Assessment Methodology for the Application of FPGA Based I&C Systems in NPPs

Dagmar Sommer, Manuela Jopen, Claudia Quester
Gesellschaft für Anlagen- und Reaktorsicherheit (GRS) gGmbH, Germany

10th Workshop on Application of FPGAs in NPPs, South Korea
December 4th – 6th, 2017

Contents

- **Introduction**
- **Recent research** – CAMIC methodology for safety assessment of complex electronic components (CEC)-based I&C equipment and systems
- **Current research** – Diversity assessment of qualified CECs available for usage in the nuclear industry and other safety-critical applications
- **Future research** – Taking CAMIC further
- **Summary**

GRS – Introduction (1)

GRS is

- Main Technical Support Organization (TSO) in nuclear safety for the German federal government
  - BMUB (Federal Ministry for the Environment, Nature Conservation, Building and Nuclear Safety),
  - BMBF (Federal Ministry of Education and Research),
  - BMWi (Federal Ministry of Economic Affairs and Energy) and
  - AA (Federal Ministry of Foreign Affairs) and

- Major German research organization in nuclear safety

- GRS participates in international activities of
  - IAEA, OECD, EU (DG Energy, DG RTD, DG DevCo), …
- GRS supports authorities of other countries as a TSO

GRS – Staff, Locations and Subsidiary

GRS

- about 440 staff members at 4 locations (Cologne, Garching, Braunschweig and Berlin)
- thereof about 310 technical-scientific experts in process and mechanical engineering, physics, chemistry, geology, etc.

Subsidiary

- **RISKAUDIT IRSN/GRS International**
  - a non-profit European Economic Interest Grouping (EEIG)
  - located in Paris (headquarters), also office in Kiev

RISKAUDIT

Motivation

Situation in NPPs – GRS view

- Complex electronic components (CECs) like FPGAs and CPLDs are increasingly applied in the I&C systems of NPPs
  - Implementation of new I&C systems
  - Replacement or upgrade of existing I&C systems or single components within I&C systems

  → *Regulatory approval is required for all safety I&C*

- Regulatory approval of safety I&C demands proof concerning
  - Execution of intended functions only
  - Fulfillment of safety and reliability requirements

  → *Assessment of safety I&C comprising FPGAs or other complex electronic components is essential*

Contents

Recent research –CAMIC methodology

What is CAMIC (Cyclic Analytic Methodology for I&C)?

- Designed for the assessment of safety I&C systems and equipment in NPPs
  - CEC-based I&C systems
  - CEC equipment

- Wide range of applicability for regulatory approval
  - Implementation of new I&C systems
  - Replacement of existing I&C systems and equipment
  - Retrofitting measures

- Modular design provides flexibility and enables targeted course of action
  - Assessment procedure is self-adapting to the situation, i. e. assessment procedure depends on extent and type of I&C, requirements, intermediate results etc.
  - Approach employs various analysis tools (established tools and GRS-developed tools) that are selected according to the situation via decision making diagrams

→ *CAMIC is a versatile, systematic approach aimed at assessing the application of CEC-based I&C systems and equipment in NPPs*

Recent research –CAMIC methodology

Concept of CAMIC

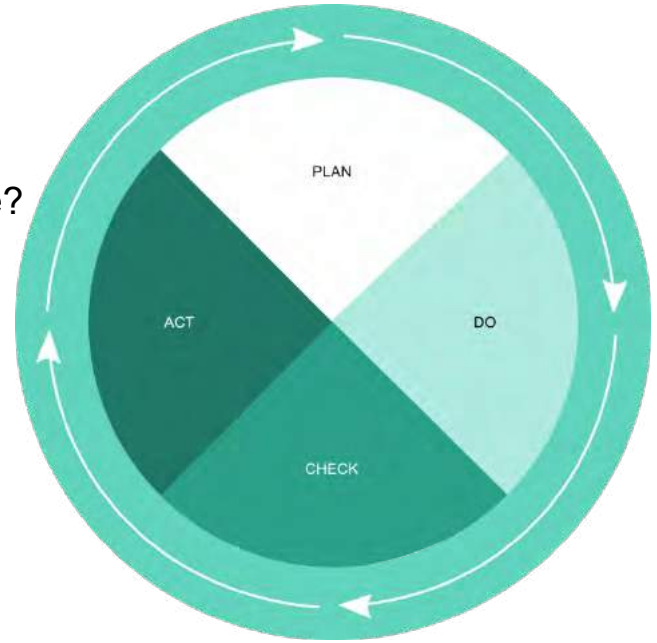
- based on a model of continual improvement by the Plan-Do-Check-Act (PDCA) cycle

