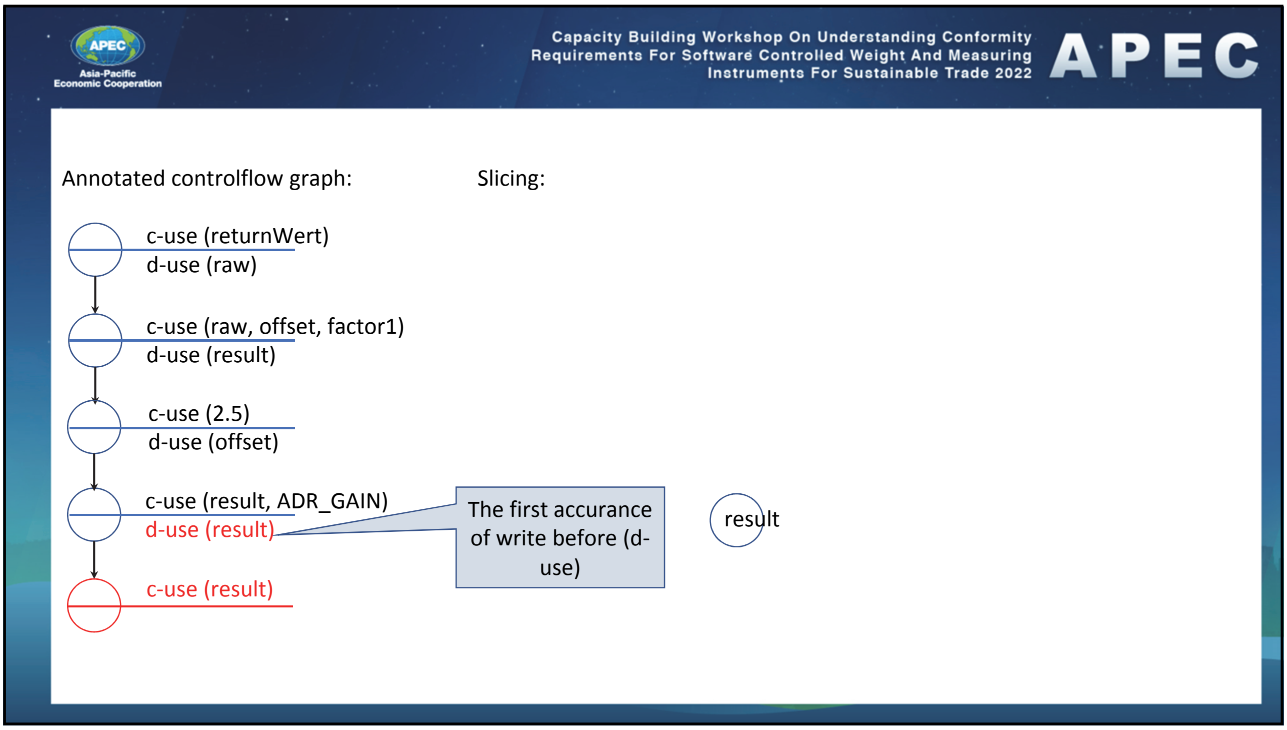
```
...
raw = curr_sensor_value();

result = (raw – offset) * factor1;

offset = 2.5;

result = result * ADR_GAIN;

print (result);
...
```

