

**A deterministic approach for establishing a narrow band
dynamic operating envelope to detect and locate hardware
deterioration in nuclear power plants**

AC CILLIERS

11858176

Thesis submitted for the degree Philosophiae Doctor at the Potchefstroom
Campus of the North-West University, South Africa

Promoter: Prof E.J. Mulder (North-West University, South Africa)

May 2013

Declaration

I, Anthonie Christoffel Cilliers, hereby declare that this thesis entitled:

A deterministic approach for establishing a narrow band dynamic operating envelope to detect and locate hardware deterioration in nuclear power plants

is my own work and has not been submitted to any other University before. Where publications involving co-authors were used, the necessary permission from these authors had been obtained in writing. Relative contributions by the different authors are acknowledged in the relevant chapters.

Signed at Potchefstroom on _____.

Format of this thesis

The format of the thesis is in accordance with academic rule 5.4.2.7 states: “Where a candidate is permitted to submit a thesis in the form of a published research article or articles or as an unpublished manuscript or manuscripts in article format and more than one such article or manuscript is used, the thesis must still be presented as a unit, supplemented with an inclusive problem statement, a focused literature analysis and integration and with a synoptic conclusion, and the guidelines of the journal concerned must also be included.”

Rule 5.4.2.8 states: “Where any research article or manuscript and/or internationally examined patent is used for the purpose of a thesis in article format to which other authors and/or inventors than the candidate contributed, the candidate must obtain a written statement from each co-author and/or co-inventor in which it is stated that such co-author and/or co-inventor grants permission that the research article or manuscript and/or patent may be used for the stated purpose and in which it is further indicated what each co-author's and/or co-inventor's share in the relevant research article or manuscript and/or patent was.”

Rule 5.4.2.9 states: “Where co-authors or co-inventors as referred to in 5.4.2.8 above were involved, the candidate must mention that fact in the preface and must include the statement of each co-author or co-inventor in the thesis immediately following the preface.”

Styles of numbering and referencing

It should be noted that the formatting, style of referencing, figure and table numbering and general outline of the four original articles, as required by the editors of the publications, were retained. No modifications to the original texts (apart from minor spelling or typographical errors) of the papers were made because the three of the four of these had already been peer-reviewed and accepted for publication, the fourth paper had been submitted for review. Two of the papers have already appeared in print and is available online. The cover page of these papers was included at the beginning of each paper.

For clarity, all references used in all of the papers were listed again at the end of the thesis in the correct style, according to the guidelines of this University.

View of the faculty of engineering of the North West University on article based PhDs

From the minutes of the post graduate faculty management committee meeting held on 13 June 2012:

“Die voorstel word goedgekeur dat drie geakkrediteerde joernalartikels waarvan 2 aanvaar is vir publikasie en een reeds ingedien is, as genoegsaam beskou word om 'n artikelgebaseerde PhD in te handig vir eksaminering.”

Translation from Afrikaans to English:

“The proposal was approved that three accredited journal articles of which 2 are already accepted for publication and a third already submitted, is considered sufficient for an article based PhD to hand in for examination.”

Statements from co-authors

Contributions from the following co-authors are recognised, and their statements follow:

D.R. Nicholls (page vii)

A.S.J. Helberg (page viii)

E.J. Mulder (page ix)

Statement of consent: D.R. Nicholls

To whom it may concern,

I, David Richard Nicholls, give my consent to Anthonie Christoffel Cilliers, candidate for the degree Philosophiae Doctor in Nuclear Engineering at the North-West University, to include in his thesis entitled: A deterministic approach for establishing a narrow band dynamic operating envelope to detect and locate hardware deterioration in nuclear power plants, the following publication, of which I am a co-author:

Cilliers, A.C., Nicholls, D., Helberg, A.S.J., 2011. Fault detection and characterisation in Pressurised Water Reactors using real-time simulations, *Annals of Nuclear Energy*. 38, 1196-1205.

The relative contributions to the paper by the different authors are given in Chapter 3. This statement serves to comply with academic rules 5.4.2.8 and 5.4.2.9 of the University.

Signed at Sunninghill on _____.

D.R. Nicholls

Statement of consent: A.S.J. Helberg

To whom it may concern,

I, Albert S J Helberg, give my consent to Anthonie Christoffel Cilliers, candidate for the degree Philosophiae Doctor in Nuclear Engineering at the North-West University, to include in his thesis entitled: A deterministic approach for establishing a narrow band dynamic operating envelope to detect and locate hardware deterioration in nuclear power plants, the following publication, of which I am a co-author:

Cilliers, A.C., Nicholls, D., Helberg, A.S.J., 2011. Fault detection and characterisation in Pressurised Water Reactors using real-time simulations, *Annals of Nuclear Energy*. 38, 1196-1205.

The relative contributions to the paper by the different authors are given in Chapter 3. This statement serves to comply with academic rules 5.4.2.8 and 5.4.2.9 of the University.

Signed at Potchefstroom on _____.

A.S.J. Helberg

Statement of consent: E.J. Mulder

To whom it may concern,

I, Eben J Mulder, give my consent to Anthonie Christoffel Cilliers, candidate for the degree Philosophiae Doctor in Nuclear Engineering at the North-West University, to include in his thesis entitled: A deterministic approach for establishing a narrow band dynamic operating envelope to detect and locate hardware deterioration in nuclear power plants, the following publication, of which I am a co-author:

Cilliers, A.C., Mulder, E., 2012. Adapting plant measurement data to improve hardware fault detection performance in Pressurised Water Reactors. *Annals of Nuclear Energy*. 49, 81-87.

The relative contributions to the paper by the different authors are given in Chapter 4. This statement serves to comply with academic rules 5.4.2.8 and 5.4.2.9 of the University.

Signed at Potchefstroom on _____.

E.J. Mulder

List of Publications

The publications presented in this thesis in accordance with rule 5.4.2.8, are:

Journal articles (peer-reviewed)

Cilliers, A.C., Nicholls, D., Helberg, A.S.J., 2011. Fault detection and characterisation in Pressurised Water Reactors using real-time simulations, *Annals of Nuclear Energy*. 38, 1196-1205.

Cilliers, A.C., Mulder, E., 2012. Adapting plant measurement data to improve hardware fault detection performance in Pressurised Water Reactors. *Annals of Nuclear Energy*, 49, 81-87.

Cilliers, A.C., 2013. Correlating hardware fault detection information from distributed control systems to isolate and diagnose a fault in Pressurised Water Reactors. *Annals of Nuclear Energy*. 54, 91-103.

Cilliers, A.C., 2013. Benchmarking an expert fault detection and diagnostic system on the Three Mile Island accident event sequence. *Annals of Nuclear Energy*, under review.

Guidelines of “Annals of Nuclear Energy”

In accordance to the rule 5.4.2.7 the guidelines to authors to Annals of Nuclear Energy states:

“Annals of Nuclear Energy provides an international medium for the communication of original research, ideas and developments in the field of nuclear energy. In particular, its scope includes reactor physics of all types, fuel management, radioactive waste disposal, environmental effects, safety, siting and economics of reactors. There should be strong links to the physics of the problem in the areas of thermal hydraulics, and in nuclear fusion the Editors would consider blanket studies. Specific areas the Editors would not consider are the magnetic or laser aspects of fusion reactors, and chemical reprocessing of nuclear fuel. Occasionally the Editors will accept review articles of a subject of special current interest.

In addition to Technical Papers, the Editors will also consider short papers describing intermediate results of continuing investigations, which are of interest but possibly incomplete or tentative. Such papers will be called Technical Notes. Authors should state whether they wish their manuscript to be considered under this heading.”

For acceptance, the submitted paper is evaluated according to the following:

“Originality:

Is the article sufficiently novel and interesting to warrant publication? Does it add to the canon of knowledge? Does the article adhere to the journal's standards? Is the research question an important one? In order to determine its originality and appropriateness for the journal, it might be helpful to think of the research in terms of what percentile it is in? Is it in the top 25% of papers in this field? You might wish to do a quick literature search using tools such as Scopus to see if there are any reviews of the area. If the research has been covered previously, pass on references of those works to the editor.

Structure:

Is the article clearly laid out? Are all the key elements (where relevant) present: abstract, introduction, methodology, results, conclusions? Consider each element in turn:

- Title: Does it clearly describe the article?
- Abstract: Does it reflect the content of the article?
 - Where graphical abstracts and/or highlights are included, please check the content and if possible make suggestions for improvements. Follow these links for more information on graphical abstracts and highlights.
- Introduction: Does it describe what the author hoped to achieve accurately, and clearly state the problem being investigated? Normally, the introduction should summarize relevant research to provide context, and explain what other authors' findings, if any, are being challenged or extended. It should describe the experiment, the hypothesis(es) and the general experimental design or method.
- Method: Does the author accurately explain how the data was collected? Is the design suitable for answering the question posed? Is there sufficient information present for you to replicate the research? Does the article identify the procedures followed? Are these ordered in a meaningful way? If the methods are new, are they explained in detail? Was the sampling appropriate? Have

the equipment and materials been adequately described? Does the article make it clear what type of data was recorded; has the author been precise in describing measurements?

- **Results:** This is where the author/s should explain in words what he/she discovered in the research. It should be clearly laid out and in a logical sequence. You will need to consider if the appropriate analysis has been conducted. Are the statistics correct? If you are not comfortable with statistics, please advise the editor when you submit your report. Interpretation of results should not be included in this section.
- **Conclusion/Discussion:** Are the claims in this section supported by the results, do they seem reasonable? Have the authors indicated how the results relate to expectations and to earlier research? Does the article support or contradict previous theories? Does the conclusion explain how the research has moved the body of scientific knowledge forward?
- **Language:** If an article is poorly written due to grammatical errors, while it may make it more difficult to understand the science, you do not need to correct the English. You should bring this to the attention of the editor, however.

Finally, on balance, when considering the whole article, do the figures and tables inform the reader, are they an important part of the story? Do the figures describe the data accurately? Are they consistent, e.g. bars in charts are the same width, the scales on the axis are logical.

Previous Research:

If the article builds upon previous research does it reference that work appropriately? Are there any important works that have been omitted? Are the references accurate?

Ethical Issues:

- **Plagiarism:** If you suspect that an article is a substantial copy of another work, please let the editor know, citing the previous work in as much detail as possible.
- **Fraud:** It is very difficult to detect the determined fraudster, but if you suspect the results in an article to be untrue, discuss it with the editor
- **Other ethical concerns:** For medical research, has confidentiality been maintained? Has there been a violation of the accepted norms in the ethical treatment of animal or human subjects? If so, then these should also be identified to the editor.”

Elsevier publishing rights and responsibilities

“Copyright

Intellectual property, in particular copyright (rights in editorial content), trademarks (rights in brands for services or journals), and database rights (rights in compilations of information), form the foundation of Elsevier’s publishing services and communications businesses. We in Elsevier embrace the opportunities the digital environment offers for communication and access, while at the same time we recognize the new risks that this environment poses, that being the ease with which unauthorized copies can be made and distributed worldwide.

Our objective

We aim to manage digital rights and brands amidst the structural changes that the “information society” represents, while at the same time recognizing the shared goals we have with our customers and authors. These include providing the widest possible distribution of scientific and medical content and services in a financially sustainable business model.

Elsevier wants to ensure a proper balance between the scholarly rights which authors retain (or are granted/transferred back in some cases) and the rights granted to Elsevier that are necessary to support our mix of business models. We routinely analyse and modify our policies to ensure we are responding to authors’ needs and concerns, and to the concerns in general of the research and scholarly communities.

What rights do I retain as a journal author*?

- the right to make copies (print or electronic) of the journal article for your own personal use, including for your own classroom teaching use;
- the right to make copies and distribute copies of the journal article (including via e-mail) to research colleagues, for personal use by such colleagues for scholarly purposes*;
- the right to post a pre-print version of the journal article on Internet websites including electronic pre-print servers, and to retain indefinitely such version on such servers or sites for scholarly purposes* (with some exceptions such as The Lancet and Cell Press.
- the right to post a revised personal version of the text of the final journal article (to reflect changes made in the peer review process) on your personal or institutional website or server for scholarly purposes*, incorporating the complete citation and with a link to the Digital Object Identifier (DOI) of the article (but not in subject-oriented or centralized repositories or institutional repositories with mandates for systematic postings unless there is a specific agreement with the publisher for further information);
- the right to present the journal article at a meeting or conference and to distribute copies of such paper or article to the delegates attending the meeting;
- for your employer, if the journal article is a ‘work for hire’, made within the scope of the author’s employment, the right to use all or part of the information in (any version of) the journal article for other intra-company use (e.g. training);
- patent and trademark rights and rights to any process or procedure described in the journal article;
- **the right to include the journal article, in full or in part, in a thesis or dissertation;**
- the right to use the journal article or any part thereof in a printed compilation of your works, such as collected writings or lecture notes (subsequent to publication of the article in the journal); and

- the right to prepare other derivative works, to extend the journal article into book-length form, or to otherwise re-use portions or excerpts in other works, with full acknowledgement of its original publication in the journal.

***Commercial purposes and systematic distribution**

Authors of Elsevier-published articles may use them only for scholarly purposes as set out above and may not use or post them for commercial purposes or under policies or other mechanisms designed to aggregate and openly disseminate manuscripts or articles or to substitute for journal-provided services. This includes the use or posting of articles for commercial gain or to substitute for the services provided directly by the journal including the posting by companies of their employee-authored works for use by customers of such companies (e.g. pharmaceutical companies and physician-prescribers); commercial exploitation such as directly associating advertising with such postings; the charging of fees for document delivery or access; the systematic distribution to others via e-mail lists or list servers (to parties other than known colleagues), whether for a fee or for free; the posting of links to sponsored articles by commercial third parties including pharmaceutical companies; institutional, funding body or government manuscript posting policies or mandates that aim to aggregate and openly distribute the accepted, peer reviewed manuscripts or published journal articles authored by its researchers or funded researchers; and subject repositories that aim to aggregate and openly distribute accepted peer reviewed manuscripts or published journal articles authored by researchers in specific subject areas.”

Abstract

Being able to detect and describe hardware deterioration in nuclear power plants benefits the nuclear industry tremendously as it would enable appropriate outage and maintenance planning. Being able to detect and describe this faulty behaviour also assists in fault analysis of nuclear power plants.

This thesis describes the development of narrow band dynamic operating envelope that makes use of real-time simulated plant measurements and control operations to compare with actual plant measurements and control operations. By simulating the plant behaviour in real-time whilst comparing it with the real-time transient the plant is following, a second set of plant measurements is generated. The newly generated plant measurements represent plant measurements if the control system did not introduce control operations to nullify the effect of the fault.

This enables the calculation of the unknown disturbance introduced into the plant as a fault condition. The benefit of such a system is that plant faults that are too small to detect (especially during transients when the plant operating point is moving around) can be identified.