- PDCA cycle
  - widely applied in the industry for process and quality management,
  - described in many standards, e. g. ISO 9001:2015, KTA 1402
  - a general approach
  - the four steps Plan-Do-Check-Act can be adapted to specific objectives and requirements of the qualification, certification and licensing of the I&C equipment and systems, e.g.
    - Design and implementation phases of new I&C, replacement of I&C, retrofitting measures
    - Identification of improvement possibilities
    - Evaluation of safety issues, e.g. Defense-in-Depth, CCF potential
  - PDCA is a four-step iterative approach, the cycle being repeated until either plans are good enough to be put into action or plans are omitted

→ *PDCA is very well suitable for assessing the application of CECs in the I&C of a NPP*

Recent research –CAMIC methodology

General description of a PDCA cycle



- A PDCA cycle consists of four steps answering certain questions:
  - Before starting
    - To which issue or project the PDCA principle is applied here?
    - What is the aim of the PDCA process in this case?
  - PLAN
    - What is necessary to achieve this aim?
  - DO
    - What are the results of the analysis of this issue or project?
    - What will happen should the project be implemented?
  - CHECK
    - Are analysis results and project impact in accordance with the requirements?
  - ACT
    - Are any changes necessary before the issue or project may be implemented?
  - After undergoing one cycle:
    - Will any changes be made to project or issue?

→ *The adaptation of PDCA for CAMIC methodology is presented on the following slides*

Recent research –CAMIC methodology

PDCA adapted for CAMIC approach

- CAMIC uses PDCA for the assessment of CEC-based I&C
  - Before starting
    - To which issue or project is the PDCA principle applied here?
      → *Planned implementation of CEC-based I&C in a NPP*
    - What is the aim of the PDCA process in this case?
      → *Assessment of the impact of the planned implementation regarding accordance with relevant requirements*
  - PLAN
    - What is necessary to achieve this aim?
      → *Gathering all information relevant for the assessment (i. e. documents concerning planned implementation of I&C and standards comprising relevant requirements)*
  - DO
    - What are the results of the analysis of this issue or project?
      → *Performing an analysis of the planned implementation of I&C based on information gathered in process step PLAN*
    - What will happen should the project be implemented?
      → *Estimation of the impact of potential failure modes of the CEC-based I&C when implemented as planned*

Recent research –CAMIC methodology

PDCA adapted for CAMIC approach (continued)