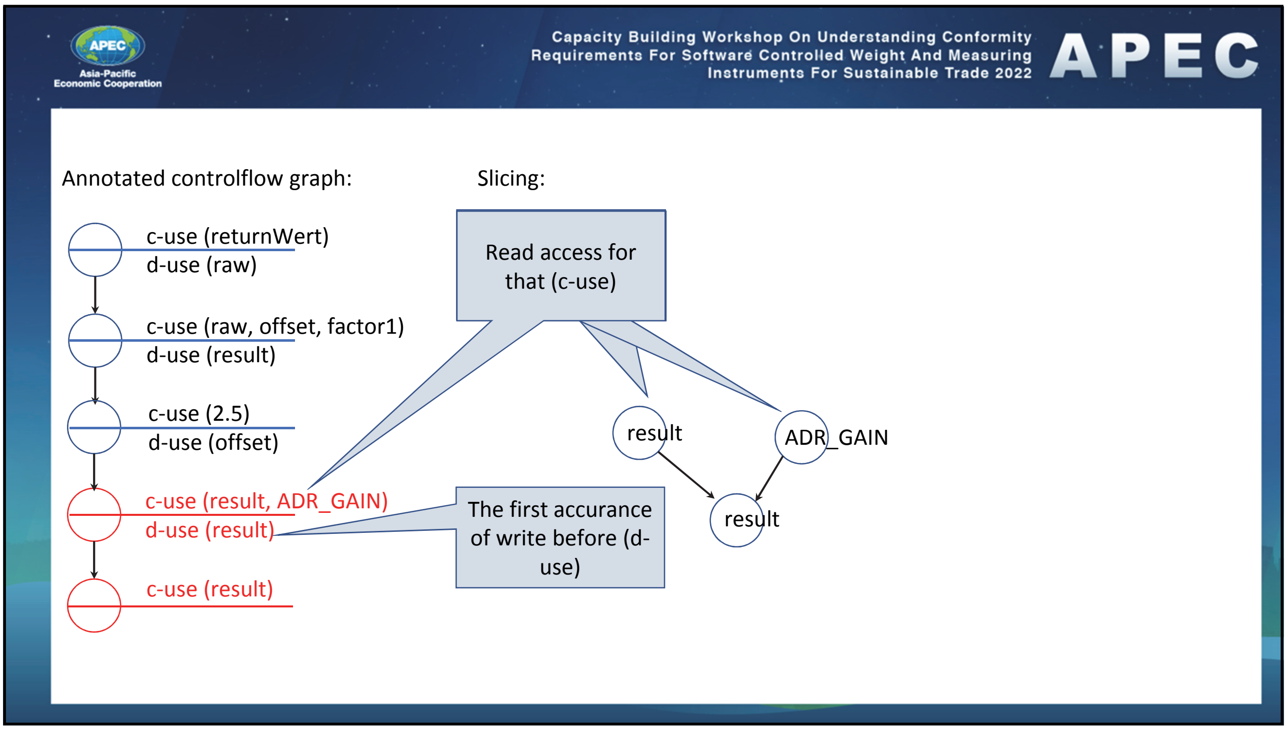
Annotated controlflow graph:

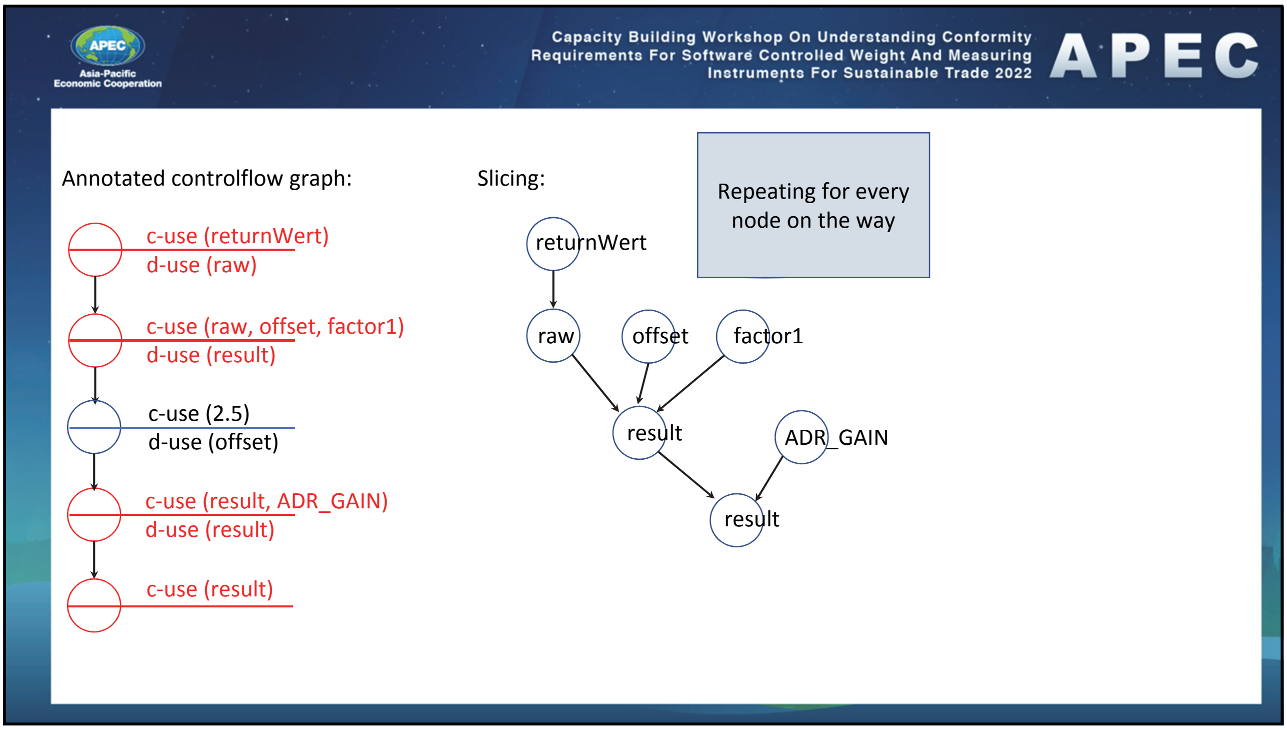
d: write acces (definition)
c: simple read access (c-use)
p: read access with decision (p-use)