The behaviour of the control system is also continuously predicted so the effect of the control system compensating for fault effects (which in most cases hides the fault condition) is used to characterise the fault condition in terms of magnitude, position and subsystem being affected. The combination of the fault detection and fault characterisations produces a complete fault identification system.

The approach is verified by making use of an implementation of the fault identification system on a simulated plant. Typical faults (small enough to go undetected for an extended period of time during a typical transient) are introduced into the virtual plant and continuously compared with another plant simulation, producing the same transient without the introduction of the fault. A comparison is done to evaluate the speed and detail provided by the fault identification system as opposed to the conventional plant protection system. Using the described methodology, the fault is detected and characterised before plant design limitations are reached or the fault is detected by the conventional protection system.

In addition to the fault identification system, this research develops the functional requirements for a full scope engineering and training simulator that would allow the simulator to be fully utilised to simulate postulated accident scenarios, plan plant modification procedures as well as provide an in-transient real time reference for plant diagnostic systems.

To ensure practical implementation of the system in the regulated nuclear industry, an implementation framework that keeps the conventional plant protection system intact, is created. It allows the implementation of narrow band dynamic operating envelope operating within the conventional operating envelope. The framework allows the implementation of the developed fault identification system and other plant diagnostic systems on existing nuclear power plants without impacting on existing nuclear power plant licences as well as the licensing process of new nuclear power plants.

Acknowledgements

In January 2008 the research contained in this thesis started, and in the same month I also married Joe-Nimique. During the last 5 years, the research, new path in our careers and life together has taken us on a journey with many challenges and triumphs. Thank you, Joe-Nimique for the support, the listening, advice and the overall confidence you had in me to make a success of this project. On 5 October 2011 our baby boy Wilhelm was born. Wilhelm, thank you for the smiles, the hugs and the love, and for reminding me what is important in life.

I would like to thank all my friends who supported me with encouragement that made me believe in myself and in the project.

To my Manager and mentor David Nicholls at Eskom Nuclear, I would like to extend a word of gratitude for the opportunity to take on the research project, the sessions of advice on the project and on my career as well as the overall managing style which enabled me to work as productively as possible while developing as a professional and academic – it made all the difference. Thank you.

Prof Eben Mulder, my promoter, thank you for the support and advice and for believing in me when it counted. Prof Albert Helberg, who contributed a lot of wisdom and advice throughout the course of this research, thank you very much.

Lastly I need to mention that Joe-Nimique and I were thoroughly blessed in our careers and personal life over the past 5 years, and for that I thank our Heavenly Father, all glory belongs to You.

Table of Contents

Declaration.....	i
Preface	ii
Format of this thesis.....	ii
Styles of numbering and referencing	ii
View of the faculty of engineering of the North West University on article based PhDs	ii
Statements from co-authors	iv
Statement of consent: D.R. Nicholls.....	v
Statement of consent: A.S.J. Helberg	vi
Statement of consent: E.J. Mulder	vii
List of Publications	viii
Journal articles (peer-reviewed).....	viii
Guidelines of “Annals of Nuclear Energy”	ix
Elsevier publishing rights and responsibilities.....	xi
Abstract.....	xiii
Acknowledgements.....	xiv
1. Introduction.....	1
1.1. Problem statement	1
1.2. Research objectives	1
1.3. Conventional and proposed operating envelope.....	2
1.4. Original contributions.....	3
1.5. Thesis layout.....	5
2. Literature analysis.....	7
2.1. Dynamic reference model.....	7
2.2. Closed-loop control system fault masking	10
2.3. Fault characterisation.....	11
2.4. Summary and conclusions	13
3. Article 1: Fault detection and characterisation in Pressurised Water Reactors using real-time simulations	15
3.1. Relative contributions by authors	15
Fault detection and characterisation in Pressurised Water Reactors using real-time simulations	17
ABSTRACT.....	17
1. Introduction	17
2. PWR simulation accuracy	18
3. The PWR primary circuit control system.....	19

3.1.	Pressuriser pressure control.....	20
3.2.	Pressuriser level control	21
3.3.	Average temperature control	22
4.	Implementation of proposed fault detection and characterisation system.....	24
5.	Fault detection system functional proof	27
6.	Proposed control room implementation	29
7.	Conclusion.....	31
8.	References	31
3.2.	Additional notes.....	32
3.2.1.	Modelling and simulation needs for advanced nuclear energy systems.....	32
3.2.2.	Nuclear plant simulator requirements for fault identification	33
3.2.3.	Conclusion.....	36
4.	Article 2: Adapting plant measurement data to improve hardware fault detection performance in Pressurised Water Reactors.....	37
4.1.	Relative contributions by authors	37
	Adapting plant measurement data to improve hardware fault detection performance in Pressurised Water Reactors.....	39
	ABSTRACT.....	39
1.	Introduction	39
2.	Fault masking by the control system	41
3.	Measurement adaptation process.....	43
4.	Reintroducing the fault information into the measurement data	46
5.	In-transient fault example.....	47
6.	Inaccuracies in the plant model or measurement equipment.....	48
7.	Conclusion.....	49
8.	References	50
4.2.	Additional notes.....	52
4.2.1.	Deriving the plant process from the simulator	52
4.2.2.	Conclusion.....	55
5.	Article 3: Correlating hardware fault detection information from distributed control systems to isolate and diagnose a fault in Pressurised Water Reactors.	56
	Correlating hardware fault detection information from distributed control systems to isolate and diagnose a fault in pressurised water reactors.....	58
	ABSTRACT.....	58
1.	Introduction	58
2.	Fault characterisation.....	61
3.	Conventional and adapted operating envelope	62

4.	Plant fault diagnosis	63
4.1.	Fault diagnosis examples.....	64
4.2.	Loss of coolant accident	65
4.3.	Steam generator tube rupture.....	71
5.	Conclusion.....	76
6.	References	77
5.1.	Additional notes.....	79
5.1.1.	Conclusion.....	79
6.	Article 4: Benchmarking an expert fault detection and diagnostic system on the Three Mile Island accident event sequence.	80
	Benchmarking an expert fault detection and diagnostic system on the Three Mile Island accident event sequence.	81
	ABSTRACT.....	81
1.	Introduction	81
2.	The TMI accident sequence of events	82
3.	Cause 1: Feedwater supply block to Steam Generator	84
4.	Cause 2: Power-operated relief valve failure	86
5.	Summary and conclusions	91
6.	References	91
6.1.	Additonal notes.....	92
6.1.1.	Conclusion.....	92
7.	Conclusion	93
7.1.	Introduction	93
7.2.	Conclusions	94
7.3.	Simulation-based fault detection system	94
7.4.	Fault characterisation method.....	95
7.5.	Control and protection implementation framework	96
7.6.	Recommendations for future research.....	96
8.	Bibliography	98
A.	Appendix.....	100
A.1.	General nuclear plant control and protection systems.....	100
A.2.	The protection operating window of a pressurised water reactor.....	100
A.3.	The PWR primary circuit control system	103
A.4.	Power control.....	106
A.5.	Average temperature control	106
A.6.	Rod cluster control system	109

A.7.	Pressuriser control	109
A.8.	Steam pressure control	115
A.9.	Steam generator level control	116
A.10.	Condenser level control	116
A.11.	Generator voltage control	117
A.12.	Safety Functions	117
A.13.	Instrumentation and transmission accuracies	119
A.14.	Summary and conclusions	120
B.	Appendix.....	121
B.1.	Implementation.....	121
B.2.	Power control PDS	123
B.3.	Pressuriser level control PDS	126
B.4.	Pressuriser pressure control PDS.....	128
B.5.	Steam generator control PDS	130
B.6.	Accounting for inaccuracies and time delays in the system implementation.....	133
B.7.	Simulator and plant synchronisation	133
B.8.	Summary and conclusions	134
C.	Appendix.....	135
C.1	Additional reference faults	135
C.1.1.	Steam line break inside containment	135
C.1.2.	Steam line break outside containment	140

List of Figures

Fig. 1-1. Typical operating envelope of a PWR.....	2
Fig. 1-2. Proposed dynamic operating envelope.....	3
Fig. 1-3. Original contribution knowledge pillars.....	5

Article 1

Fig. 1. Pressuriser pressure and level control.....	20
Fig. 2. Pressuriser pressure control diagram.....	21
Fig. 3. Pressuriser level control diagram.....	22
Fig. 4. Average temperature control.....	23
Fig. 5. Average temperature control diagram.....	23
Fig. 6. System for comparing real and simulated measurements and control parameters.....	24
Fig. 7. No Fault 100% power to 80% power pressure transient.....	25
Fig. 8. No Fault 100% power to 80% power pressuriser level transient.....	26
Fig. 9. No Fault 100% power to 80% power nuclear power transient.....	26
Fig. 10. Pressuriser pressure – measured, simulated and effective.....	27
Fig. 11. Reactor Coolant System Volume - measured, simulated and effective.....	28
Fig. 12. The control system response to a small loss of coolant fault.....	29
Fig. 13. Adapted control and protection schematic.....	30

Article 2

Fig. 1. Open-loop system.....	42
Fig. 2. Closed-loop control system.....	42
Fig. 3. Fault identification control diagram.....	44
Fig. 4. Unmasked measurement generation diagram.....	46
Fig. 5. In-transient pressure measurement and adapted measurement.....	48
Fig. 6. Multiplication factor for changing values of $C(s)P_p(s)S_p(s)$ due to inaccuracy.....	49

Additional notes

Fig. 4-1. Pressure control block diagram.....	52
Fig. 4-2. Pressuriser heater effect on pressure in time.....	53
Fig. 4-3. Pressuriser heater power effect on pressure change rate.....	53

Article 3

Fig. 1. Temperature – Pressure operating envelope.....	62
--	----

Fig. 2. RCS pressure and heater operation.....	66
Fig. 3. RCS pressure and percentage difference.....	67
Fig. 4. RCS average temperature.....	68
Fig. 5. Pressuriser level and residual inflow.....	68
Fig. 6. RCS coolant volume.....	69
Fig. 7. Unexpected flow and introduced fault flow.....	69
Fig. 8. Containment pressure.....	70
Fig. 9. RCS pressure and heater operation.....	72
Fig. 10. RCS pressure and percentage difference.....	73
Fig. 11. RCS average temperature.....	73
Fig. 12. Pressuriser level and residual inflow.....	74
Fig. 13. RCS volume.....	74
Fig. 14. Steam generator level and inflow.....	75
Fig. 15. Primary and secondary flow compensation for fault.....	75

Article 4

Fig. 1. Three Mile Island faulty valves (Cause 1).....	83
Fig. 2. Three Mile Island faulty valves (Cause 2).....	84
Fig. 3. Pressuriser level and feed flow.....	85
Fig. 4. RCS pressure and spray.....	85
Fig. 5. SG pressure and level.....	86
Fig. 6. RCS pressure.....	88
Fig. 7. Actual and expected pressure difference.....	88
Fig. 8. Pressuriser level and residual inflow.....	89
Fig. 9. RCS volume.....	90
Fig. 10. Flow out of open PORV.....	90

Apendix A

Fig.A-1. Overtemperature and overpower ΔT protection (Koeberg, 1997).....	102
Fig.A-2. Pressure temperature curve for pressure protection.....	103
Fig.A-3. PWR general control schematic (Koeberg, 1997).....	105
Fig.A-4. Average temperature control.....	106
Fig.A-5. Average temperature control diagram.....	108
Fig.A-6. Pressuriser pressure and level control.....	110
Fig.A-7. Pressuriser pressure control diagram.....	112
Fig.A-8. Pressuriser level control diagram.....	114

Fig. A-9. Steam generator with related controls.....	115
Fig. A-10. Multiplication factor for maximum instrumentation errors.....	120

Appendix B

Fig.B-1. Full PDS implementation.....	122
Fig.B-11. Reactor temperature control with PDS.....	124
Fig.B-12. Power control schematic with PDS.....	125
Fig.B-13. Pressure and level control with PDS.....	127
Fig.B-14. Pressuriser level control schematic with PDS.....	128
Fig.B-15. Pressure control schematic with PDS.....	129
Fig.B-16. Steam generator control.....	131
Fig.B-17. Steam generator controls with PDS.....	132

Appendix C

Fig.C-1. RCS pressure and heater operation.....	136
Fig.C-2. Secondary pressure.....	137
Fig.C-3. Steam generator flow.....	137
Fig.C-4. Steam generator level.....	138
Fig.C-5. Steam line break size.....	139
Fig.C-6. RCS pressure and heater operation.....	141
Fig.C-7. Secondary pressure.....	141
Fig.C-8. Steam generator level and inflow.....	142

List of Tables

Article 3

Tab. 1. Fault groups with initiating measurements.....	64
Tab. 2. Loss of coolant accident configuration.....	65
Tab. 3. Loss of coolant accident diagnostic system results.....	70
Tab. 4. SG tube rupture configuration.....	71
Tab. 5. SG tube rupture accident diagnostic system results.....	76

Article 4

Tab. 1. Three Mile Island accident configuration.....	87
---	----

Appendix A

Tab.A.1. Trip set points and time delays of a reference PWR (Koeberg, 1997).....	100
Tab.A.2. Fault groups with initiating measurements.....	118
Tab.A.3 Instrumentation accuracies.....	119

Appendix C

Tab.C.1. Steam line break configuration.....	135
Tab.C.2. Steam line break accident PDS results.....	139
Tab.C.3. Steam line break configuration.....	140
Tab.C.4. Steam line break accident PDS results.....	143

Definitions

Fault identification:	The complete process of fault detection and characterising the fault to describe the location, magnitude and source of the fault.
Fault detection:	Detecting the existence of an abnormal and unexpected disturbance in the system.
Fault characterisation:	Describing the nature, magnitude, position and/or cause of abnormal or unexpected disturbance in the system.
Dependability:	The ability to respond to faulty operation in a correct and timely manner.
Sensitivity:	The combination of accuracy, precision, and resolution when identifying faults.
Speed:	The time it takes to detect, characterise and clear a fault condition in a system.
Security:	The confidence in the protection system decision - the ability of not reacting to false alarms whilst acting quickly for true faults.
Transient:	Transient as referred to in this thesis is the period in which the plant is in transition between operational modes.