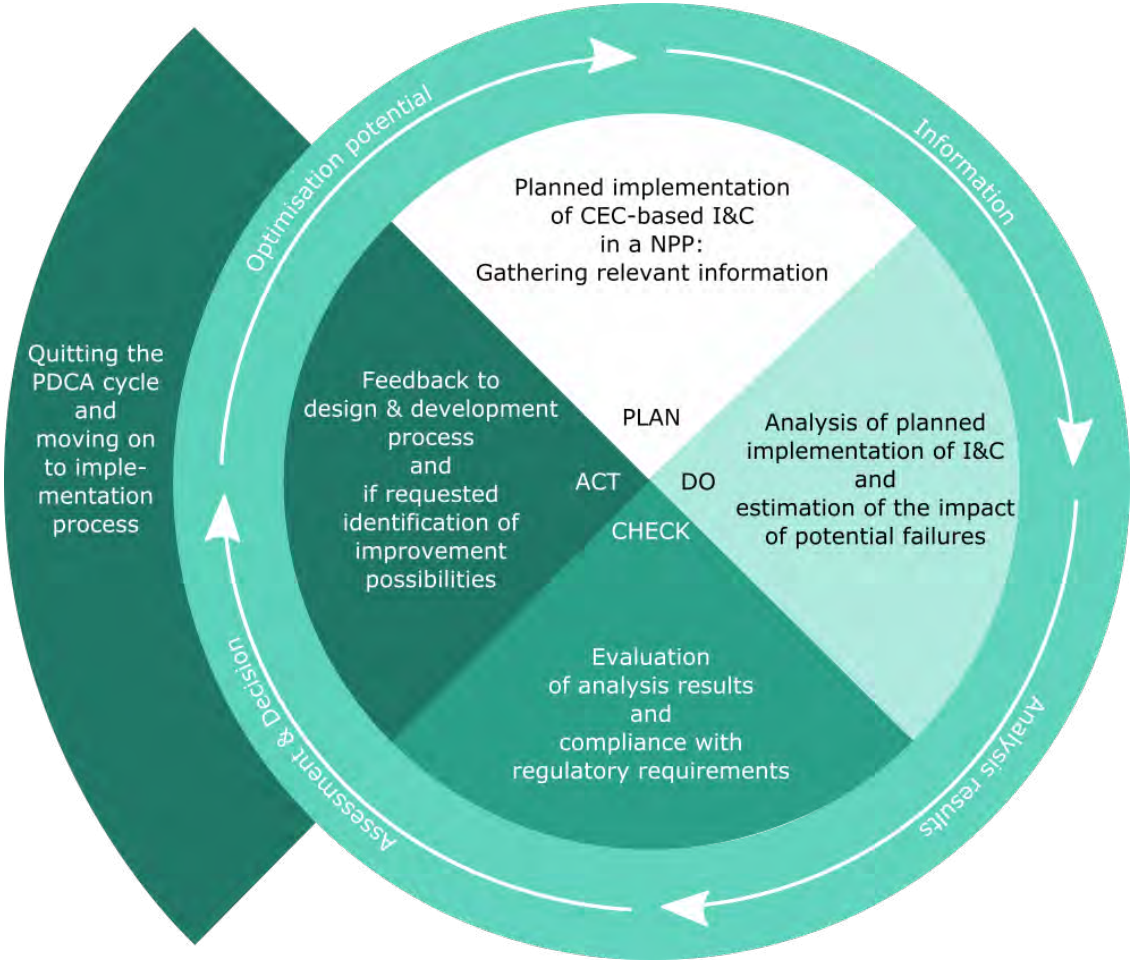
- CHECK
  - Are analysis results and project impact in accordance with the requirements?
    → *Evaluation of possible CEC-induced failure modes and effects within the I&C architecture as determined in process step DO*
    → *Evaluation of compliance of analysis results with regulatory requirements*

- ACT
  - Are any changes necessary before the issue or project may be implemented?
    → *Decision making based on process step CHECK as to whether the CEC-based I&C may be implemented as intended*
    → *"Yes": Exit the PDCA cycle and move on to implementation process*
    → *"No": Remain in PDCA cycle and give feedback to team responsible for planning the implementation of CEC-based I&C,*
    → *OR: identification of improvement possibilities and add the results or resulting demands to the feedback*

- After undergoing one cycle:
  - Will any changes be made to project or issue?
    → *"Yes": New start of the PDCA cycle, taking into account and analysing the changes*

Recent research –CAMIC methodology

PDCA adapted for CAMIC approach (continued)



Recent research –CAMIC methodology

CAMIC toolbox

- For assessment of the planned implementation of CEC-based I&C system or equipment:

  CAMIC comprises a range of analysis tools in the CAMIC toolbox

- Analysis tools (examples)
  - Failure mode and effects analysis (FMEA)
    - Identification of potential failure modes and analysis of their possible effects
    - initially done on component level (failure effects on CEC-based equipment),
    - may be extended to system level (failure effects on the output signal of the I&C system) or
    - function level (failure effects on I&C function/safety function)
  - Fault tree analysis (FTA)
    - Top-down analysis of causes of one selected failure that has to be avoided
    - FTA may be done on system level or function level
  - GRS-developed diversity matrix
    - Assessment of diversity of I&C components or systems with respect to the CCF potential