APEC
Asia-Pacific Economic Cooperation
Capacity Building Workshop On Understanding Conformity Requirements For Software Controlled Weight And Measuring Instruments For Sustainable Trade 2022
APEC
Annotated controlflow graph:
Slicing:
c-use (returnWert)
d-use (raw)
c-use (raw, offset, factor1)
d-use (result)
c-use (2.5)
d-use (offset)
c-use (result, ADR_GAIN)
d-use (result)
c-use (result)
Start: c-use of the value of interest
result

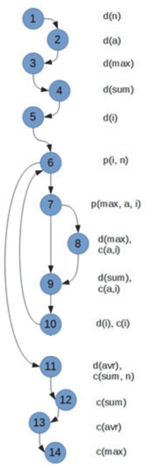

APEC
Asia-Pacific Economic Cooperation
Capacity Building Workshop On Understanding Conformity Requirements For Software Controlled Weight And Measuring Instruments For Sustainable Trade 2022
APEC
Annotated controlflow graph:
Slicing:
c-use (returnWert)
d-use (raw)
c-use (raw, offset, factor1)
d-use (result)
c-use (2.5)
d-use (offset)
c-use (result, ADR_GAIN)
d-use (result)
c-use (result)
The first accurance of write before (d-use)
result


Capacity Building Workshop On Understanding Conformity Requirements For Software Controlled Weight And Measuring Instruments For Sustainable Trade 2022
APEC
Annotated controlflow graph:
c-use (returnWert)
d-use (raw)
c-use (raw, offset, factor1)
d-use (result)
c-use (2.5)
d-use (offset)
c-use (result, ADR_GAIN)
d-use (result)
c-use (result)
Slicing:
Read access for that (c-use)
result
ADR_GAIN
result
The first accurance of write before (d-use)


Capacity Building Workshop On Understanding Conformity Requirements For Software Controlled Weight And Measuring Instruments For Sustainable Trade 2022
APEC
Annotated controlflow graph:
c-use (returnWert)
d-use (raw)
c-use (raw, offset, factor1)
d-use (result)
c-use (2.5)
d-use (offset)
c-use (result, ADR_GAIN)
d-use (result)
c-use (result)
Slicing:
Repeating for every node on the way
returnWert
raw
offset
factor1
result
ADR_GAIN
result

Annotierter Kontrollflussgraph

```
1: input (n);
2: input (a);
3: max:=0;
4: sum:=0;
5: i:=2;
6: while (i<=n) {
7:     if (max<a[i]) {
8:         max:=a[i];}
9:     sum:=sum+a[i];
10:    i++;}
11: avr:=sum/n;
12: output(sum);
13: output(avr);
14: output(max);
```

