Note:
This is a translation of the RSK statement entitled “Redesign von leittechnischen Baugruppen und Komponenten in Kernkraftwerken”
In case of discrepancies between the English translation and the German original, the original shall prevail.

RSK statement
(450th meeting on 26/27 September 2012)

Redesign of I&C modules and components in nuclear power plants

CONTENTS

1 Reason for and course of the deliberations

By advisory request RS I 3 - 17018/0 of 08 March 2011 [1], the BMU tasked the RSK with examining whether the discontinuation of I&C components and systems and their substitution by redesign components is expected to have adverse safety-related effects on nuclear power plants. The ELECTRICAL INSTALLATIONS Committee began its deliberations at its 211th meeting on 28 June 2011.

As a first step, the Committee on ELECTRICAL INSTALLATIONS felt that it should be clarified to what extent and at what level of defence redesign components are already being used today. VGB was asked to report on this in a letter dated 01 July 2011. The VGB report ([2], [3]) was presented at the 213th meeting of the ELECTRICAL INSTALLATIONS Committee on 19 October 2011 and formed the basis for continuing the deliberations. These deliberations did not result in the conclusion that there was a need to carry out any further working steps. The committee adopted the DRAFT/statement as a submission for the RSK at its 218th meeting on 25 April 2012.

The RSK adopted the statement in hand at its 450th meeting on 26/27 September 2012.

2 Background

2.1 Advisory request

The background behind these deliberations is that spare parts, replacement assemblies and replacement components for instrumentation and control (I&C) systems currently in operation are largely or partially no longer available. One reason for this is that manufacturers have cancelled subsequent deliveries for systems such as DM (dynamic magnetic core system), ISKAMATIC A/B or EDM. Against this background, there were plans to replace the existing safety I&C technology with new digital I&C systems. In contrast, publications point out that subsequent developments and the redesign of selected I&C components would be an alternative to replacing entire I&C systems.

In accordance with the BMU's advisory request [1], the “redesign” products are divided into the following three groups:

Group 1 are 1:1 redesigns of existing assemblies and components (copies). This involves creating a redesign that does not differ or differs only insignificantly from the original in terms of its electrical connection sizes, range of functions, circuit diagram, (circuit board) layout and physical dimensions.

Group 2 includes assemblies and components that are redesigned on the basis of modern programmable modules in such a way that although the electrical connection sizes, range of functions and physical dimensions correspond to the originals and pin compatibility with the originals is ensured, the circuit diagram, circuit board layout and design concept are fundamentally different from the original due to the new technology used.

Group 3 comprises assemblies and components that are compatible in terms of electrical connection sizes, functional scope and physical dimensions as well as pin assignment but only use modern analogue components on advanced circuit boards instead of programmable components.

The scope of consideration also includes components that may entail a change in the design configuration (back panel wiring). In the opinion of the Committee on ELECTRICAL INSTALLATIONS, the scope of consideration should include larger-scale measures as part of modifications to the power plant or maintenance and be clearly differentiated from simple repairs of individual assemblies (e.g. by using more modern components due to problems in procuring the original components).

In this context, the BMU asks the RSK to answer the following questions:

1. What adverse safety-related effects have been identified to date due to the cancellation of spare parts deliveries by the manufacturers of I&C systems and what effects are expected in the future?

2. To what extent and at what levels of defence are redesign components from one of the three groups mentioned already being used today?

3. Can the same or greater reliability be achieved with redesign components than with original components and can this be demonstrated quantitatively and with concrete examples?

4. To what extent must systematic failure also be taken into account when using redesign components, especially Group 2 components?

5. Can the reliable continued operation of existing systems be achieved without lowering the current safety level by using redesigned Group 3 components that may not be manufactured by the original manufacturer but elsewhere? What measures, over and above existing measures for type and performance testing, are necessary to ensure this?

2.2 Enquiry to VGB

In a letter [4] dated 1 July 2011, the Committee on ELECTRICAL INSTALLATIONS asked VGB to answer the following questions:

1. Assembly identification and system designation:
   Which redesign components have been replaced or are to be replaced?

2. Qualification:
   How and according to which standard were the redesign components qualified and were type tests carried out?

3. Functionality:
   Has the functionality of the original assembly been retained or modified?

4. Point in time:
   When was an exchange made or is an exchange planned?

5. Group assignment:
   To which of the above groups can the redesign components be assigned (with a more detailed explanation: analogue, digital, FPGA, etc.)?

6. Pin compatibility:
   Have the redesign components been or will they be made pin-compatible?

7. Functional compatibility:
   Are the redesign components functionally identical or do they differ from the assembly to be replaced?