Recent research –CAMIC methodology

Application of CAMIC approach

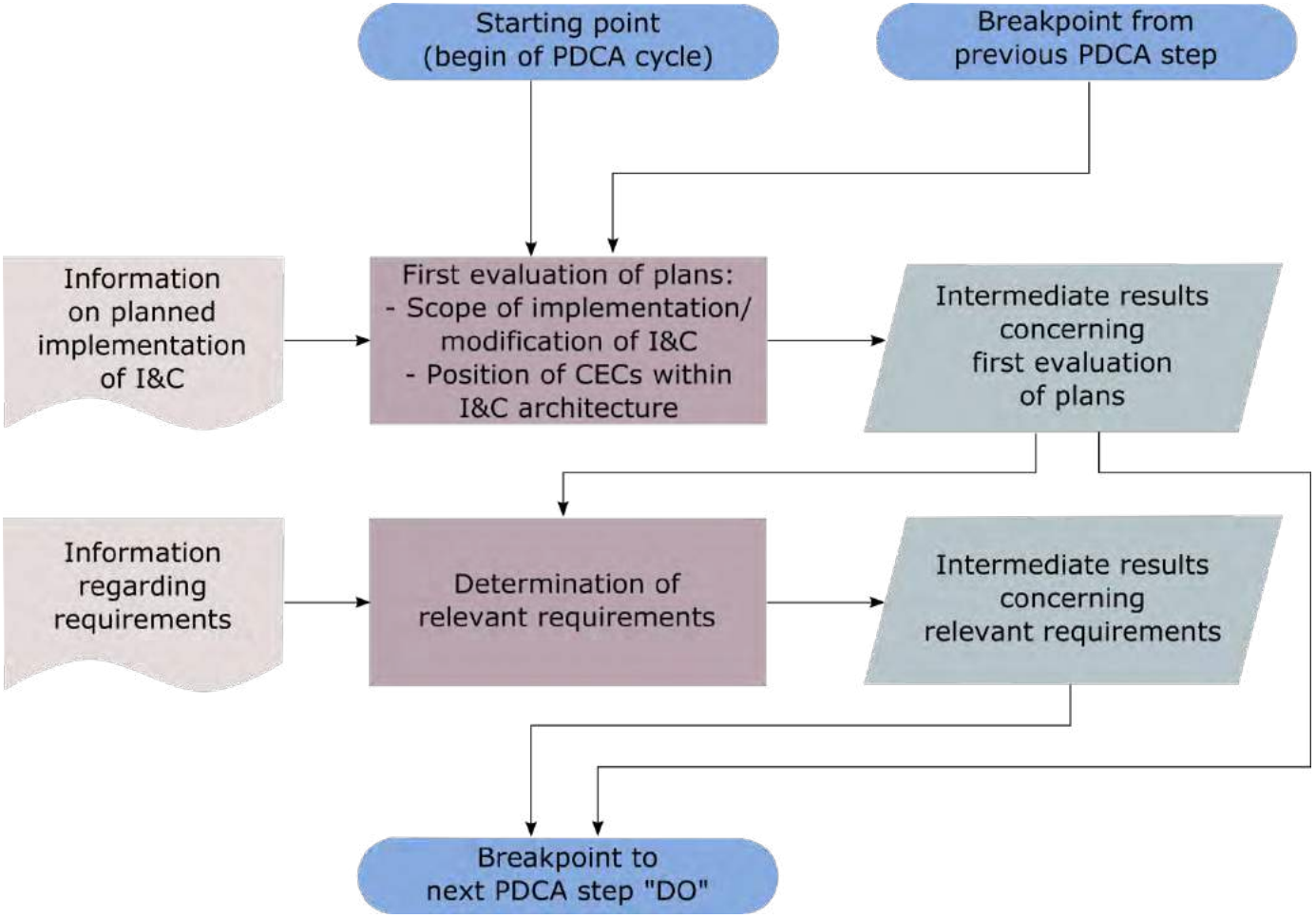
- Modular structure of CAMIC
  - provides flexibility and
  - a tailored assessment procedure for the planned implementation of CEC-based I&C
  - steps of the PDCA-cycle may be handled separately

- Assessment using CAMIC starts at the starting point of the PDCA cycle and ends at a final point, where the PDCA cycle is quitted
  - Starting point: initial plans for I&C implementation → PLAN
  - Final point: ACT → either approval of plans or refusal of plans
- Each PDCA step starts with the situation at the end of the previous step: pre-defined breakpoint
  - Breakpoints: transition between process steps
    PLAN (assessment basis) → DO (intermediate assessment results) → CHECK (accordance with requirements) → ACT (additional claims, change of plans for I&C implementation) → PLAN….