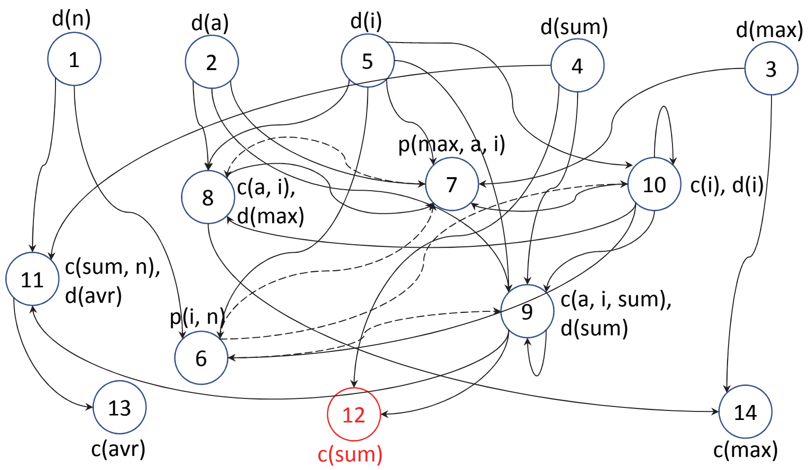


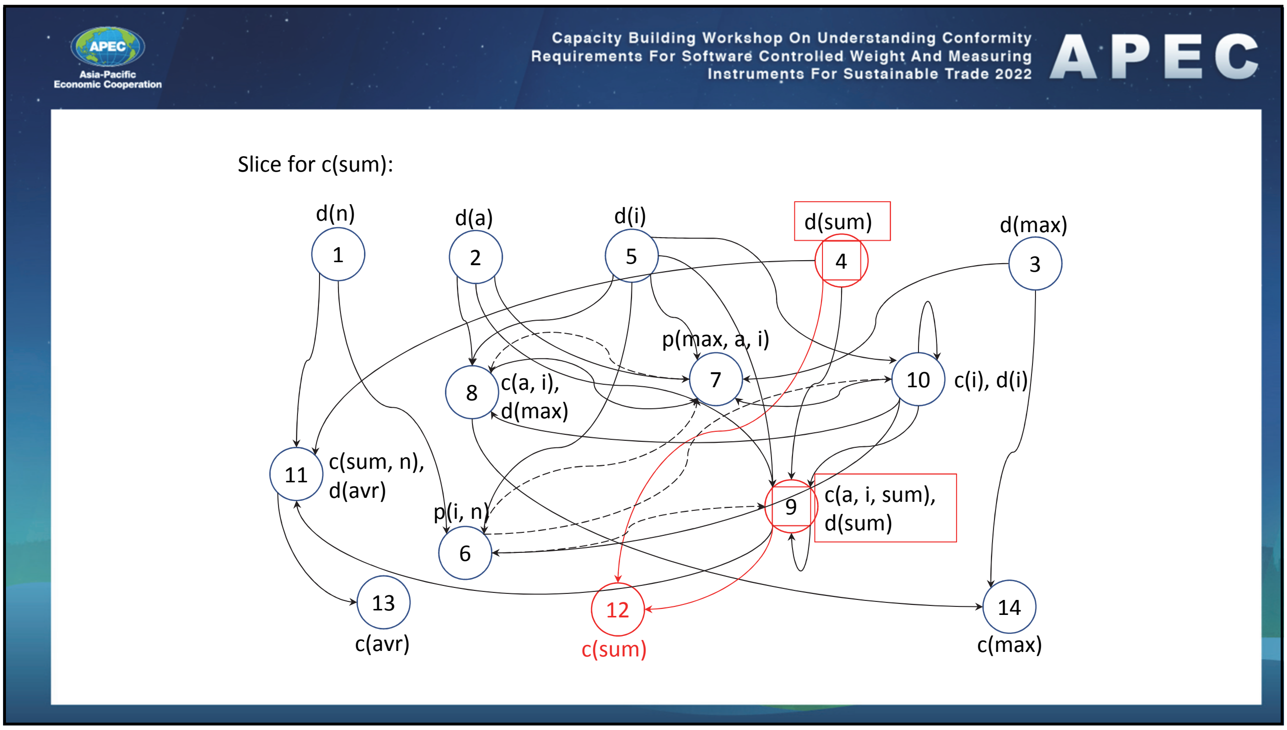
d: write acces (definition)
c: simple read access (c-use)
p: read access with decision (p-use)