8. Environment compatibility:
   Do the redesign components have the same environmental conditions as the originals (humidity, voltage, temperature, EMC, vibration resistance, etc.)?

9. Allocation:
   At which level of defence (defence-in-depth concept levels of defence 1 to 4) or safety category (according to KTA, RSK or IEC regulations) was the redesign component used or is it planned to be used?

10. Is there any operating experience with redesign components?

2.3 Report of VGB

VGB stated ([2], [3]) that, in addition to the procurement of spare parts and repairs, replacements were carried out in nuclear power plants both in the past and today as part of the maintenance measures for I&C equipment, namely when

- the manufacturers of the I&C equipment did or do not offer any replacement solutions or discontinued product support,

- no replacement components were or are available for maintenance measures and could not or cannot be procured elsewhere,

or

- replacement solutions become necessary due to preventive measures from ageing management.

With the discontinuation of devices or systems, manufacturers normally offer successor devices/systems. For use in safety-relevant areas of nuclear installations, these successor devices/systems must be tested or qualified in accordance with the nuclear regulations. These successor devices/systems are often not directly compatible with the previously used device technology, so that a replacement in these cases would only be possible in the sense of a complete realisation in the new device technology. In these cases in particular, if the supply of spare parts for the previous device technology cannot be secured in the long run, redesign is used for individual devices or assemblies of I&C systems.

The repair measures for I&C equipment in German nuclear power plants are carried out by four certified workshops. In order to maintain the underlying quality level, these workshops have defined a graduated qualification system and the associated qualification procedures are evaluated by the authorised experts consulted by the supervisory authorities in accordance with § 20 AtG.

If the repair of a device is no longer possible because no similar component type can be procured according to standard comparison criteria, the device has to be replaced by a ‘redesign’ or a new ‘design’.

In contrast to the grouping in the BMU's advisory request, the term ‘redesign’ is used for a function-, pin- and plug-compatible substitution while the term ‘design’ is used for a substitution with modified technical data or extended functionality. An example of a redesign assembly is, for example, the development of an I/U converter as a successor device to a discontinued assembly that cannot be repaired or can only be repaired at great economic expense. The development of a four-wire box to replace four-wire transmitters with two-wire transmitters was cited as an example of a design module.

For these two types of substitutions, components (including integrated circuits) that are comparable to those used for initial deployment are used for safety-critical equipment, albeit with a modified design (Group 3 as specified by the BMU). The use of programmable circuits has so far been generally excluded.

In addition to the substitutions from the redesign and design process, there are also replacements of the device technology (completely or for certain I&C system parts) in which programmable circuits or a completely software-based technology can also be used. According to VGB's explanations, such a replacement requires a corresponding licensing procedure for safety-relevant equipment and is not the subject of VGB's explanations.

Both the redesign and the design process in accordance with VGB Guideline no. RL005/A follow a phase model according to the specifications of the applicable nuclear regulations with the following phases:

- preparation of a description of the needs
- preparation of a requirements specification
- preparation of a user requirements specification
- selection of the manufacturer
- preparation of functional specifications by the manufacturer

- production and preliminary testing of the prototype series
- carrying out the initial qualification.

The qualification of these substitutions is carried out in accordance with the applicable nuclear regulations in coordination with the authorised experts consulted by the supervisory authorities in accordance with § 20 AtG.

The report says that substitutions following the redesign or design process have so far been carried out for modules from the Geamatik, DM, Teleperm B, Simatik P device systems and for Siemens special modules and have been used in device categories E1 and E2 in accordance with the definitions of the RSK guidelines for PWRs (note from the Committee on ELECTRICAL INSTALLATIONS: The device categories mentioned therefore include devices that perform I&C functions at all four levels of defence of the RSK's defence-in-depth concept). The available operating experience is unreservedly positive. In all cases, the failure rates of the substitutions are lower than the failure rates of the replaced assemblies.

One manufacturer offers redesign components with PLD technology (Programmable Logic Devices). According to the VGB-WG, the products of this manufacturer are not used in safety-relevant equipment in nuclear power plants. Neither the manufacturer nor the products are qualified accordingly. However, it cannot be ruled out that one of these products is used in operational applications. There are currently no plans to use PLD technology for redesign components in safety I&C technology. These products are reported to be used in conventional systems. It can be assumed that these products do not fulfil the requirements of a nuclear type test.

VGB responded in the affirmative to the enquiry of the Committee on ELECTRICAL INSTALLATIONS as to whether the current practice is suitable for ensuring the maintenance of nuclear power plants also in the long run. Due to the limited remaining operating lives, it can be assumed that all necessary substitutions in safety-relevant equipment can be ensured by best practice. Restrictions would only arise if a large-scale replacement were required, as this could overstretch the available qualification, production and component resources. However, a need for this is not discernible.