→ *Application of CAMIC leads to an assessment process that stimulates continuous improvement and can react directly to any changes in the initial plans*

Recent research –CAMIC methodology

PDCA-step PLAN of CAMIC approach (exemplary)



Recent research –CAMIC methodology

Decision making process of CAMIC approach

- Decision making diagrams
  - In each PDCA step, decision making has to be done
  - Selection of the analysis tools from CAMIC toolbox via decision making diagrams
  - Most decision making diagrams comprise decision criteria, which may be either fulfilled or not fulfilled

- Decision criteria
  - Each decision criterion: a question that can only be answered with “yes” or “no”
  - Most decision criteria describe a specific aspect of the situation and then pose the question “does this apply here”?

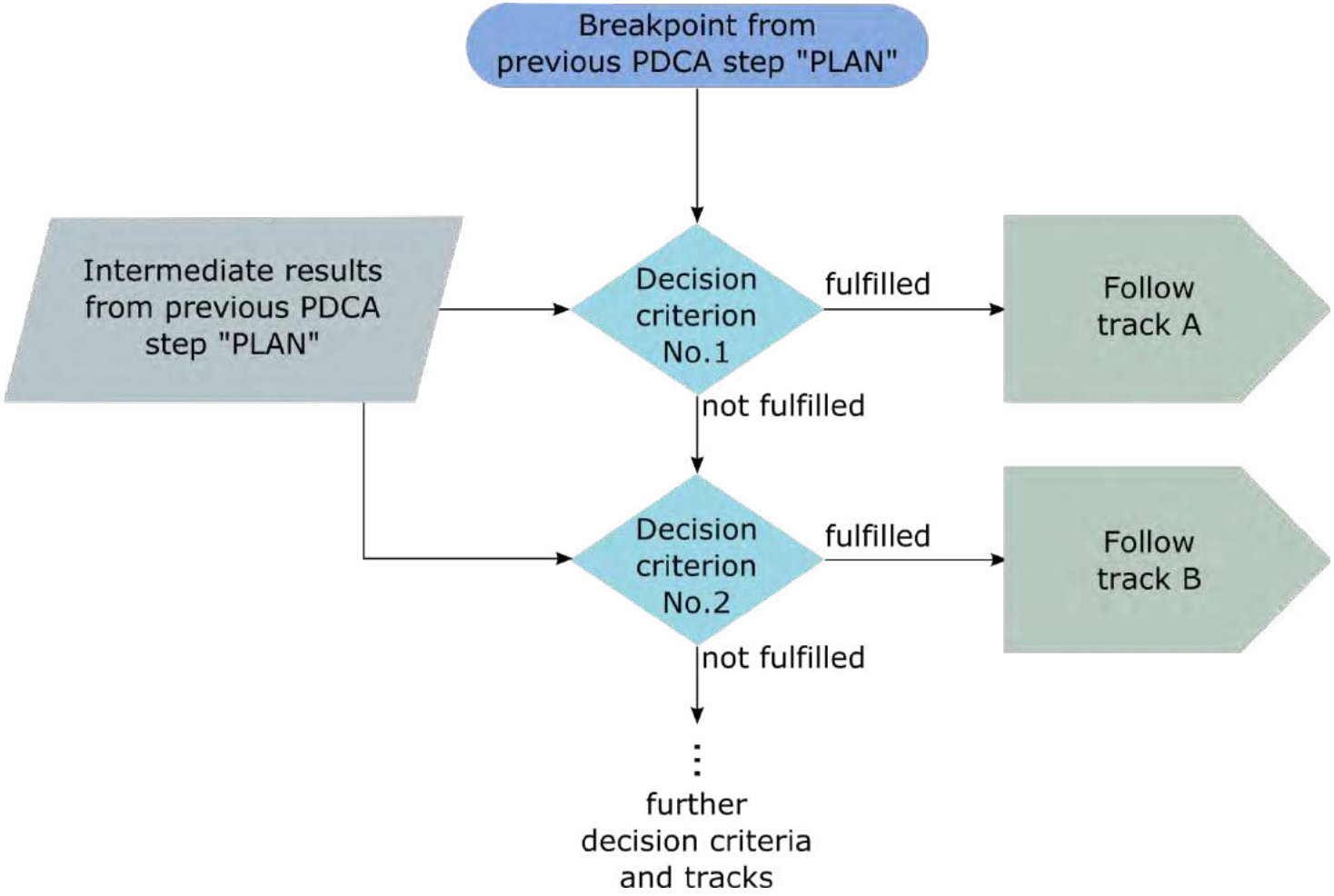
    → *Whether such a decision criterion is fulfilled depends on gathered information and intermediate analysis results*
  - In special cases, a decision criterion describes one possible way to continue the assessment and then ask “is this way of proceeding intended”?