General notation

Eskom	Eskom (Pty.) Ltd
PCTran	PCTran®

Acronyms

ALARA	As low as reasonably attainable
ANN	Artificial neural networks
CANDU	Canadian deuterium uranium
CUSUM	Cumulative summation
D3	Diversity and Defence-in-Depth
DNBR	Departure from nucleate boiling ratio
DNNA	Dynamic neural network aggregation
DPPS	Digital plant protection system
EKF	Extended Kalman Filter
FDC	Fault detection and characterisation
FDD	Fault detection and diagnosis
FDI	Fault detection and isolation
FDS	Fault diagnostic system
GBPC	Gas cycle bypass control valve
GEN II	Generation II
HMI	Human machine interface
HP	High pressure
HPI	High-pressure injection
HTGR	High temperature gas-cooled reactor
HV	High voltage
I&C	Instrumentation & Control (sometimes referred to as C&I)
IAEA	International Atomic Energy Agency
ICS	Inventory control system
IPB	Rod cluster position monitoring system
LHSI	Low head safety injection
LOCA	Loss of coolant accident
LP	Low pressure
LPC	Low-pressure compressor

MFC	Model feedback control
MPS	Main power system
MRAC	Model reference adaptive control
MS	Main steam
NF	Neuro-fuzzy
NNR	National Nuclear Regulator
NPP	Nuclear power plant
NRC	Nuclear Regulatory Commission
OLM	Online monitoring
PBMR	Pebble bed modular reactor
PCA	Principal component analysis
PCDA	Plant control and diverse actuation
PCU	Power conversion unit
PDS	Plant diagnostic system
PFD	Probability of failure on demand
PI	Proportional and integral
PI+D	Proportional-integral and derivative
P_n	Unit-rated power
PORV	Power-operated relief valve
PPB	Primary pressure boundary
PRA	Probabilistic risk assessment
PRBFN	Probabilistic radial basis function network
PT	Power turbine
PWR	Pressurised water reactor
RBF	Radial basis function
RCCA	Rod cluster control assembly
RHR	Residual heat removal
RPSA	Reactor protection and safeguard actuation
RCS	Reactor coolant system
RCS	Reactor chemical and volume control system
RLS	Recursive least squares
ROT	Reactor outlet temperature
R_x	Receive
SCRAM	Safety control rod axe man (emergency trip by dropping safety control rods into the core)

	and initiating safety actuating systems)
SG	Steam generator
SGTR	Steam generator tube rupture
SLB	Steam line break
SVM	Support vector machine
TMI	Three Mile Island
Tx	Transmit
URS	User requirement specification
UTSG	U-tube steam generator
V&V	Verification and validation

1. Introduction

This thesis contains a collection of four accredited journal articles published or submitted for publication over the last five years on the topic of fault identification in nuclear power plants. These papers cover a range of related topics, from the fundamentals of fault detection in nuclear power plants, fault identification development, system implementation architecture, to finally benchmarking the developed system using the Three Mile Island accident scenario. Chapter 1 introduces the research and principles the novel fault identification method is built on.

1.1. Problem statement

Nuclear plant protection systems creates an operating envelope around the operating point large enough to allow changes in the operating point due to expected transients. Hardware failures with effects too small to move the operating point outside the operating envelope goes undetected.

Implementing a dynamic operating envelope around the operating point to allow early fault detection during transient operation in nuclear power plants is problematic due to the absence of a reliable dynamic reference to compare plant measurements with during transients. Often heuristic methods are used to create a dynamic operating envelope. This, in its nature is problematic to implement in the nuclear industry due to the uncertainty it introduces into the system.

The distributed application of control systems operating independently to keep the plant operating within the safe operating envelope boundaries complicates the problem since the control systems would not only operate to reduce the effect of transient disturbances but fault disturbances as well.

Implementing expert fault detection methods in new or existing nuclear power plants is problematic due to the strict regulatory requirements in the nuclear industry.

1.2. Research objectives

The goal of the research is to develop a dynamic operating window that allows improved protection dependability in nuclear power plants. The method should then be developed further to provide fault characterisation that would otherwise go undetected and undefined for long periods. The system is developed to be effective during steady-state and transient conditions.

The main objectives of the research are:

1. Develop an early fault detection system making use of a real-time simulator model of the nuclear power plant as a dynamic reference, continuously monitoring and comparing simulated measurement data and control outputs of the plant model with the actual measured data and

control outputs from the plant. The fault detection system should detect small faults that would normally go undetected as well as detect faults during plant operating transients.

2. Develop a fault characterisation method, making use of measured and simulated data together with the actual and simulated control system response. The fault characterisation system should provide information on the magnitude and location of the fault.
3. Develop a control and protection framework that allows nuclear power plant licensing within the existing licensing framework, but is still able to uncover the benefits of expert control and protection systems.

1.3. Conventional and proposed operating envelope

In Fig. 1-1 a typical conventional operating envelope is depicted, a load change transient causes the 100% steady state operating point to move to a new steady state position following a path of large pressure and temperature changes. The static operating envelope is specified large enough to accommodate the various possible operating points as well as the paths that are followed during transient states. The result is that hardware degradation or failures that do not cause large enough changes in the operating point will go undetected until developed to an extent where the plant integrity is under threat, only then the fault will be detected and a trip will be issued. In such a case an emergency shutdown procedure includes the actuation of safety features that results in extended downtime periods and costly start up procedures.

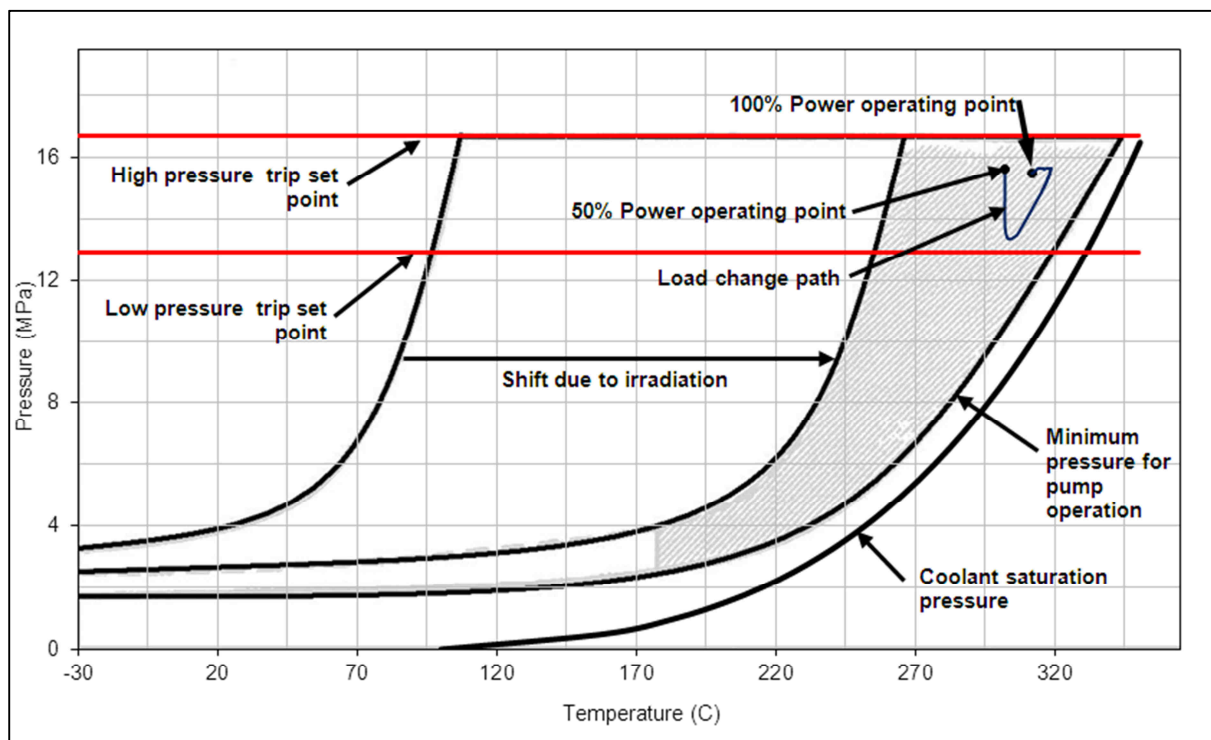


Fig. 1-1. Typical operating envelope of a PWR

The proposed solution depicted in Fig. 1-2 is the development of a dynamic operating envelope around the operating point, moving with anticipated changes in the operating point. Should any

unanticipated changes result in a movement of the operating point, the operating point will move outside the dynamic operating envelope indicating a fault condition. This will happen whilst all plant parameters remain well within the safe operating region of the plant.

To establish a dynamic operating envelope a dynamic reference is required that can anticipate operating changes in the plant. This is achieved by implementing a full scope plant simulator code to run in real time in parallel with the plant while receiving all external inputs from the control room that the plant receives. All changes in the plant operations would thus be mirrored by the plant simulator, and so, the simulated and measured operating point will move together through operational changes. If any unexpected disturbance such a component failure or component operations deteriorate to outside the accepted tolerance, the operating point will move outside the dynamic operating envelope and signal a fault condition.

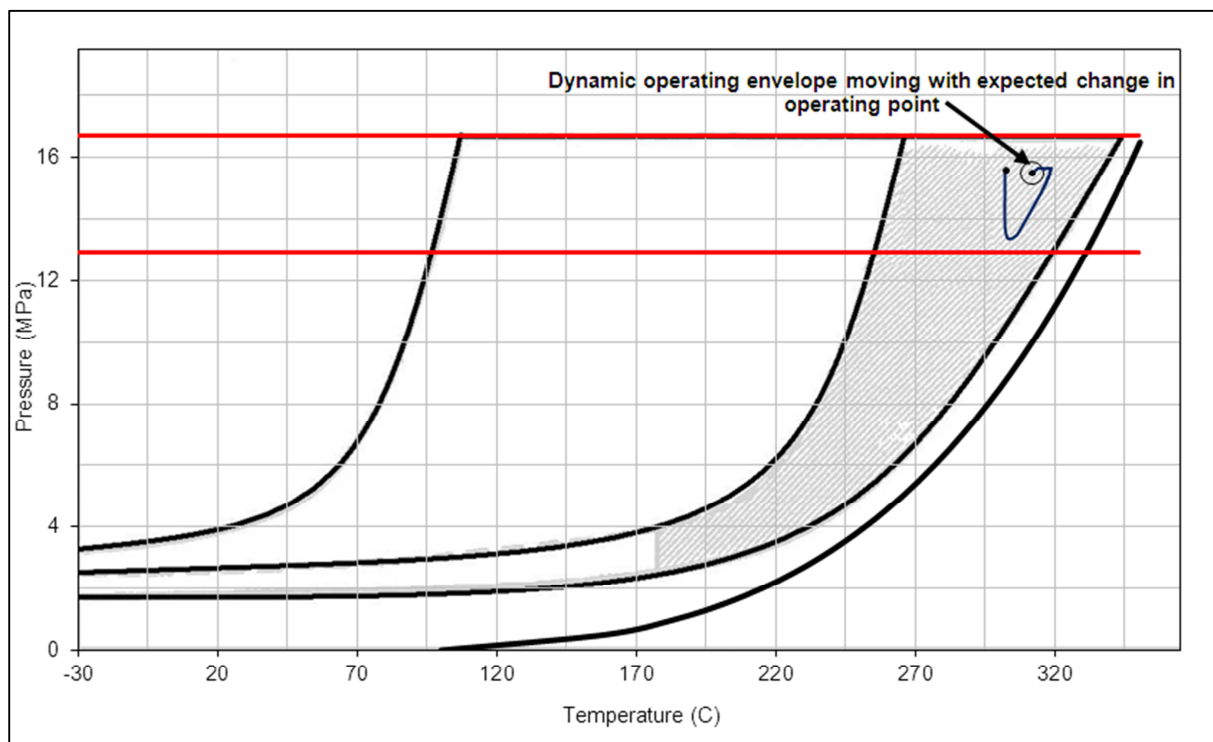


Fig. 1-2. Proposed dynamic operating envelope

1.4. Original contributions

The main scientific contributions of the thesis are summarised as follows:

- A novel deterministic approach to establish a dynamic operating window around the operating point to detect faulty plant operations as soon as it occurs. The faulty plant behaviour is also characterised and the cause of the fault is described.
- The conventional control and protection architecture is adapted to allow for the introduction of fault identification and data analysis systems that will improve system dependability without

additional risk to the protection system integrity and without impacting the licence or licensing process of the plant.

The approach to detect and characterise faulty hardware in nuclear power plants relies on a knowledge base from varying disciplines as depicted in Fig. 1-3:

- Plant simulation and modelling is used to provide a dynamic reference to compare the plant operations with, but also in providing reference control inputs, to isolate fault information from expected transient information in the plant.
- As all changes on plant operations, whether from an expected external input or due to faulty equipment, are controlled or mitigated by the plant control systems, utilising these systems and the fundamental theories they rely on is required to detect small faults or equipment deterioration.
- Conventional plant protection systems rely on static operating envelopes in various systems if any operating variable cross the boundary of the operating envelope. By this time the plant is already at the limits of the structural integrity and a SCRAM and safety actuation process is initiated. The safety system that responds to the system depends on the operating envelope that detected the fault. Many of the principles used to decide on which safety system to initiate is of interest as describes in some way the nature of the fault and remains applicable in a dynamic operating envelope.
- All protection and control systems in nuclear plants are implemented according to specific implementation architecture. The architecture comprises various system philosophies that will determine how information is shared between systems as well as establishing a hierarchy of system importance. Conventional control and protection implementations architecture were designed keep control and protection functions completely separate. Modern control and protection implementation architectures attempted to share information between these functions resulting in licencing difficulties. In order to allow expert fault identification systems to be implemented in existing and new nuclear power plants, novel implementation architecture is required building on lessons learned and strengths of conventional architectures.

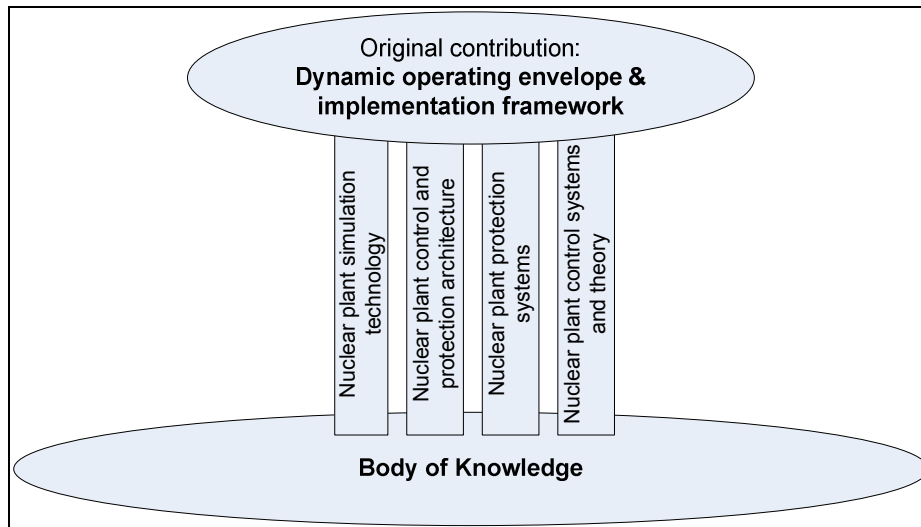


Fig. 1-3. Original contribution knowledge pillars

In the following chapters, the state of each of these pillars is examined together with recent advances in research of these fields. The original contribution described in this thesis will build upon this work.