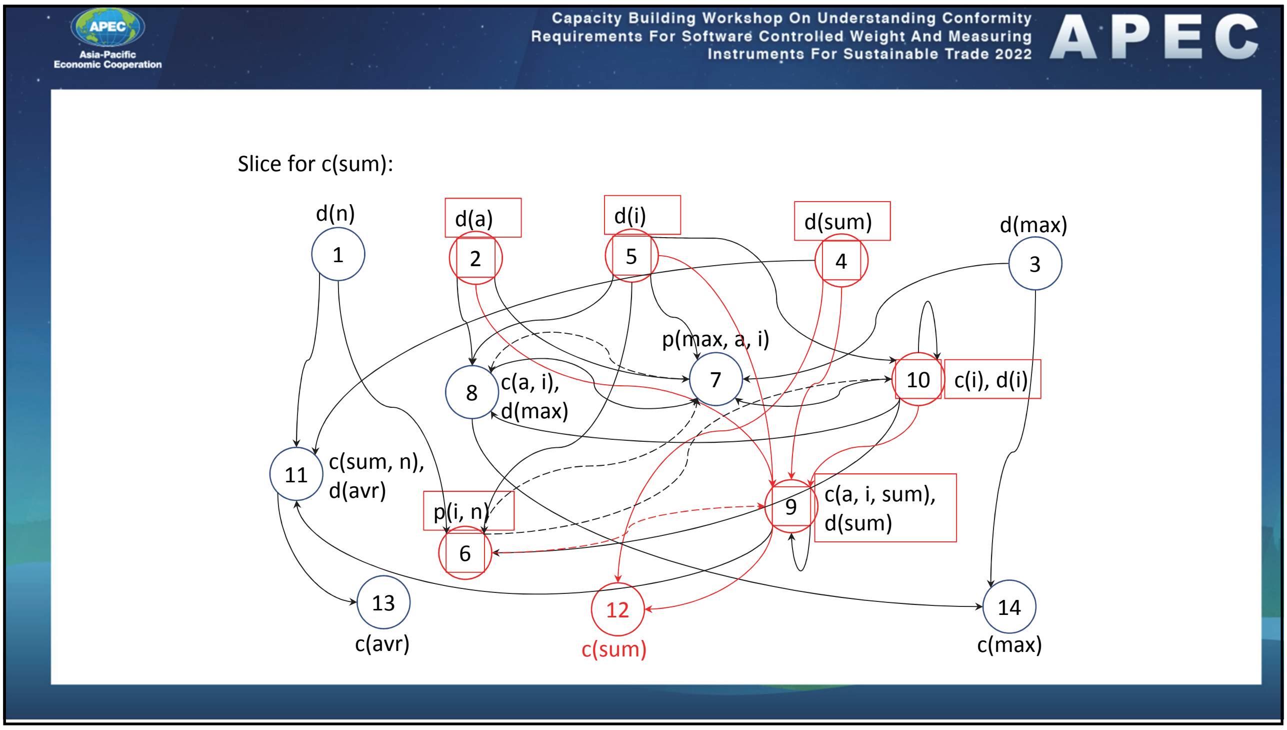
s. Liggesmeyer: „Softwarequalität“, Spektrum-Verlag, S.266ff.

Capacity Building Workshop On Understanding Conformity Requirements For Software Controlled Weight And Measuring Instruments For Sustainable Trade 2022
APEC
Asia-Pacific Economic Cooperation

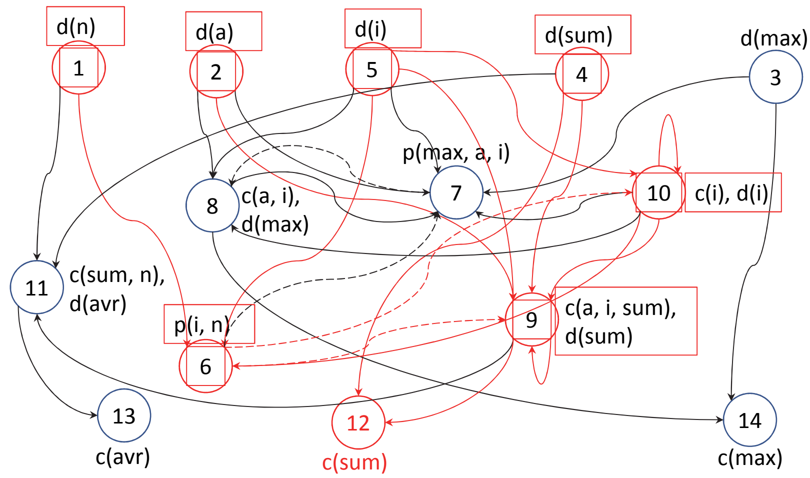
Slice for c(sum):