    → *Usually the case when CAMIC toolbox offers a tool for an analysis that may be done either within this PDCA cycle or in another process*

    → *Fulfillment of such a criterion is based upon a process-based decision of the assessor*

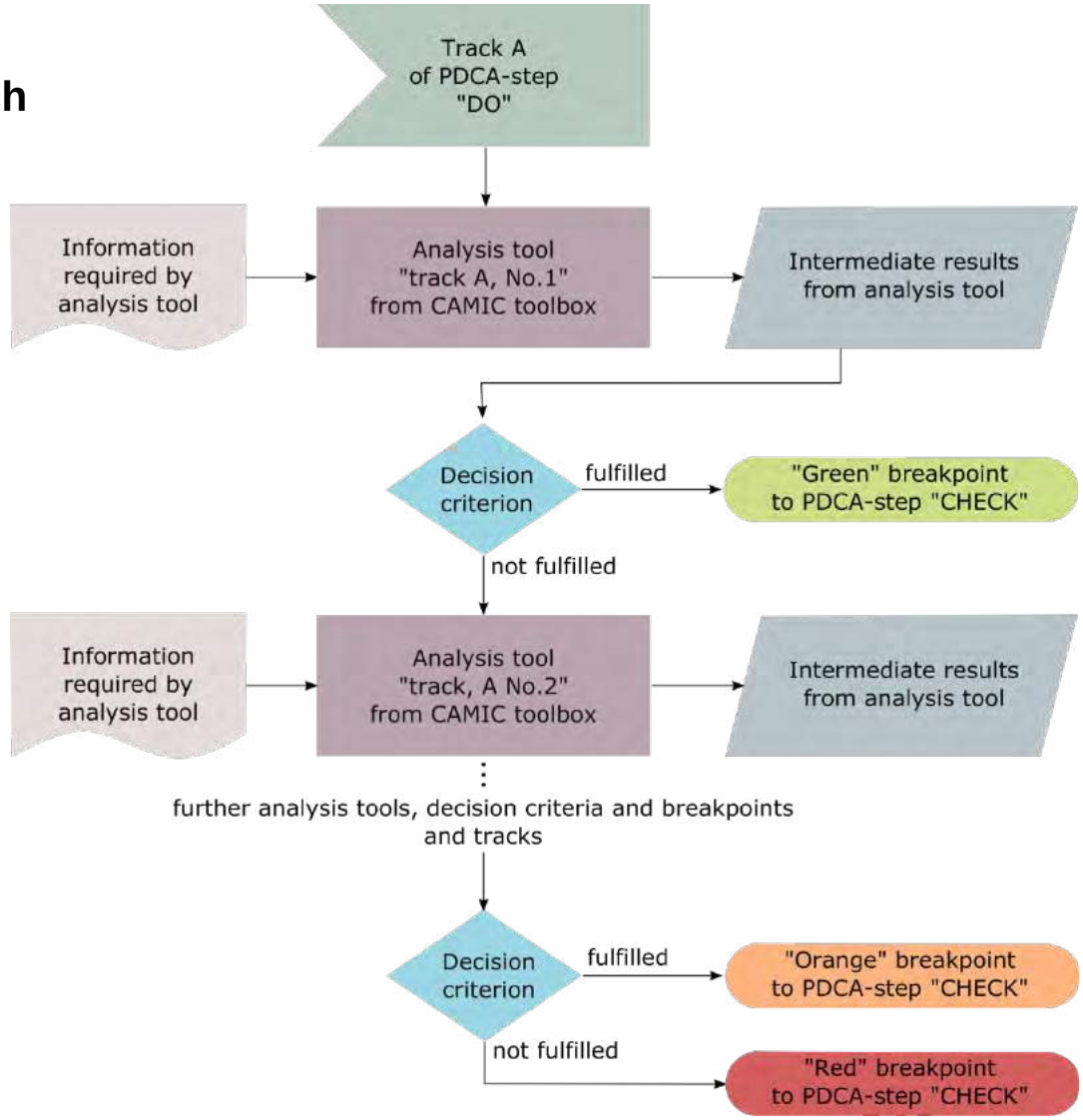
Recent research –CAMIC methodology

PDCA-step DO of CAMIC approach



Recent research –CAMIC methodology

PDCA-step DO of CAMIC approach (continued)