The Committee's question as to whether unplanned differences in functional behaviour had also been observed in the case of substitutions was answered in the affirmative. Such a deviation had been observed in one assembly during the type test, but not during operation of the system.

2.4 Summary of VGB's statements

As part of the maintenance measures for I&C equipment in nuclear power plants, substitutions have been carried out in the past as well as today in addition to the procurement of spare parts and repairs. For all substitutions that can be categorised as ‘redesign’ or ‘design’, the circuits used in safety-relevant equipment are basically comparable to those used in the initial installation, albeit generally with a modified design and, in the ‘design process’, possibly with functional changes. However, the use of programmable circuits is generally excluded in both processes. The qualification of these substitutions is carried out in line with the

applicable nuclear regulations and in coordination with the authorised experts consulted by the supervisory authorities in accordance with § 20 AtG. Substitutions after the redesign or design process have so far been carried out in the equipment categories E1 and E2 in accordance with the RSK guidelines for PWRs for assemblies from the Geamatik, DM, Teleperm B, Simatik P equipment systems and for Siemens special assemblies. The available operating experience is positive.

In addition to the substitutions from the redesign and design process, there is also a replacement of the device technology (complete or for certain I&C system parts) than can also involve the use of programmable circuits or a completely software-based technology. According to VGB, such a replacement requires a corresponding licensing procedure and is not the subject of VGB's explanations.

3 Assessment by the RSK and answers to the BMU's questions

3.1 General

With reference to an article in VGB-PowerTech[1], the BMU's advisory request [1] uses the term ‘redesign’ to refer to the post-development and replication of selected I&C components as an alternative to the replacement of I&C subsystems. According to this article, a ‘redesign’ is the pin- and function-compatible new development of a module that is no longer available and can be used in a given system instead of the original part. A further subdivision into three groups according to the scope of the new product is made by the BMU, whereby Group 1 is assigned copies of existing assemblies, Group 2 describes components based on modern programmable modules, and the components in Group 3, in contrast, contain modern analogue components instead of programmable modules.

In contrast to this understanding of redesign, VGB used other definitions in its presentation ([2], [3]) at the 213th meeting of the Committee on ELECTRICAL INSTALLATIONS on 19 October 2011.

Accordingly, replicas that are associated with the term ‘redesign’ represent a functional, pin and plug-compatible substitution with possibly modified assembly technology. Replicas where the substitution also includes modified technical data and changes in functionality are categorised as ‘design’. VGB has provided examples of both cases.

Applying the groups used in the BMU's advisory request, it was explained in the presentation that only substitutions in Group 3 had been carried out in the completed projects with safety relevance. Projects with safety relevance that are currently in the planning phase are also only planned for Group 3.

VGB's definitions of the terms ‘redesign’ and ‘design’ are comprehensible to the Committee on ELECTRICAL INSTALLATIONS. According to VGB, the use of programmable circuits for such substitutions is generally excluded for safety-related equipment.

[1] Reinhard Hentschel, Wolfgang Kochs und Ralf-Michael Zander „Alterungsmanagement der Elektro- und Leittechnik in Kraftwerken der RWE Power“, VGB PowerTech 10/2010

Provided that the facts underlying this statement of VGB are implemented in practice in all plants and that this will continue to be the case in the future, the RSK currently sees no need for further deliberations for Group 2 with respect to [1].

Irrespective of this, the questions of the advisory request will be addressed below, taking into account the content of the VGB presentation ([2], [3]) from the 213th meeting of the Committee on ELECTRICAL INSTALLATIONS on 19 October 2011.

This statement does not deal with the replacement of peripheral components with standardised interfaces (such as transmitters). Aged or obsolete devices can be replaced with devices of a newer generation, in some cases with a change in technology, without changing the central I&C technology. The replacement devices must also be qualified in accordance with the nuclear regulations. Such a replacement of individual devices with new devices from original manufacturers is not a substitution according to the above definition of a redesign/design process (see page 5), which is why the RSK does not consider such a replacement to be covered by the advisory request [1].

3.2 Answers to the BMU's questions

3.2.1 Question 1 of the BMU: Consequences of a cancellation of spare parts deliveries

What adverse safety-related effects have been identified to date due to the cancellation of spare parts deliveries by the manufacturers of I&C systems, and what effects are expected in the future?