1.5. Thesis layout

Chapter 3 to Chapter 6 consists of peer reviewed articles that examines the pillars used to build the original contribution on, each pillar being studied in terms of recent research done in the field, technological advances and the applicability of using the gained knowledge as a tool in the development of a dynamic operating envelope. Specific problems associated with the application of the field in realising a dynamic operating envelope is identified to be solve, or disqualify the field as a supporting pillar.

In **Chapter 2** a study on existing and proposed fault detection and characterisation methods is done. In particular, fault identification research papers are selected that highlight the limitations and needs at the time of conducting this project. These papers provide a basis on which to develop the proposed fault identification system.

The research article in **Chapter 3** describes the principles when using a real-time plant simulators running in parallel with a nuclear plant to predict the control system behaviour and highlighting unexpected plant behaviour. The basis of the theory is established in this chapter together with preliminary results. The control and protection architecture for implementation is developed and the system requirements of a nuclear plant simulator that would enable the proposed system are described.

In the research article in **Chapter 4** the method to adapt plant measurements that isolates the control actions on the fault and re-introduces it into the measurement data, thereby improving plant diagnostic performance is described.

The research article in **Chapter 5** introduces the use of improved fault detection information received from all distributed systems in the plant control system and correlating the information to not only detect the fault, but also to diagnose it based on the location and magnitude of the fault cause.

The final research article in **Chapter 6** makes use of the techniques and processes developed in the previous papers and apply it to a case study of the Three Mile Island nuclear power plant accident. In this way we can determine and showcase how the improved information available could present the operator with a better idea to the state of the plant during situations where a combination of faults and transients prevents the operator and conventional systems to recognise the abnormal behaviour.

2. Literature analysis

When proposing and developing a fault identification system a number of obstacles to effectively detect and characterise faults are encountered. These obstacles are not new, with various solutions proposed by researchers is shown in this chapter. The main obstacles are:

- providing a dynamic reference model with which to compare the plant during transients,
- extracting meaningful information when the plant outputs are compared with the reference, especially since changes caused by faults are masked by the control system operation, and
- characterising the detected fault by combining fault diagnostics information from a number of systems, each reacting differently to the same fault.

The nuclear industry is unique in the sense that it is highly regulated and strict requirements on the analytical proof of proposed systems' effectiveness are set. All nuclear plants are equipped with a full scope simulator that is able to simulate all expected plant transients. Because of these slight differences between the nuclear industry and other industries, unique solutions can be found to common obstacles highlighted by the following research topics.

2.1. Dynamic reference model

In order to detect abnormal operations in any plant, a reference with which to compare the measured outputs, is required. Various methods of implementing reference models exist. The conventional method used in nuclear power plants is that of a fixed reference for each operational mode. Should the plant measurements move beyond these fixed reference points, the plant's structural integrity is compromised and a trip signal is issued.

The use of dynamic reference models provides information on the abnormal behaviour of the plant while the plant measurements are still well within the safe operating range of the plant. In most cases a dynamic reference is realised by means of building a first principles model that represents the plant accurately within expected operating limits. Another effective way of providing a dynamic reference is making use of learning systems such as neural networks to learn the expected and unexpected plant operations and to distinguish between them. Each of these methods has different characteristics suitable for various fault detection applications.

Chen and Howell (2001) motivate their use of a combination of dynamic models and quantified modelling errors used in machine fault detection and diagnosis by stating that: "Although a lot of approaches have since been developed, none can be viewed as having general applicability." They state that learning methods are fast and do not require a plant model, but are comparatively brittle because they cannot handle situations that are not explicitly anticipated. The 'brittleness' referred to makes the implementation of heuristic methods particularly problematic in the nuclear industry where analytical proof of system dependability is required.

Chen and Howell (2001) also state that model-based techniques in comparison are less brittle, but pose other problems: “Most industrial chemical processes are unique, it is expensive to build high fidelity first principles models of these processes and very difficult to anticipate all the abnormal situations that might arise.” In contrast to this, the nuclear industry has been using plant simulators to aid training and design since the 1980s with on-going improvements in fidelity. This makes the use of high fidelity first principles models possible for use in fault detection techniques in the nuclear industry.

Embrechts et al. (2004) attempts to alleviate the associated brittleness problem with neural networks in the nuclear industry by making use of a hybrid neural network methodology. Since a feed-forward neural network trained with a back propagation algorithm that are frequently applied to model simulated nuclear power plant malfunctions presents a challenge to correctly identify unknown faults. The hybrid neural network they propose proves to correctly classify faults that have not been included in the simulator training model. They state that previous methods to identify nuclear power plant transients were based on time series data of various transient signals which relied mainly on rule based procedures to preselect proper combined groups of malfunctions. They trained various neural networks and used them to select the proper malfunction from an appropriate combination. The rules for combined network selection were generally driven by variables that were derived from the time series data. The drawback to their approach is that it takes a certain amount of time into the fault condition before the variables can be properly evaluated, causing a slower response time in the system.

Chen and Howell (2001) limited their system to the detection of abnormalities that occur during the functioning of complex operations such as those found in industrial processes. Their system does not do any characterisation of these abnormalities. Petersen and McFarlane (2004) define the requirements for process fault detection and diagnosis as the following:

- the availability of well defined, accurate first principles models (with any modelling errors also suitably represented),
- clearly identified fault modes and models to represent these, and
- appropriately located sensors (often with levels of redundancy).

We have found these requirements to also be generic requirements applicable to the fault identification system developed in this thesis.

Chen and Howell concentrated on the problem of fault detection only, in order to remove the requirement of fault modelling. Their methodology combines the use of dynamic models and quantified modelling errors used in machine fault detection and diagnosis with a data-driven approach to validate observed process dynamics. In this thesis the requirement of fault modelling is also removed by making use of the distributed configuration of the control systems used in nuclear power plants with each control system revealing different characteristics of the fault as it attempts to maintain the plant within the safe operating region.

The methodology used by Chen and Howell (2001) is based on the development of simple models via system identification methods, the estimation of the modelling errors likely to have occurred and the

application of model validation techniques with on-line data to determine whether a process abnormality has occurred. The methodology described in this thesis, on the other hand, is based on first principles models as dynamic reference.

Most of the methods making use of artificial neural networks to identify faults are all based on one single artificial neural network, rather than combined and/or rule-based networks as Embrechts (2004) proposed. The key advantages of their method are the avoidance of statistical rules and the potential for a faster and more reliable identification of the fault in question. Two different classes of artificial neural networks are compared in their study: those trained with raw time-series data (where the raw signals are deviations from steady state values and might include various drift phenomena), and those trained with Fourier transformed data.

In Embrechts' (2004) study, neural networks were trained for 20 distinct malfunctions where each distinct malfunction had a two-sample pattern, leading to a total of 40 training patterns. They used 29 malfunctions for testing where the last nine patterns were novel faults that were not encountered in the training set. The data were scaled between zero and one and a standard sigmoid function was used as transfer function. The neural network outputs for these malfunctions are categorized with 20 distinct output values. Depending on which transient occurs, a different output value is set to one, and all other outputs set to zero. For the faults in the test set that were not encountered in the training set, the so-called 'unlabelled faults,' all of the 20 output variables are set to zero. Various network configurations were tested. The most successful networks had two hidden layers and required a relatively large number of neurons (e.g., 35 and 25) in the hidden layers. The results were not sensitive to the choice of the network size as long as two hidden layers of neurons were retained and at least 25 neurons were present in each hidden layer. Training was halted as soon as all the malfunctions were recognised during the training phase and the reported least-squares error measure dropped below 0.02.

All test networks gave satisfactory results for the labelled transients. The unlabelled faults were not necessarily recognised, but where an unlabelled fault was confused with a labelled transient, the network selected a labelled fault that was closely related to the unlabelled fault.

In all mentioned cases the faults are detected and/or characterised during steady state conditions, where the only disturbance input into the system was that of the fault. Owing to the operation of the control system during operating transitions and expected transients, both neural networks and model-based fault detection systems find it difficult to isolate and identify the fault component in the transient. The problem is also encountered during steady-state conditions where the fault disturbance is of such a small magnitude that the closed-loop control system is able to return the operating point to the reference value and maintain this position for extended periods of time.

Hamelin and Sauter (2000) realised that most of the developed algorithms make many idealised assumptions such as steady state conditions which are very often not satisfied, since in reality the system parameters may either be uncertain or time dependent, resulting in a mismatch between the actual system and the associated mathematical model used for reference. They state that even though the problem of uncertain parameters is of crucial importance to the industrial implementation of fault

detection methods, it has however received little attention with only a handful of works so far devoted to it.

Hamelin and Sauter (2000) also noticed that in other research contributions, the robustness problem is addressed in the time domain and has seldom been considered in the frequency domain. In a fault detection problem, it is known that faults as well as unknown input disturbances have typical frequency characteristics, which differ from each other and may thus be used as a criterion for comparison. Their proposed approach has been compared to another approach which does not consider interval type parameters, and simulation results have shown its effectiveness.

Hamelin and Sauter (2000) state that future developments will be concerned with the incorporation of the proposed approach into a closed-loop system. The optimal frequency of the detection filter is given from the minimization of a performance index involving the transfer functions from fault to residual and from inputs to residual. “Clearly, in a closed-loop system, the controller gain will also have an effect on the residual output.”

Other work related to creating a system model was done by Barhen et al. (2000) making use of an information fusion method for system identification. Information fusion is the merging of information from different sources with differing conceptual, contextual and typographical representations. It is used in data mining and consolidation of data from unstructured or semi-structured resources.

2.2. Closed-loop control system fault masking

While Hamelin and Sauter (2000) recognise the effect a closed loop control system will have on the residual output of a system, Chen and Howell (2001) state that feedback control adds to the complexity of fault detection in process plants by masking measurement deviations that might indicate a fault. By making it difficult to distinguish between a sensor, actuator, or plant failure, control systems offer little decision-making assistance to an operator during the occurrence of process faults or abnormal disturbances, and in many cases, the actions of the control system can mask manifestations of the fault that would aid the operator in determining the cause of the process fault. The problem is compounded during transient states of the plant as the control system acts upon a combination of expected and unexpected disturbances. Chen and Howell (2001) have set requirements for their proposed fault detection system to work, it specifies the conditions required to effectively detect a fault:

1. The controllers themselves must perform to specification and all control loops must guarantee zero steady state error, e.g. because they have integral action.
2. The fault must remain until a new steady state is reached and that this change in steady state must be detected.
3. Multiple faults can only be diagnosed if they are separated either spatially, i.e. in different parts of the plant, or by time, i.e. a new steady state is arrived at before the next fault occurs.
4. Analysis is performed qualitatively and hence no quantitative results are obtained.
5. Controller outputs, together with measurements of the control variables, must be available as observations.

The above requirements proposed by Chen and Howell (2001) limit the system to detecting faults during steady state conditions. The objective of the fault identification system developed in this thesis is to detect and characterise faults during transient operation.

Simani and Fantuzzi (2000) explain that most methods of fault detection are using dynamic models of a process because faults are supposed to appear as state changes caused by malfunctions. These methods are often monitored using estimation techniques or parity equations. They state that the basic idea is very simple: the behaviours (i.e., input $\pm$ output time series) of the model and real system are compared to generate residual signals, which, in the presence of faults, take non-zero values. Again, this assumes that the only disturbance input is that of the fault disturbance and that the fault is large enough not to be masked by the control system operation.

To develop a fault detection system independent of plant dynamics, Simani and Fantuzzi (2000) introduce a methodology in which a model-based approach and neural networks are combined to detect and identify the fault occurring in industrial processes. Faults modelled by step functions create changes in several residuals obtained by using dynamic observers (Kalman filters) of the process under examination. A neural network is exploited in order to obtain a link between a particular fault input and output sensors to a particular residual. In such a way, the observers generate residuals independent of the transient state of the plant that are dependent only on sensors' faults. Therefore, the neural network evaluates static patterns of residuals, which are uniquely related to particular fault conditions.

In 2001 Zhang et al. (2001) proposed a fault identification scheme making use of the controller output from the closed-loop control system to indicate unexpected operations. The proposed method is however only effective during steady state conditions and makes use of adaptive learning systems to estimate the fault cause.

The fault detection system developed in this thesis is intended to separate the fault and transient disturbance inputs into a closed-loop system in order to evaluate the effect of the fault disturbance input on the open-loop control system during plant operational mode changes.

2.3. Fault characterisation

Once a fault is detected in a system, a trip can be initiated to shut the plant down and to keep it safe, whilst being able to characterise the detected fault to assist in repairing the plant. The characterisation of a fault could vary from indicating the sub-system in which the fault is located, to indicating the magnitude and spatial location of the fault.

Roy et al. (1998) developed a fault characterisation system to address the need to have improved predictive maintenance techniques in an operating plant. Guidance into the methodology came from one of the earliest applications of state estimation-based fault detection methods in nuclear plants. Roy's primary objective was to provide an early warning to the human operator regarding the failing health of control equipment, in the process averting major breakdown with its associated large plant

downtime. Further, an attempt is made to identify subcomponent faults, so as to carry out fault event sequencing and root cause analysis. They state that most fault detection and characterisation algorithms proposed up to 2000 have been essentially limited to the detection and identification of global faults in a system and so, a further step to this would be to develop fault identification methods for identifying subcomponent faults in equipment, resulting in improved fault localization and providing better predictive maintenance aids.

The methodology developed by Roy et al. (1998) relies on the fact that different types of faults cause changes in either the model structure, the model parameters or in the function of the linear differential equation constituting the model. These changes cause variations in the residues, state estimates, and covariances when a Kalman filter-based algorithm is used for fault identification. As a first step of the parameter estimation process the recursive least square estimation technique is used to determine the coefficients of the proposed difference equation from the input–output data of the particular system.

The produced equations are then used as a model for the Kalman filter and a filter for estimating the states, residues, and covariances. The fault models obtained from the physics of the system are then incorporated in the difference equation models and the resultant changes in the states, residues, and covariances are observed for the different types of postulated faults. The resulting fault characterisation method indicates that effective isolation of different types of subcomponent faults are possible, based on suitable pattern matching of the filter plots.

Once the faults are detected, they are characterised in the following manner:

1. Faults which cause parametric changes or structure changes of the nominal linear model result in altered steady state values of the estimated states and residues.
2. Faults which cause addition of zeros in the transfer function result in altered speed of convergence of the covariances during the initial computation and an increased steady state value.
3. Those which result in the addition of sine/cosine terms in the forcing function of the linear model, then result in amplitude modulation of the state estimates.

The fault characterisation is enhanced by studying the performance of the fault's generalised likelihood ratio, whereby the patterns obtained by auto-correlation and cross-correlation of the filter residues provide further isolation based on their steady state values.

The described method is very effective to characterise faults while still being limited to only being able to identify faults during steady state conditions. The fault identification system developed in this thesis aims to detect and characterise faults during transient or operational mode change conditions when a plant tends to be exposed to higher stresses than under steady state conditions.