Recent research –CAMIC methodology

PDCA-step DO of CAMIC approach (continued)

- Breakpoints
  - All tracks of the PDCA-step “DO” end in a green, orange or red breakpoint
  - Several breakpoints of each colour

- Red breakpoints
  - A failure mode within CEC-based I&C has been identified that impacts at least one I&C function

  → *Failure on demand or spurious actuation of a safety function cannot be excluded*

- Orange breakpoint
  - A failure mode within the CEC-based I&C has been identified that leads to an erroneous output signal of the I&C system using CEC-based equipment

  → *Failure of the I&C system cannot be excluded*

  →*But: failure is compensated by the correct output of a diverse I&C system, so that no failure of a safety function is to be expected*

- Green breakpoint
  - A failure mode within the CEC-based equipment leads to local failures within the I&C system

  → *Potential failures are compensated within the I&C system*

Recent research –CAMIC methodology

PDCA-step CHECK of CAMIC approach

- There are three tracks of PDCA-step CHECK
  - Track starting with green breakpoint from PDCA-step DO
  - Track starting with orange breakpoint from PDCA-step DO
  - Track starting with red breakpoint from PDCA-step DP

- Possible impacts of failure modes within the CEC-based I&C on I&C systems and safety functions are evaluated with respect to the relevant requirements as identified in PDCA-step PLAN

- Compliance of possible failure impacts with requirements is checked

→ *PDCA-step CHECK identifies requirement that are not fulfilled*

Recent research –CAMIC methodology

PDCA-step ACT of CAMIC approach

- All requirements fulfilled: the PDCA cycle might end with an approval of the planned implementation of CEC-based I&C

- At least one requirement not fulfilled: the PDCA-step ACT provides several possibilities
  - Final disapproval of the planned implementation (PDCA-cycle is quitted)
  - Temporary disapproval of the planned implementation
    - Feedback to the process of design with request to change the plans for implementing CEC-based equipment so that all requirements are fulfilled
    - Optional analysis tools for identification of improvement possibilities, so that more detailed requests can be fed back to the process of design
    - Changed plans will be the basis for the next step in the PDCA-cycle (cycle starts again with PDCA-step PLAN)

→ *PDCA-step ACT leads to approval or final/temporary disapproval of the plans for implementation of CEC-based I&C*

Contents

- **Introduction**
- **Recent research** – CAMIC methodology for safety assessment of complex electronic components (CEC)-based I&C equipment and systems
- **Current research** – Diversity assessment of qualified CECs available for usage in the nuclear industry and other safety-critical applications
- **Future research** – Taking CAMIC further
- **Summary**

Current research – Diversity assessment

Researching CECs

- Study on the state of the art of different types of qualified CECs like FPGAs, CPLDs with the focus on the following aspects
  - Which qualified CECs are currently available on the market?
  - Which of these CECs are already implemented in the I&C of a NPP?
  - What are the regulatory requirements concerning the usage of CECs in NPPs?

- Subject of the study
  - Emphasis on single, qualified CECs designed for usage in a safety-critical environment
  - CEC-based I&C systems are not included, but the single CECs that are used within these I&C systems are considered (where information is available)

- Challenges
  - Information concerning CECs that are actually used in NPPs or other safety-critical environments is scarce
  - Descriptions of CEC-based I&C systems often do not include information concerning manufacturer or type of CEC that is used

Current research – Diversity assessment

Researching CECs (continued)

- Suppliers of CEC chips
  - Manufacturers of CECs currently considered in the study are
    - Xilinx
    - Intel/Altera
    - Microsemi/Actel
    - Lattice Semiconductor/SiliconBlue
    - Microchip/Atmel
    - Cobham/Aeroflex
    - QuickLogic
    - Achronix Semiconductor
  - At this stage, not enough information available on other CEC chip manufacturers