Response from the RSK

The presentations ([2], [3]) of VGB at the 213th meeting of the Committee on ELECTRICAL INSTALLATIONS on 19 October 2011 showed that redesign components have been used in individual cases since 1984 and are still used today. Since the newly used components had at least the same functionality as the assemblies to be replaced - in individual cases additional functional features were implemented, e.g. in the form of overvoltage protection - and also had to fulfil at least the same requirements for resistance to environmental influences as the original assemblies, the RSK believes that, according to the operating experience gained in this regard, there have been no adverse safety-related effects to date due to the cancellation of spare parts deliveries by the manufacturers of I&C systems. Another reason for this assessment is that the redesign components are only manufactured by appropriately qualified manufacturers and have been or are being subjected to quality assurance measures in accordance with the nuclear safety standards (KTA 1401, KTA 3503, KTA 3505).

Nevertheless, it should be noted that the discontinuation of device systems and the resulting need for a design/redesign of individual components causes a great deal of effort for the parties involved in each case, as such production is associated with a complete development process (creation of a description of the needs/requirements specification, selection of a manufacturer, creation of functional specifications by the manufacturer, production and preliminary testing of the prototype series as well as initial qualification). In the opinion of the RSK, it is not to be expected that operators will carry out

comprehensive redesign projects with regard to the substitution of complete device systems. However, according to the explanations of VGB in the presentation at the 213th meeting of the Committee on ELECTRICAL INSTALLATIONS on 19 October 2011, no need was seen for the substitution of entire device systems due to the currently existing conditions regarding the remaining operating lives of the German nuclear power plants. The RSK agrees with these statements of VGB.

The bottom line from the point of view of the RSK with regard to the question of the safety significance of the cancellation of spare parts deliveries by the manufacturers is that no adverse safety effects have been identified so far and are not to be expected in the future if the qualification requirements continue to be met.

3.2.2 Question 2 of the BMU: Use of redesign components

To what extent and at what levels of defence are redesign components from one of the three groups mentioned already being used today?

Response from the RSK

The information provided by VGB [2] shows that substitutions of individual components after the redesign or design process have so far been carried out for device categories E1 and E2 in accordance with RSK guidelines, e.g. for assemblies from the Geamatik, DM, Teleperm B, Simatik P device systems and for Siemens special assemblies, and thus at all four levels of defence. According to the data presented [3], approximately 2,600 assemblies/components have been used as substitutes for seven different types of assemblies/components between 1984 and 2007. The majority of these were Geamatik and Simatik-P assemblies, each with around 1,000 units. According to VGB, the substitution process for three further assembly types is currently in the planning phase. VGB's statements correspond to the state of knowledge of the RSK.

According to the RSK's findings, approx. 220 different module types from the most important I&C device systems ISKAMATIC, EDM, SINUPERM and TELEPERM alone are used in a pre-convoy plant. From this, the RSK concludes that the existing need for substitution of seven module types to date is low compared to the total number of module types used in German nuclear power plants.

3.2.3 Question 3 of the BMU: Reliability of redesign components

Can the same or greater reliability be achieved with redesign components than with original components and can this be demonstrated quantitatively and with concrete examples?

Response from the RSK

The VGB has shown that the substitution processes for safety-relevant equipment are subject to a supervisory procedure in accordance with the requirements of the nuclear rules and regulations. This guarantees the implementation of the quality assurance steps required in the respective application. According to VGB, operating experience to date has been positive. In detail, it has been shown that the reliability of the newly used redesign assemblies is consistently higher than that of the original assemblies used to date ([2], [3]). The RSK considers the statements of VGB to be comprehensible even though there have been deviations in quality in individual cases. Thus, according to the current state of knowledge, sufficient reliability is given for these substitutions and the further application of redesign and design processes is not questioned by the RSK.

The nuclear supervisory procedure ensures that any anomalies will also be identified in the future and that the necessary measures will be implemented to prevent safety-relevant effects resulting from a reduction in the reliability of the I&C system due to the use of redesign assemblies.

3.2.4 Question 4 of the BMU: Failure assumptions when using redesign components

To what extent must systematic failure also be taken into account when using redesign components, especially Group 2 components?

Response from the RSK

As already mentioned, VGB stated in its presentation that neither are any substitutes of Group 2 currently used in the plants nor are any corresponding substitution processes planned. Provided that this statement of VGB remains valid in the future and is supported by all German operators, the RSK currently sees no reason to question the assessments on systematic failure carried out so far in licensing and supervisory practice on the basis of the requirements of the applicable rules and regulations for substitutes of Groups 1 and 3 according to [1]. If Group 2 equipment were to be used, the RSK is of the opinion that further measures are required to implement these requirements.