Cheon et al. (1993) make use of neural networks to process alarms to aid in the diagnosis of nuclear power plants, while a lot of work has been done to detect and locate faulty sensors in plants, such as the work done by Dorr et al. (2007) and Ming et al. (2006). The research in this thesis does not intend to detect faulty sensors although it could potentially aid in locating such faults.

As recently as 2007 Yan et al. (2008) developed a distributed fault identification system with the objective to address problems arising from the models that typically exhibit complex nonlinearity and compensates for the effects of the faults on the residuals that are hidden owing to noise, both of which can prevent an analytical solution. The noise referred to in this case can also be equivalent to disturbances due to operational mode changes which makes the method developed by Yan et al. (2008) come close to identifying faults during transient states of the plant.

To realise the proposed system Yan et al. (2008) made use of a fault tracking approximator to detect and identify system faults. A network of distributed estimators is constructed where the fault tracking approximator based on an iterative learning algorithm is embedded into each estimator. Compared with a neural network-based fault identification scheme, the approach proved to be more efficient although still based on approximation schemes that are very difficult to license in the nuclear industry.

Similar to Yan's approach Hadad et al. (2008) used neural networks to detect and characterise faults occurring in the Russian VVER pressurised water reactor. Ming et al. (2006) made use of a hybrid approach to diagnose faults with neural networks. Ferrari et al. (2008) designed a fault isolation scheme in an input-output discrete-time framework and derived detectability and characterising properties making it of analytical methods.

In 2010 Villez et al. 2010 initiated a project to integrate diverse fault detection systems and automation into closed loop supervisory control systems to reduce the human interaction when a fault is detected. The integration approach in their research requires new control paradigms to be created which would make the nuclear licensing of the new systems difficult.

2.4. Summary and conclusions

In the following chapters, a deterministic method is pursued that combines some of the practices highlighted in this chapter while making use of advantages obtained from the nuclear industry (such as the availability of accurate simulation models of all plants) to develop a robust fault identification system that could be used as an early fault detection system while being effective during transient states of the plant.

From the literature study of fault detection systems and the state of control and instrumentation in the nuclear industry the following was learned:

- Fault detection systems based on neural networks are effective but brittle. The implementation of such systems will be difficult in the nuclear industry because of the uncertainties associated with such systems.
 - The possibility of developing a fault detection system based on neural networks is eliminated.
- Developing a model of a plant based on first principles to be used as a dynamic reference is expensive and time-consuming.

- Nuclear plants are equipped with engineering and training simulators that can provide a first principles dynamic reference for a fault detection system. A set of specifications of such a simulator was developed in chapter 3.
- The effectiveness of fault detection systems are diminished by the closed-loop response of the control system to disturbances.
 - A method should be developed to measure the effect of the fault on the system without the closed-loop response of the control system.
- During expected transients the effect of the fault is hidden further owing to the operation of the control system on both the fault and the expected disturbance.
 - A method should be developed to measure only the fault effect on the system outside the closed-loop control system.
- Fault characterisation methods rarely make use of distributed control systems due to the fault-hiding effect of the control system.
 - Having a method that produces the full effect of the fault on each subsystem allows distributed control systems to be used in fault characterisation. It should prove effective in the sense that each subsystem responds differently to the fault disturbance and each should reveal a part of the nature and cause of the fault.

In the following chapters the development process of both the fault detection and the fault characterisation system will be described.

3. Article 1: Fault detection and characterisation in Pressurised Water Reactors using real-time simulations

By A.C. Cilliers, D.R. Nicholls and A.S.J. Helberg

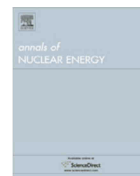
School of Nuclear and Mechanical Engineering

North West University

This peer-reviewed paper was published in Annals of Nuclear Energy 38 (2011) pp. 1196 - 1205, after being presented at the International Conference on Opportunities and Challenges for Water-cooled Reactors in the 21st Century, Vienna, Austria, October 2009.

3.1. Relative contributions by authors

D.R. Nicholls was the Nuclear Programmes Engineering Manager at the time of writing this paper. As a Senior Engineer at the Nuclear Programmes Engineering A.C. Cilliers reported to D.R. Nicholls, whilst D.R. Nicholls also acted as Mentor to A.C. Cilliers whilst providing his knowledge and experience as soundboard to the research team. A.S.J. Helberg acted as study leader during this stage of the research with the task to provide guidance and support to A.C. Cilliers whilst also evaluating the academic soundness and strength of the research. All research was conducted and documented by A.C. Cilliers.



Fault detection and characterisation in Pressurised Water Reactors using real-time simulations

A.C. Cilliers^{a,*}, D. Nicholls^a, A.S.J. Helberg^b

^a Eskom – Nuclear Division, Sunninghill, South Africa

^b North West University – School of Electrical, Electronic and Computer Engineering, South Africa

ARTICLE INFO

Article history:

Received 24 May 2010

Received in revised form 10 November 2010

Accepted 11 November 2010

Available online 1 February 2011

Keywords:

Control and instrumentation

Simulator

Online monitoring

Pressurised Water Reactor

Fault detection

Fault characterisation

ABSTRACT

The use of real-time plant simulators running in parallel with a nuclear plant to predict the control system behaviour and highlighting unexpected plant behaviour is presented. The study is performed on a 910 MW Generation II Framatome Pressurised Water Reactor model and simulator. By simulating the plant behaviour in real-time whilst comparing it with the real-time transient the plant is following, a complete second set of expected control operations and simulated plant measurements is generated. This enables the calculation of the unknown set of variables introduced into the plant as a fault condition. The benefit of such a system is that plant faults that are too small to detect (especially during transients when the plant operating point is moving around) can be identified as unexpected or faulty plant behaviour. The behaviour of the control system is also continually predicted so the effect of the control system compensating for fault symptoms (which in most cases hides the fault condition) is used to characterise the fault as a control variable acting on the plant. The approach is illustrated by simulating a specific fault, small enough to go undetected for an extended period of time, during a typical transient. This is continually compared with a plant simulation, simulating the same transient without the fault. Using the described methodology, the fault is detected and characterised long before the plant safety is jeopardised or the fault is detected by the conventional protection system.

© 2010 Elsevier Ltd. All rights reserved.

1. Introduction

With the advances of microprocessor technology and the development of integrated simulation codes over recent years, it has become possible to simulate large parts of a nuclear power plant as an integrated system in real-time with an astonishing level of accuracy. This has long been a focus area in plant simulator development (Finc et al., 2006) and is resulting in the unification of the traditional training simulator and the various simulation codes used for engineering purposes, with a complete simulation model based on first principle calculations, able to simulate a nuclear power plant in real-time and so enabling real-time online monitoring of the plant.

The effectiveness of such an online monitoring system is largely dependent on the accuracy of the simulation model being used. This is problematic since it would be very difficult to build and maintain a simulator at the accuracy required for the application. To overcome this problem, the implementation illustrated in this study focuses on the operations of the control system, which require a lower degree of accuracy since the control system follows

the trend of various measurements inside the plant and interacts with the plant to control these variables. The implementation of an exact replica of the control system and logic in a software environment is fairly simple.

For a fault detection system to be effective it needs to improve the system dependability. A dependable operation requires that the fault be detected (sensitivity), that the detection process is quick enough to be of value (speed) and that the decision taken is the correct one (security). A completely dependable protection system will always operate correctly for a detected fault (Wall, 2005).

- Sensitivity is critical to being able to detect actual faults as they occur. The three measurement components measurement, being accuracy, precision and resolution are independent qualities of a measurement.
- Speed is important for limiting exposure and potential damage. The time to clear a fault is mainly determined by the time it takes the system to make the decision. This decision time is based on the extent to which a value should drift from the norm before it is flagged as a fault.
- Security reflects the sureness of the protection system decision. In plant protection, it refers to the ability of not operating for false alarms, but acting fast for true faults.

* Corresponding author. Tel.: 011 800 2328; fax: 086 664 8796.

E-mail address: anthonie.cilliers@eskom.co.za (A.C. Cilliers).

Fault detection and characterisation in Pressurised Water Reactors using real-time simulations

ABSTRACT

The use of real-time plant simulators running in parallel with a nuclear plant to predict the control system behaviour and highlighting unexpected plant behaviour is presented. The study is performed on a 910MW Generation II Framatome Pressurised Water Reactor model and simulator. By simulating the plant behaviour in real-time whilst comparing it with the real-time transient the plant is following, a complete second set of expected control operations and simulated plant measurements is generated. This enables the calculation of the unknown set of variables introduced into the plant as a fault condition. The benefit of such a system is that plant faults that are too small to detect (especially during transients when the plant operating point is moving around) can be identified as unexpected or faulty plant behaviour. The behaviour of the control system is also continually predicted so the effect of the control system compensating for fault symptoms (which in most cases hides the fault condition) is used to characterise the fault as a control variable acting on the plant. The approach is illustrated by simulating a specific fault, small enough to go undetected for an extended period of time, during a typical transient. This is continually compared with a plant simulation, simulating the same transient without the fault. Using the described methodology, the fault is detected and characterised long before the plant safety is jeopardised or the fault is detected by the conventional protection system.

1. Introduction

With the advances of microprocessor technology and the development of integrated simulation codes over recent years, it has become possible to simulate large parts of a nuclear power plant as an integrated system in real-time with an astonishing level of accuracy. This has long been a focus area in plant simulator development (FINC, 2006) and is resulting in the unification of the traditional training simulator and the various simulation codes used for engineering purposes, with a complete simulation model based on first principle calculations, able to simulate a nuclear power plant in real-time and so enabling real-time online monitoring of the plant.

The effectiveness of such an online monitoring system is largely dependent on the accuracy of the simulation model being used. This is problematic since it would be very difficult to build and maintain a simulator at the accuracy required for the application. To overcome this problem, the implementation illustrated in this study focuses on the operations of the control system, which require a lower degree of accuracy since the control system follows the trend of various measurements inside the plant and interacts with the plant to control these variables. The implementation of an exact replica of the control system and logic in a software environment is fairly simple.

For a fault detection system to be effective it needs to improve the system dependability. A dependable operation requires that the fault be detected (sensitivity), that the detection process is quick enough to be of value (speed) and that the decision taken is the correct one (security). A completely dependable protection system will always operate correctly for a detected fault (Wall, 2005).

- Sensitivity is critical to being able to detect actual faults as they occur. The three measurement components measurement, being accuracy, precision and resolution are independent qualities of a measurement.
- Speed is important for limiting exposure and potential damage. The time to clear a fault is mainly determined by the time it takes the system to make the decision. This decision time is based on the extent to which a value should drift from the norm before it is flagged as a fault.
- Security reflects the sureness of the protection system decision. In plant protection, it refers to the ability of not operating for false alarms, but acting fast for true faults.

Further requirements placed on the system are that no previous knowledge of fault characteristics should be required in order for the system to detect and characterise the fault. This means that any new faulty behaviour, however unlikely, would be accounted for and would be characterised.

To enable this increased dependability and intelligent fault detection any faulty operation is treated as a plant control system resulting in moving the various operating points away from the design value. The plant control system, on the other hand, has the sole objective of keeping the operating point at the designed value. In other words, we accept that a plant control system is designed such that:

For every possible movement of the operating point, an Instrumentation and Control (I&C) system is in place to counteract the movement until the I&C system is operating at maximum capacity and unable to counteract the movement.

The implication is that for every possible movement a fault induces in an operating point or number of operating points, there is a corresponding control function or control functions that could in theory counteract, or induce the same movements. This allows us to characterise the fault as a control system providing us with specific details as to the nature and cause of the fault. When making these conclusions, it is easy to lose track of the limitation that prevented such fault diagnostics from being done in the past, i.e. being unable to predict control system behaviour during various transients. This is now made possible by real-time engineering simulators.

This paper illustrates this philosophy with a discussion on PWR simulator requirements (section 2) analysis of the plant protection and control system without (section 3) and with (section 4) the implementation of the proposed fault detection and characterisation system. It then offers functional proof (section 5), by way of an example, of the effectiveness of the system detecting and characterising faults in the system. All implementation is done without affecting the existing operation of the plant protection and control system (section 6), which allows increased confidence in the system to only improve on the system dependability in all instances and which should allow easier adoption (Committee on Application of Digital Instrumentation and Control Systems to Nuclear Power Plant Operations and Safety, 1997).

2. PWR simulation accuracy

To enable the use of a plant simulator to improve the dependability of a protection system, the accuracy of the simulator model and numerical methods used is required. If the accuracy of the

simulator outputs are known during all conditions and the tolerance of the measurement instruments are known, a fault can only be detected with confidence once the error levels do not overlap. During transients that require complex calculations, or with an inaccurate plant model implemented in the simulator, the error band would become so large that the traditional protections system in the plant would detect the fault before the new system will.

The accuracy of the outputs from the simulator is not only based on the complexity of the calculations used, but also on the quality and level of detail of the plant model used in the simulator. For this reason it is important to develop the simulator with the plant to include all plant modifications.

The problem with inaccuracies is mitigated in two ways:

- The fault detection system will only compare the simulated values with measured values used by the plant protection system. Since the plant protection system is kept simple while limiting the number of different measurements the need for an overly complicated plant models are negated.
- During the development of the fault detection system, the focus was shifted from comparing measured plant parameters to comparing control system parameters. This allows the adaptation of the measured parameters to represent measured parameters that would have been seen if the control system did not counteract the fault by maintaining the parameters at certain set points. This increases the difference between the measured and simulated parameters once a fault occurs, and so allows a simulator with larger error margin to detect faults effectively. This theory is developed in this paper and forms the basis of the fault detection system's effectiveness.

It is important to note that in order to prevent false faults being detected the difference between the adapted measurements and simulated parameters should move beyond the error levels of both systems before a fault can be detected. The implication is that if an inaccurate simulator model is used, the fault would be detected by the plants traditional protection systems before the fault detection system would detect the fault with certainty. At now point would the system be allowed to detect faults while inside the uncertainty margin while accuracy improvements to the model or the algorithms would result in faster detection fault times.

3. The PWR primary circuit control system

A typical Pressurised Water Reactor (PWR) uses ten primary control systems to keep the plant operating at the requested power level and within the designed safety margins (Koeberg, 2005). Each system operates independently from the other with some shared information. The ten control systems are:

- Pressuriser pressure control.
- Pressuriser level control.
- Reactor average temperature control.
- Atmospheric steam dump control.
- Steam generator level control.
- Steam generator feed water flow control.
- Steam pressure control.

- Power control.
- Turbine speed control.
- Generator voltage control.

At this point it should be mentioned that although the control systems operate independently many of the parameters being controlled are interdependent on each other and as such, during expected or unexpected transients a number of parameters would need to be controlled to return to the reference value. This implies that unexpected faulty plant operation would have a number of control systems operating on it to reduce its effects. The unexpected disturbance would then be modelled as a number of control operations as opposed to a single control operation. The benefit obtained from such a combination of modelled control operations is that it describes the nature of the fault in totality, resulting in effective fault identification.