→ *Information concerning additional CEC chip manufacturers would be needed*

Current research – Diversity assessment

Researching CECs (continued)

- Suppliers of CEC-based I&C systems and platforms
  - Several manufacturers of CEC-based I&C systems and platforms like e. g.
    - Radiy
    - Westinghouse/CS Innovations
    - AREVA
    - Lockheed Martin
    - SNPAS
    - Toshiba
  - study focusses on CEC chips, so the CEC-based systems and platforms are not considered directly, but indirectly via the CEC chips they are based on
  - study aims at including all the types of CECs used in these platforms

- Challenges
  - Platform descriptions often do not include information on the types of CECs used

→ *Further information concerning types of CECs used in such I&C platforms would be needed*

Current research – Diversity assessment

Analysis of CEC properties

- Analysis of manufacturer information regarding CEC-specific component properties
  - Which properties of CEC chips can be determined on the basis of available manufacturer information?

- Creation of CEC database based on manufacturer information
  - How comparable is information concerning different CEC chips?
  - The CEC database will include the available information on the CEC chips, emphasising on information possibly relevant for diversity assessment like
    - possibilities for programming and reconfiguration,
    - programming software
    - development tools
    - CEC architecture
    - memory type
    - clock management
    - hardware suppliers
    - security aspects

→ *CEC database will be used for establishing differentiation criteria for single, qualified CEC chips*

Current research – Diversity assessment

Diversity assessment of CEC chips

- Establishment of differentiation criteria for CECs
- A double-track approach for the differentiation criteria
  - General differentiation criteria for FPGAs and CPLDs
  - Type-specific differentiation criteria for currently available CEC chips

- Development of a methodology for diversity assessment of FPGAs and other CECs
  - Adaption of the GRS-developed diversity matrix designed for diversity assessment of digital I&C systems and components in general
  - Focus on diversity assessment of CEC chips
  - Review of all diversity criteria in the diversity matrix against the background of the following issues
    - Relevance of the diversity criteria for application on CEC chips
    - Possible adjustments of diversity criteria for application on CEC chips
    - Potential additional diversity criteria specifically for application on CEC chips

→ *Methodology for diversity assessment of qualified CECs available for usage in the nuclear industry and other safety-critical applications using adapted diversity matrix*

Contents

- **Introduction**
- **Recent research** – CAMIC methodology for safety assessment of complex electronic components (CEC)-based I&C equipment and systems
- **Current research** – Diversity assessment of qualified CECs available for usage in the nuclear industry and other safety-critical applications
- **Future research** – Taking CAMIC further
- **Summary**

Future research – Taking CAMIC further

Further development of CAMIC methodology and tools including

- Extension of the scope of application of CAMIC methodology to all complex I&C equipment and systems

- Enhancement of CAMIC methodology
  - Inclusion of additional analysis tools
  - Inclusion of CEC-specific diversity assessment into CAMIC (adapted diversity matrix)

- Development of CAMIC software

- Model-based V&V of the CAMIC approach and CAMIC software
  - Continuation of modelling and V&V as done in recent GRS research
  - Demonstration of consistency of results from decision-diagram-based CAMIC approach and software-assisted CAMIC approach

Contents

- **Introduction**
- **Recent research** – CAMIC methodology for safety assessment of complex electronic components (CEC)-based I&C equipment and systems
- **Current research** – Diversity assessment of qualified CECs available for usage in the nuclear industry and other safety-critical applications
- **Future research** – Taking CAMIC further
- **Summary**

Contents

Summary

- GRS has developed **CAMIC methodology** for safety assessment of CEC-based I&C equipment and systems in NPPs
- CAMIC is a versatile, systematic approach whose modular design allows a **tailored assessment process for a wide range of applications** in the framework of regulatory approval of plans to implement CEC-based I&C in a NPP
- GRS is now working on a **CEC database** for single, qualified CEC chips that are currently available for safety-critical applications
- Based on the CEC database, a methodology for **diversity assessment of CECs** will be developed
- Next step: Further enhancement of CAMIC methodology and development of **CAMIC software**