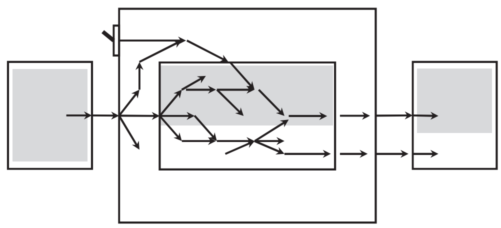

APEC
Asia-Pacific Economic Cooperation
Capacity Building Workshop On Understanding Conformity Requirements For Software Controlled Weight And Measuring Instruments For Sustainable Trade 2022
APEC
Slice for c(sum):
d(n)
1
d(a)
2
d(i)
5
d(sum)
4
d(max)
3
p(max, a, i)
7
8
c(a, i), d(max)
10
c(i), d(i)
11
c(sum, n), d(avr)
p(i, n)
6
9
c(a, i, sum), d(sum)
13
c(avr)
12
c(sum)
14
c(max)


APEC
Asia-Pacific Economic Cooperation
Capacity Building Workshop On Understanding Conformity Requirements For Software Controlled Weight And Measuring Instruments For Sustainable Trade 2022
APEC
Slice for c(sum):
d(n)
1
d(a)
2
d(i)
5
d(sum)
4
d(max)
3
p(max, a, i)
7
8
c(a, i), d(max)
10
c(i), d(i)
11
c(sum, n), d(avr)
p(i, n)
6
9
c(a, i, sum), d(sum)
13
c(avr)
12
c(sum)
14
c(max)

Slice for c(sum):



Asia-Pacific Economic Cooperation
Capacity Building Workshop On Understanding Conformity Requirements For Software Controlled Weight And Measuring Instruments For Sustainable Trade 2022
APEC



Is some part of the software non-legally relevant?:

Manufacturer says the gray part is not influencing measuring results. Really?

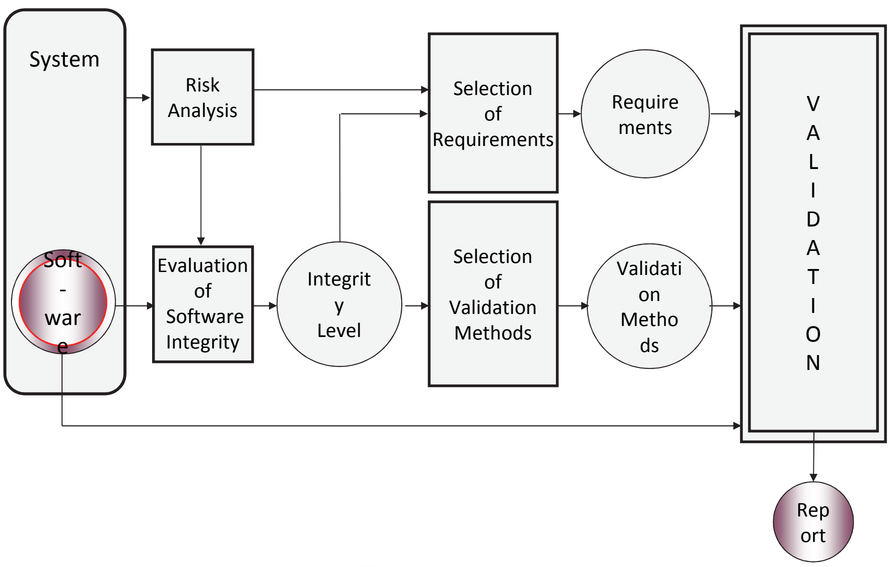
Slicing through the code from input to output, result it influences the output!

Enhancements to WELMEC 7.2

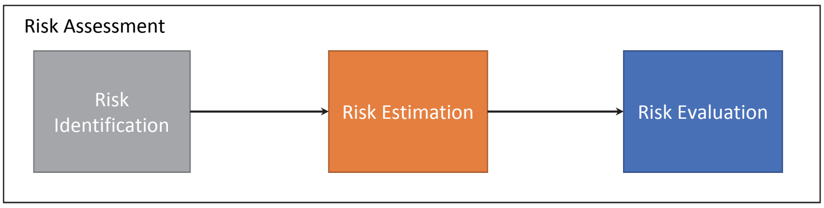
- WELMEC 7.3 Reference Architectures (2020)
- WELMEC 7.4 Exemplary Applications (2020)
- WELMEC 7.5 NAWIs (former WELMEC 2.3)
- **WELMEC 7.6 Risk Assessment (2021)**