This paper will focus on the control systems that directly impact on the primary coolant system of the PWR, being the pressuriser controls: pressure control, level control, reactor average temperature control (that is used to control power), and to a lesser extent the steam generator controls: atmospheric steam dump control, level control, feed water flow control and steam pressure control.

3.1. Pressuriser pressure control

Pressure control measurements of the pressuriser are used while the pressure is controlled by a proportional heater as well as a backup heater for low pressure (Fig. 1). For high pressure, the pressuriser spray and relief valves are used. These control parameters are able to control the pressure level for any disturbance until it reaches maximum operational capacity. Any unexpected disturbance to the pressuriser pressure can therefore be modelled as a heat source for high pressure and cooling spray or opening of relief valves for low pressure. Disturbances due to expected transients would be predicted by the real-time simulator with no unexpected operations identified.

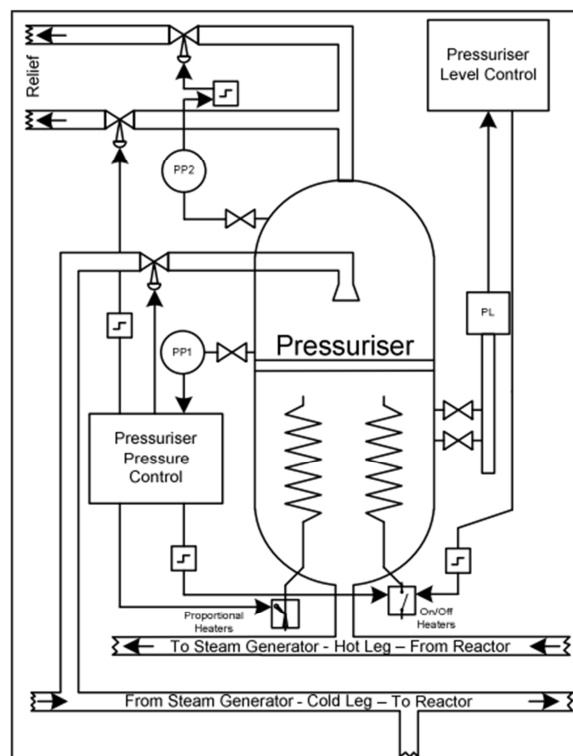


Fig. 1. Pressuriser pressure and level control

The pressuriser pressure and level control diagram (Fig. 2) depicts the logic used to control the instrumentation. Under steady state conditions, very little control actions take place since equilibrium will be reached at some point with a stable control system. A disturbance is introduced into the plant due to certain expected transients or due to an unexpected fault introduced into the system. In such a case the control actions will counteract the effect of the disturbance. In all cases, a real-time simulator can predict the effect of each control instrument as well as the expected transient. The unexpected fault, however, cannot be predicted but affects the operation of all the other control instruments acting on the same operating point. The operating speed is characterised by the transfer equation (figure 2), that is the response the system will have to a particular input. The pressuriser level is controlled by opening let down and charging valves to and from the cold leg of the coolant loops. The logic that controls the level is discussed in the following section.

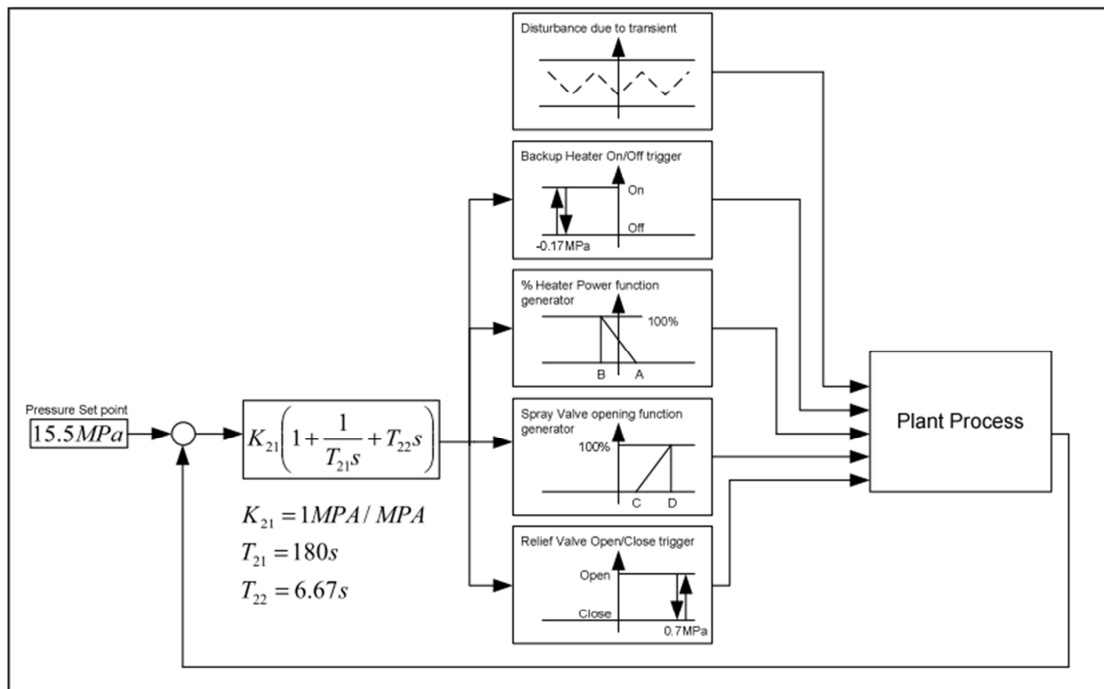


Fig. 2. Pressuriser pressure control diagram

3.2. Pressuriser level control

The pressuriser level control logic (Fig. 3) controls the timing and size of the let down and charging flow valves. The level set point is a function of the average reactor coolant temperature. It includes a dead band that allows for natural temperature induced level variations. This allows the restriction of charging flow variations during slight power variations. Once the dead band threshold is breached, the let down and charging valve opening is controlled by a transfer function (Fig. 3) dictating the response to the disturbance. The effect of an expected or unexpected disturbance is compensated for by the feedback control system and would result in a return to the reference pressuriser within the designed control system time. Since the pressuriser level can be fully controlled by the let down and charging flow, any unexpected operation in the pressuriser level control can be modelled as a let-down or charging flow action for which the pressuriser level control is compensating.

In the case of the average reactor coolant temperature remaining in the dead region of $\pm 0.8^\circ\text{C}$ on either side of the full power reference and $+2^\circ\text{C}$ and -3°C on either side of the no-load reference temperature, the control system would not interject with pressuriser level changes and thus would have

no unexpected operation acting on the pressuriser level. In such a case the information from the level measurement input is clean and can be compared to the expected pressuriser level from the simulator. During expected transients the behaviour of the level control system could be predicted by a real-time simulator with unexpected operation identified.

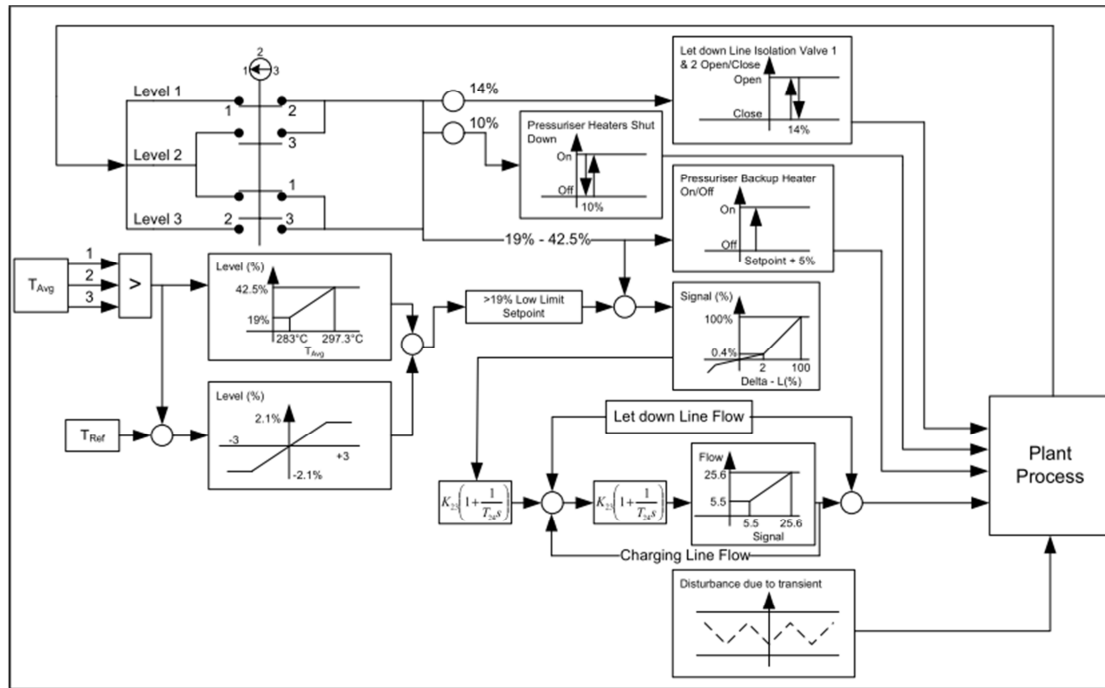


Fig. 3. Pressuriser level control diagram

3.3. Average temperature control

Average temperature control (Fig. 4) is achieved by control rod movement inside the reactor. It is designed to maintain the average temperature within $\pm 1.8^\circ\text{C}$ of the set point. This includes accepted measurement error and a dead band. It is designed to allow for expected operating transients during which time the control margin is extended beyond the $\pm 1.8^\circ\text{C}$ margin, after which the control system is expected to return the measured temperature to within $\pm 0.8^\circ\text{C}$ of the specified set point.

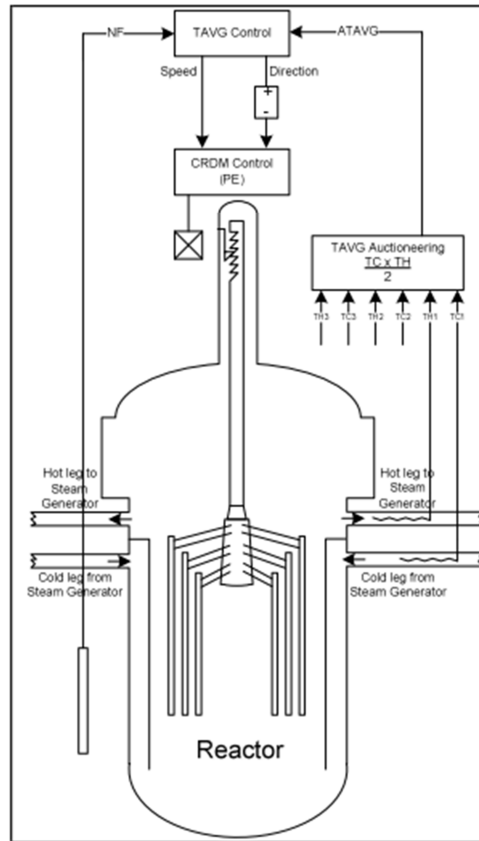


Fig. 4. Average temperature control

The control function is generated by combining measured average temperature, neutron flux and turbine power. The control diagram of the average temperature control by control rod movement (Fig. 5) compensates for any expected or unexpected disturbance of the average temperature by the moving of the control rods inside the reactor. Any unexpected movement of the control rods inside the reactor could be attributed to unexpected changes in core power, turbine power or average temperature. Since these changes are fully controlled by simply adjusting the speed and position of the control rods, any unexpected disturbance can be modelled as a control rod movement in the opposite direction of the control rod operation.

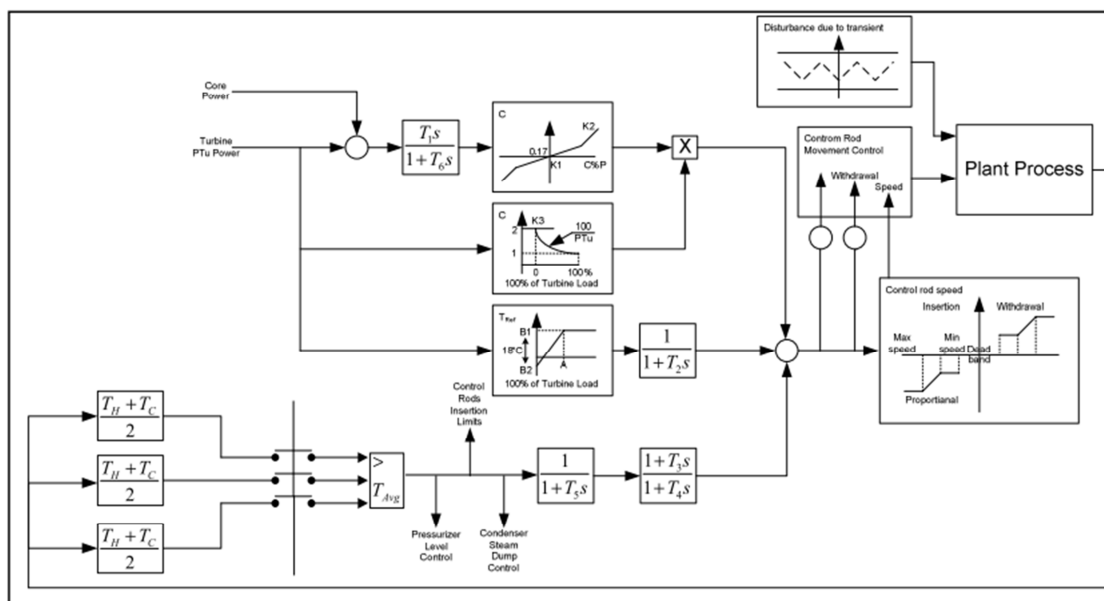


Fig. 5. Average temperature control diagram

4. Implementation of proposed fault detection and characterisation system

To implement the proposed fault detection system, an interface between the real-time simulator and the actual plant is required. The interface (Fig. 6) not only compares measured parameters of the plant with the simulated parameters from the simulator; but also compares the control system actions of the plant with the simulated control system actions of the simulator.

Often the control system information is of more value than the measured and simulated parameters, but rarely used for fault identification purposes. In this system, all plant measurements as well as the control outputs are compared with the simulated equivalents. As long as the measured and simulated variables remain within the accepted error margins and the actual and simulated control systems remain within the accepted error margins, the plant considered to be operating as anticipated.

When a small fault occurs, the measured and simulated parameters would remain within the error margins, since the control system would keep it running at the operating set point. The simulated and actual control parameters would however differ beyond the error margins. This allows the manipulation of the measured plant parameters to exclude the effect of the unexpected control operations but still include the effect of the expected control.