3.2.5 Question 5 of the BMU: Reliability requirements for the continued operation of systems when using redesign components

Can the reliable continued operation of existing systems be achieved without lowering the current safety level by using redesigned Group 3 components that may not be manufactured by the original manufacturer but elsewhere? What measures, over and above existing measures for type and performance testing, are necessary to ensure this?

Response from the RSK

In consistent application of the previous procedure for substitutions, it can be stated from the point of view of the RSK that reliable continued operation of existing systems can be achieved without lowering the current safety level if redesign components of Group 3 are used that may also not be manufactured by the original manufacturer but elsewhere. The fulfilment of the requirements of the existing regulations (in particular the safety standards KTA 3501/3503/3505) is sufficient to prove the required device quality of the substitutes by completing the required qualification procedures. The substitution processes carried out to date (see [2]) were without exception assigned to Group 3 (in accordance with [1]). The reliability of the substitutes could also be proven with the use of larger quantities (see [3]) through corresponding operating experience (slide 29 from [2]).

A replacement of complete device families in the safety systems of German nuclear power plants by commercially available systems (e.g. TELEPERM XS, automation system AC160) is not to be expected in the remaining years of operation of the nuclear power plants according to the RSK's assessment but would also include a technology change and thus no longer take place under the boundary conditions of the 'redesign' described here (Group 2 according to [1]). According to VGB, a substitution of complete device systems by modern analogue systems (Group 3) would be possible in principle.

In view of previous operating experience, the RSK sees no need for measures that go beyond existing regulations on type and qualification testing in order to ensure reliable continued operation of existing systems without lowering the current safety level when using redesign components (redesign as understood by VGB).

4 Conclusion of the RSK

The use of redesign components/assemblies is not a fundamentally new process but has been carried out since the mid-1980s as a result of the discontinuation of I&C systems operated in German nuclear power plants. Redesign components/assemblies have been used in large numbers, but not across the board as a replacement for complete device systems. Existing regulations on device qualification were applied and can also be applied in the future in order to guarantee the requirements for reliable operation of the systems with the substitutes. According to VGB, the use of redesign components/assemblies has been associated with positive operating experience in the past. The experience gained so far from the supervisory procedures of the German nuclear power plants does not contradict the statements of VGB on the positive operating experience. Thus, in the opinion of the RSK, sufficient reliability for these substitutions is given according to the current state of knowledge and the further application of redesign and design processes is not to be questioned.

Provided that programmable circuits are generally not used for a redesign or design of safety-critical equipment in the future, the RSK currently sees no need for further deliberations on these developments.

5 References

[1] Bundesministerium für Umwelt, Naturschutz und Reaktorsicherheit
„Redesign“ von leittechnischen Baugruppen und Komponenten in Kernkraftwerken
Aktuelle Diskussionen zur Nichtverfügbarkeit/Abkündigung der Hersteller von Ersatzteilen
Schreiben RS I 3 – 17018/0 vom 08.03.2011

[2] VGB PowerTech
Ersatzbeschaffung von technischen Einrichtungen der E- und L-Technik für KKW
VGB-AK „Gerätequalifizierung E- und L-Technik in KKW“ E. Sander (EnKK) und W. Schroeder (VENE „WIL“)
Folienvortrag zum TOP 6 der 213. Sitzung des RSK-Ausschusses „Elektrische Einrichtungen“

[3] VGB PowerTech
Ersatzbeschaffung von technischen Einrichtungen der E- und L-Technik für KKW
Einsatzzahlen und Reparaturmengen Folienvortrag zum TOP 6 der 213. Sitzung des RSK-Ausschusses „Elektrische Einrichtungen“

[4] Schreiben der RSK-/ESK-Geschäftsstelle an den VGB vom 01.07.2011:
Beratungsunterlagen für den RSK-Ausschuss ELEKTRISCHE EINRICHTUNGEN „Redesign von leittechnischen Baugruppen und Komponenten in Kernkraftwerken“, Az.: EE212_BR01.07.2011_VGB

[5] Kerntechnischer Ausschuss KTA 3501 „Reaktorschutzsystem und Überwachungseinrichtungen des Sicherheitssystems“, Fassung Juni 1985 (inhaltlich überprüft und unverändert weiterhin gültig 6/90, 6/95, 6/00; ein Änderungsverfahren läuft seit dem 22.11.2005, wurde aber bislang nicht abgeschlossen)

[6] RSK-Leitlinien für Druckwasserreaktoren, Änderungsstand 15.11.1996
(4. Änderung: Berichtigung (BMU-Bekanntmachung vom 29.10.1996), BAnz Nr. 214 vom 15.11.1996)