APEC Asia-Pacific Economic Cooperation
Capacity Building Workshop On Understanding Conformity Requirements For Software Controlled Weight And Measuring Instruments For Sustainable Trade 2022
APEC

Software Validation Process



Procedure according to ISO/IEC 27005



- Components needed to calculate risk:
  - list of unwanted events **(threats to assets)**
  - consequences resulting from such events **(impact/hazard/consequence)**
  - Probability of occurrence **(probability/likelihood)**

APEC Asia-Pacific Economic Cooperation
Capacity Building Workshop On Understanding Conformity Requirements For Software Controlled Weight And Measuring Instruments For Sustainable Trade 2022
APEC

Software requirements in the MID (ex.)

- **Annex I, 8.3: Software (A1)** that is critical for metrological characteristics shall be **identified (A9)** as such and shall be secured. Software identification shall be easily provided by the measuring instrument. **Evidence of an intervention (A2)** shall be available for a reasonable period of time.
- **Annex I, 8.4: Measurement data (A3)**, **software (A1)** that is critical for measurement characteristics and **metrologically important parameters (A4)** stored or transmitted shall be adequately protected against accidental or intentional corruption.

APEC Asia-Pacific Economic Cooperation

Capacity Building Workshop On Understanding Conformity Requirements For Software Controlled Weight And Measuring Instruments For Sustainable Trade 2022

APEC

Software requirements in the MID

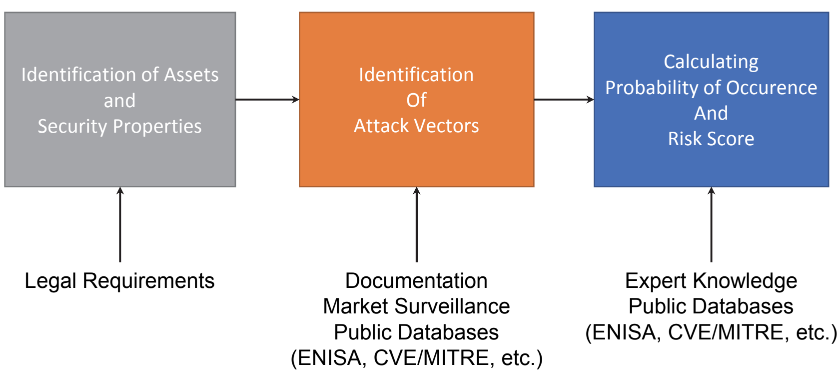
Primary Assets derived from the MID		
Number	Asset	Security Property
A1	metrological software	integrity, authenticity
A2	evidence of an intervention	availability, integrity
A3	measurement data	integrity
A4	metrological parameters	integrity
A5	inadmissible influence on the software	unavailability
A6	indication of the result	availability, integrity

APEC Asia-Pacific Economic Cooperation

Capacity Building Workshop On Understanding Conformity Requirements For Software Controlled Weight And Measuring Instruments For Sustainable Trade 2022

APEC

Risk Assessment Procedure (ISO/IEC 27005)