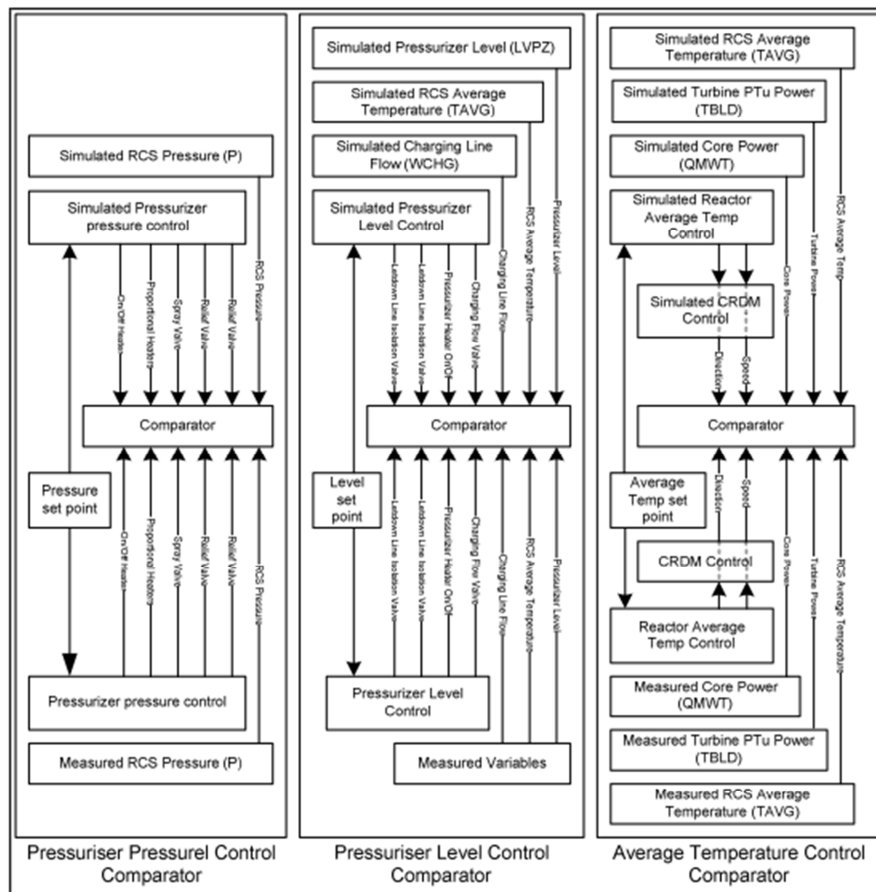


Fig. 6. System for comparing real and simulated measurements and control parameters

The information available to the comparator is manipulated to isolate the information describing the unexpected plant behaviour. This can be done since the image received from the plant and the image

received from the simulator differs only by the information that the simulator is unable to predict: unexpected plant behaviour beyond previously considered faults as well as small faults that would normally remain hidden as the control system counteracts them.

In a typical example of a 100% power to 80% power transient (Fig. 7), the power change is initiated after 400 seconds and as the power changes, the primary pressure drops with the proportional heater adapting to return the primary pressure to the pressure set point using the PID control (Fig. 2). In this particular nuclear plant, fast transients require the turbine to follow the load by bypassing steam with the reactor following at a slower rate, changing the reactor power. The turbine reduces load linearly and reaches its new load position at 1,627 seconds, which is reflected in the pressure with a slight change in the pressure response.

During the complete transient the proportional heater is able to return the pressure to within the required 0.8% of the set point. The coolant spray valve only operates once the required pressure is reached to reduce the settling time. When comparing the pressure change with the heater operation shown in Fig. 7, the proportional relationship is clear. The pressuriser level control and average temperature control systems are evaluated in the same manner (Figs. 8 & 9) with a direct relationship between the measurement and the control response visible, practically showing that for every disturbance in the system, a control function exists to counteract the disturbance.

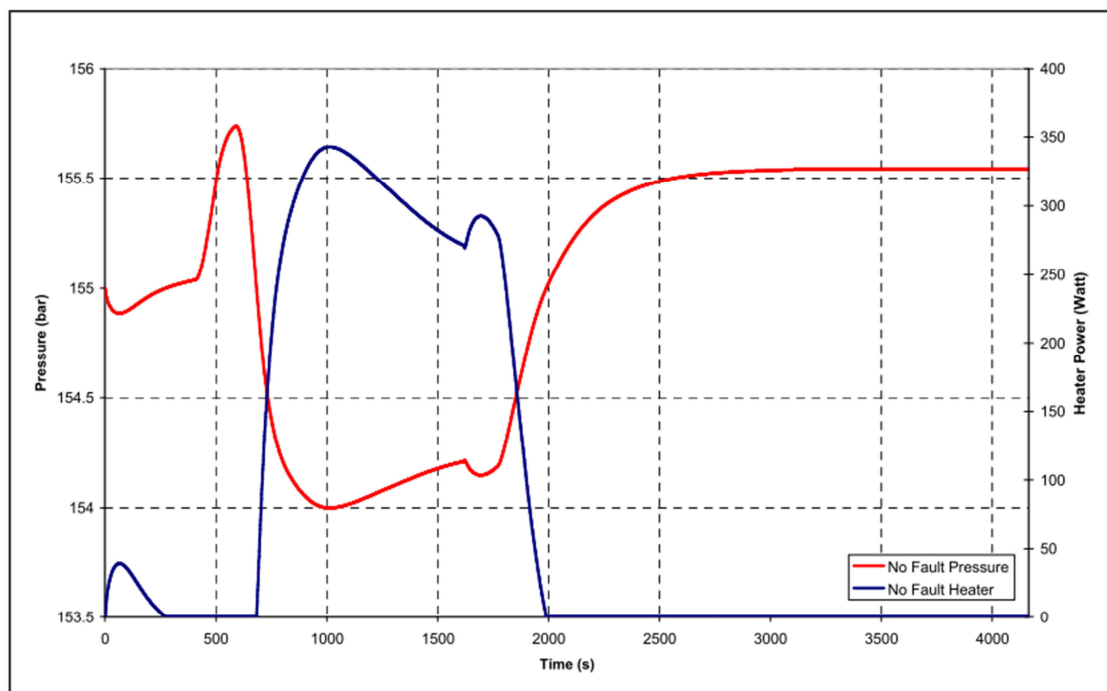


Fig. 7. No Fault 100% power to 80% power pressure transient

The relationship between the pressuriser level and the residual in/out flow from the charging and let down flow valves (Fig. 8) becomes proportional after the initial dead band tolerance is breached. It is also worth mentioning that for various power levels, the pressuriser level has different set points, hence the settling of the control system at 54% from the original 62%. Again a large flow spike is seen at 1,627 seconds due to the stop in load reduction on the secondary side.

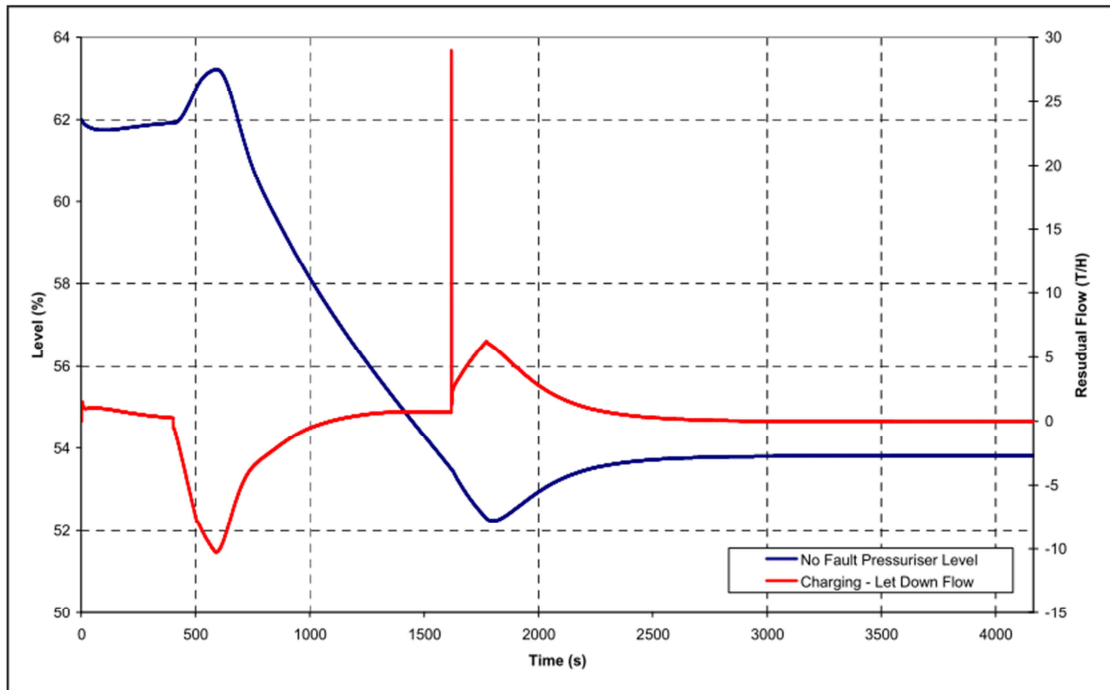


Fig. 8. No Fault 100% power to 80% power pressuriser level transient

The neutron flux power (Fig. 9) is used to control the average coolant temperature. This is done by lowering the control rods into the reactor core. The effective negative reactivity inserted by the rods results in a proportional lowering of the reactivity of the core.

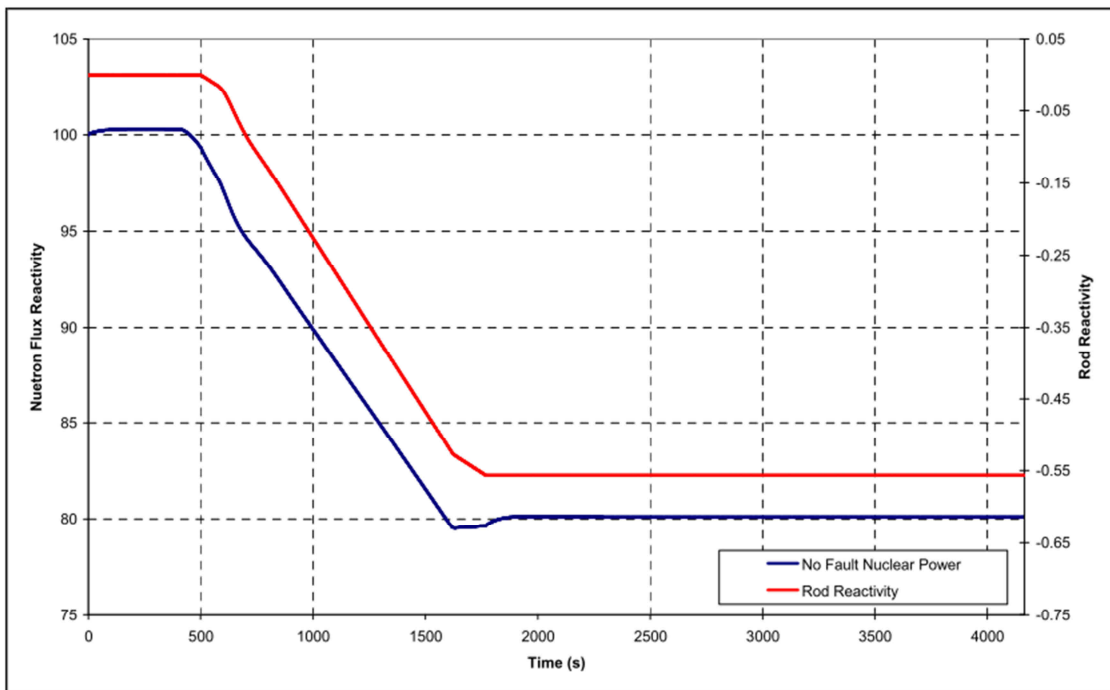


Fig. 9. No Fault 100% power to 80% power nuclear power transient

5. Fault detection system functional proof

When a fault is introduced in the system, the simulator would be unable to predict the operation of the plant correctly since the simulator would be unaware of the fault. The measured and simulated fault (Fig. 10) differs the moment the fault is initiated (at 500 s), however, the full extent of the pressure drop due to the fault cannot be seen due to the cancelling effect of the pressure control system. Based on the simulated and actual operation of the proportional heater in the pressuriser, the unexpected over-operation of the heater can be used to calculate the pressure drop in the pressuriser if the control system only controlled for expected transients.

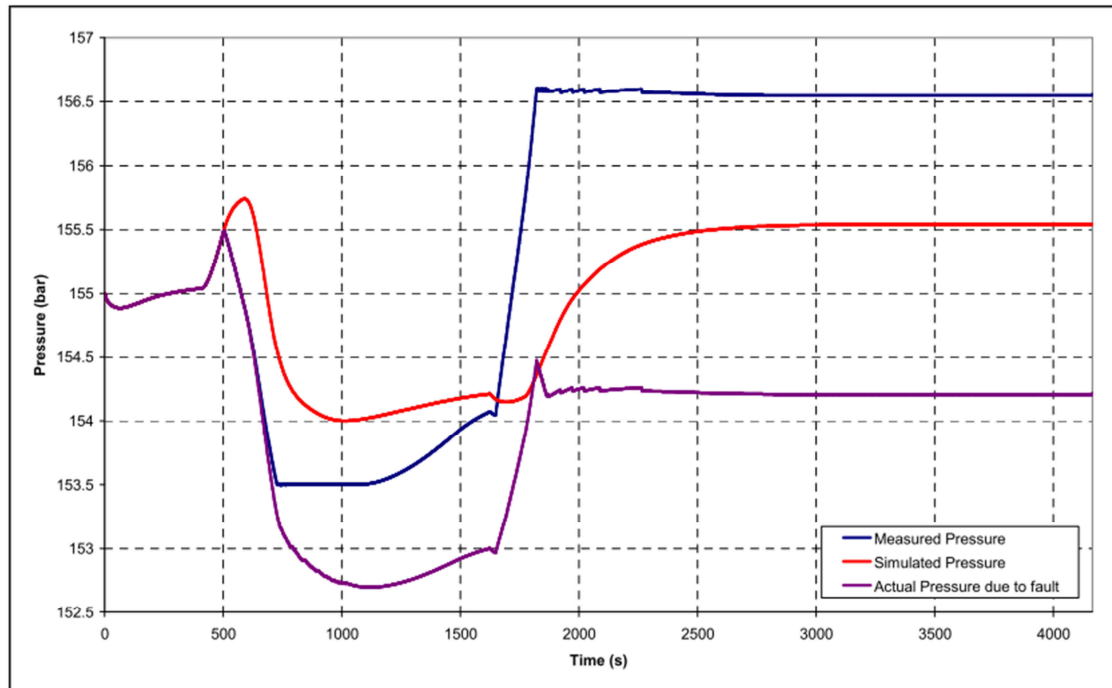


Fig. 10. Pressuriser pressure – measured, simulated and effective

The Reactor Coolant System Volume is calculated based on the pressuriser level (Fig. 11). The simulator predicts the level of a healthy plant during the power change transient. The measured values show a slight variation due to the fault, but the control system - by means of the charging and let down flow valves - reveals that the plant system is compensating for a more significant level drop than expected.