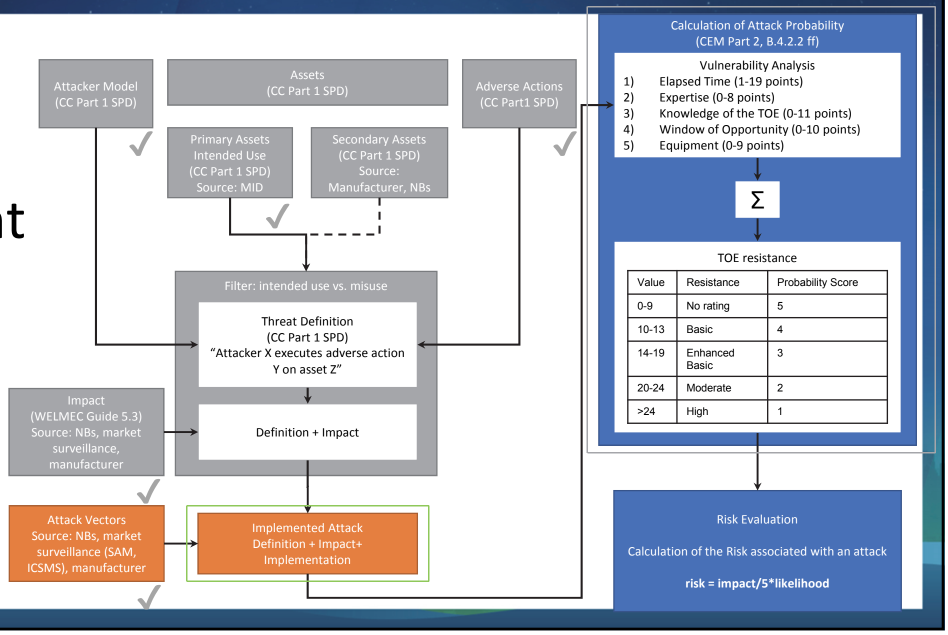


APEC Asia-Pacific Economic Cooperation

Capacity Building Workshop On Understanding Conformity Requirements For Software Controlled Weight And Measuring Instruments For Sustainable Trade 2022

APEC

Risk Assessment Procedure



Value	Resistance	Probability Score
0-9	No rating	5
10-13	Basic	4
14-19	Enhanced Basic	3
20-24	Moderate	2
>24	High	1

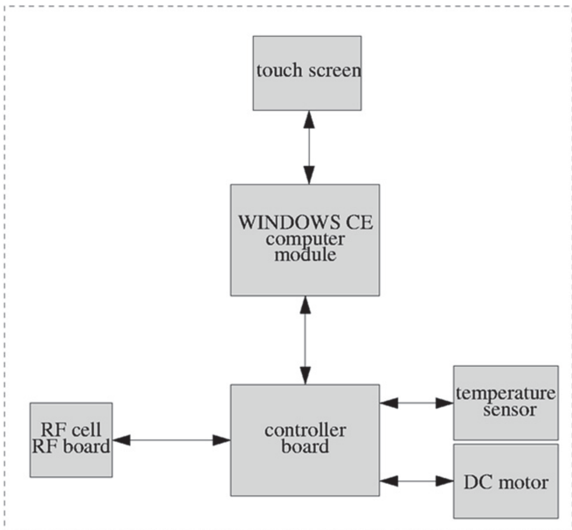
APEC Asia-Pacific Economic Cooperation

Capacity Building Workshop On Understanding Conformity Requirements For Software Controlled Weight And Measuring Instruments For Sustainable Trade 2022

APEC

Example: Grain Moisture Analyzer

- Initialization of measurement via serial port
- Setting of certain parameters via serial port
- Retrieval of results via serial port or USB
- Operating system protected by a 6-digit password



Example: Attack Vectors

- **A_PASSWORD:** An attacker retrieves the admin password by trying all 6-digit combinations.
- **A_SW_REPLACE:** An attacker retrieves the admin password and replaces the legally relevant software.
- **A_INT_SERIAL:** An attacker exploits a vulnerability of the proprietary serial protocol and causes the instrument to malfunction.
- **A_INT_SERIAL_VALUE:** An attacker exploits a vulnerability of the proprietary serial protocol and manipulates a measurement value.
- **A_INT_USB:** An attacker manages to install malicious code by disabling the USB-port‘s protection.

APEC Asia-Pacific Economic Cooperation
Capacity Building Workshop On Understanding Conformity Requirements For Software Controlled Weight And Measuring Instruments For Sustainable Trade 2022
APEC

Example: Risk Score

Threat	Description	Impact	Attack Vector	Elapsed Time	Expertise	Knowledge of the TOE	Window of Opportunity	Equipment	Sum	Score	**Risk**
T1	Local admin (S2) invalidates integrity or authenticity of the metrological software (A1).	5	A_SW_ REPLACE	(>180d) **19**	(expert) **6**	(restricted) **3**	(unlimited) **0**	(standard) **0**	28	1	**1**

Capacity Building Workshop On Understanding Conformity Requirements For Software Controlled Weight And Measuring Instruments For Sustainable Trade 2022

Challenges of WELMEC 7.2

- Accent on security-oriented requirements
- No quality requirements for documents (consistency, plausibility, usability)
- Emphasis on simple reviews of documents
- Low quality of documents / software documentation (internal quality, correspondence with product / software implementation)
- Risk to ignore a mismatch between documents and product, especially between software documentation and implementation
- Appropriate risk analysis
- Cost-intensive validations
- software separation in case of using operating systems