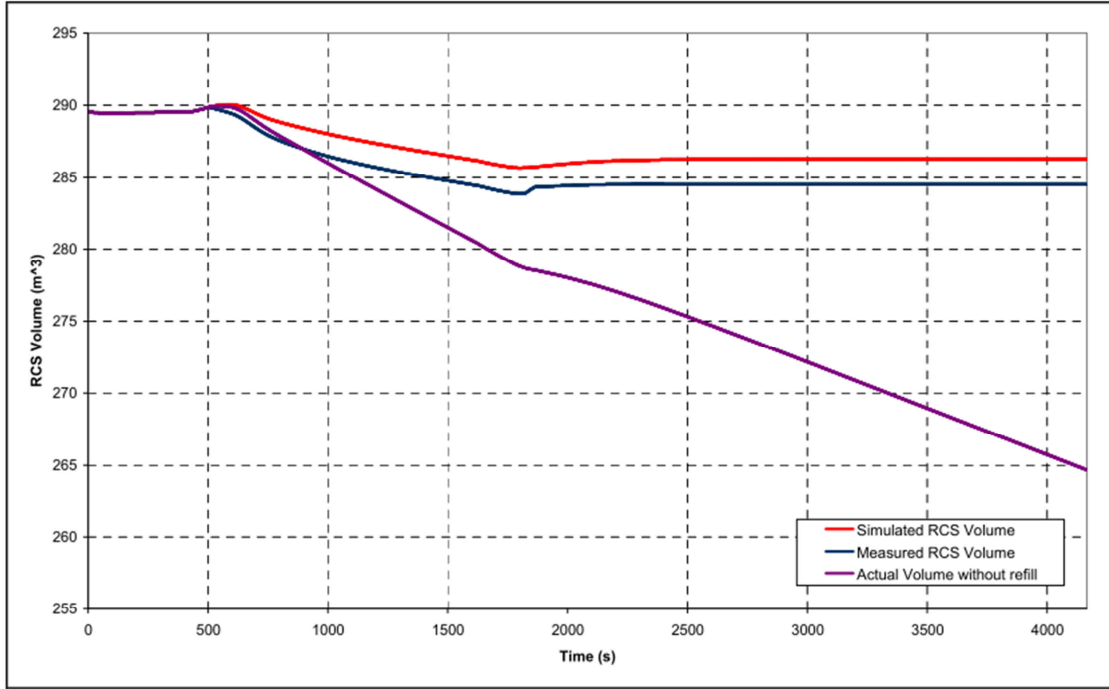


Fig. 11. Reactor Coolant System Volume - measured, simulated and effective

This information allows us to calculate the actual Reactor Coolant System volume if the control system did not compensate for an unexpected drop in the pressuriser level, with the resultant drop in pressuriser level due to the fault calculated by simple subtraction. The gradient of this resultant drop in pressuriser level provides us with valuable insight into the nature of the fault. The flow response due to the fault (Fig. 12) highlights a result corresponding to a typical response to a step input from the control system, more specifically:

$$\begin{aligned}
 &K_{23} \left(1 + \frac{1}{T_{24}s} \right) \\
 &K_{23} = 7\% / \%level \\
 &T_{23} = 720 \text{ sec}
 \end{aligned} \tag{1}$$

from the pressuriser level control system function (Fig. 3), controlling the rate of change when charging or let down flow is required. The result is very meaningful since it practically shows that the system reacts to faults in an exact but opposite direction at a rate dictated by the control transfer function. Since the transfer function is known, the fault can be calculated. It also allows us to calculate the size and severity of the fault, in this case losing coolant at a rate of 17,000kg per hour.

The process of locating the source of the faulty behaviour - in this case a small loss of coolant accident - is done by first calculating the size of the leak based on the rate of loss of coolant. A number of components may then be eliminated as a possible cause to the fault due to the physical characteristics of the component. In the case of this example a 0.5cm² leak was the cause of the loss of coolant, which could be due to a valve stuck open or a leaking pump seal. However, piping or seals with an effective area smaller than 0.5cm² could not cause such an accident.

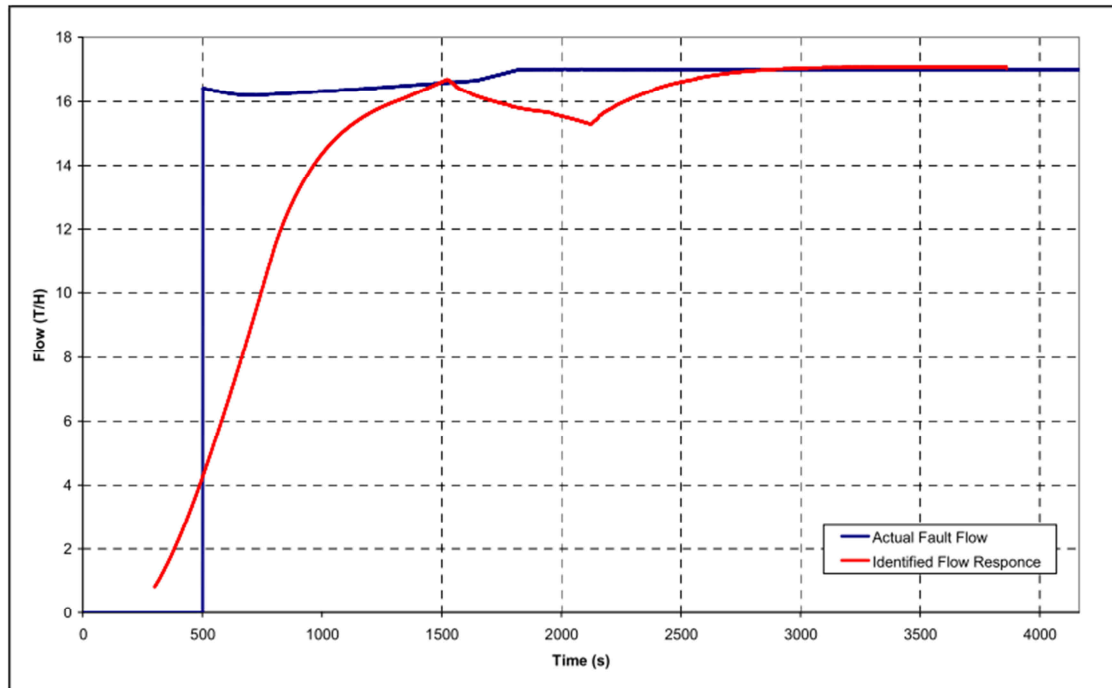


Fig. 12. The control system response to a small loss of coolant fault

6. Proposed control room implementation

Throughout the described in this paper, an attempt has been made to keep all new technological and philosophical introductions into the nuclear industry in line with regulatory requirements in order to ease the licensing process and maintain safety standards already achieved and proven in the nuclear industry. The safety case is usually proven using probabilistic risk/safety assessments (PRA/PSA). With the use of specialised systems, it is important to touch on the challenges associated with the licensing of digital I&C, as it is the use of digital I&C that allows the implementation of such systems.

The new control and protection philosophy is based on having a simple robust outer operating window that prevents fuel and other structural damage. This system is required to have a 10^{-4} per year or better failure frequency and should have no common mode failures with the second operating window inside it. It should consist of a number of fixed operating windows, based on the mode in which the plant is operating.

The second operating window will make use of control information available from the control system.

The PRA requirements for the complete system are to have a failure frequency of 10^{-7} . It is recommended that this be achieved by demonstrating the following:

The protection and safeguard system has a failure frequency of at least 10^{-4} with 99% confidence. The control and protection system needs to include at least all protection functionality as that of the protection and safeguard system implemented diversely to prevent common mode failures. The control and protection system should have a failure frequency of at least 10^{-3} with 99% confidence. The fault detection system described in this paper and other advanced fault detection systems will be embedded

in this plant control and protection system, having access to all actual measurements and control functions as well as simulated measurements and control functions.

In addition to the protective functions, the control and protection system will include the control functionality to control the plant during non-fault conditions as well as shutdown control in the event of early fault detection. All safety actuation functions are controlled by the protection and safeguard system. All software-based systems need to demonstrate a PFD of 10^{-4} with 99% confidence using, regardless of whether implementation is in the protection and safeguard system or the control and protection system.

The method allows the maintaining of existing plant safety requirements, with the provision of introducing and implementing advanced safety and diagnostic systems into the control and protection system. The benefit is that of early fault detection that would not result in a SCRAM with the associated safety actuation systems, but rather in a controlled soft shutdown or even online maintenance to repair the fault. It is important to note that the implementation provides the operating personnel with the information on the nature of the fault as well as the control functionality to safely shut the plant down. Since the faulty operation is detected before it becomes an accident, the operating personnel have the option of rectifying the fault without shutdown (if possible) or opting for a plant shutdown to rectify the problem.

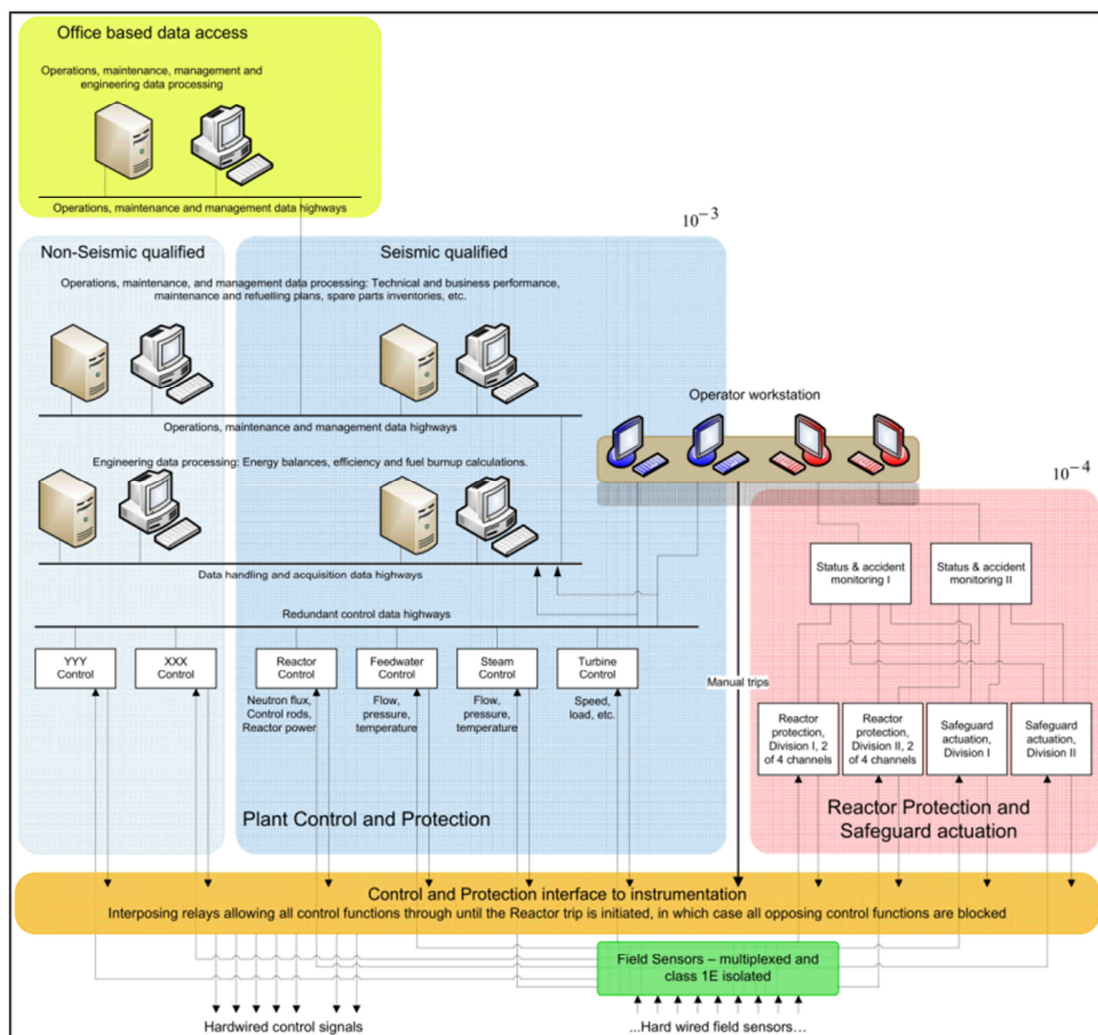


Fig. 13. Adapted control and protection schematic

Fig. 13 depicts the implementation of the protection and safeguard system, having a static operating window (changing for various plant operating modes) and maintaining the structural integrity of the plant. The control and protection system maintains a dynamic operating window inside the static operating window, which detects faulty operation before it affects the safety of the plant.

7. Conclusion

The purpose of the research as described in the introduction is to use modern sophisticated plant simulator technology in a novel fault identification application. The requirement of the implementation is to improve on the integrity of the existing system providing more sensitive, faster and more reliable with increased detail information regarding any unexpected operation inside the plant. The chosen example, that of a small break loss of coolant accident has proven that the system detects the fault well in advance but also provides detailed information about the fault within a relatively short period of time. A fault of this magnitude would not be recognised by the protection system while the control system would be able to maintain the operating point indefinitely. This would result in contaminated coolant leaking into the containment vessel which could be avoided.

The system is not limited to the detection of loss of coolant accidents. Any unexpected event in the plant can be identified using the exact same algorithms. The power of the system is unlocked due to the added information from the real-time simulator and simulated control system, without which the number of unknown variables would exceed the number of functions.

8. References

- FINC, P, et al, 2006. Workshop in Simulation and Modelling for Advanced Nuclear Energy Systems, Office of Advanced Scientific Computing Research, U.S. Department of Energy, Washington. D.C. USA.
- Wall, R.W, 2005. Power Systems Protection, University of Idaho, USA.
- Committee on Application of Digital Instrumentation and Control Systems to Nuclear Power Plant Operations and Safety, 1997. Digital Instrumentation and Control Systems in Nuclear Power Plants: Safety and Reliability Issues, National Academy of Sciences, Washington, D.C, United States of America.
- Koeberg, 1997. Koeberg Safety Analysis Report, Revision 4b, Eskom (Pty) Ltd., South Africa.
- International Atomic Energy Agency, 1999. Modern Instrumentation and Control for Nuclear Power Plants: A Guidebook. Technical Report Series No. 387. IAEA, Vienna, Austria.
- PAZ, R.A, 2002, Model Reference Design Technique, New Mexico State University: Klipsch School of Electrical and Computer Engineering. Las Cruces, USA.
- CARRASCO, J.A, 2005. Simulation Aids in the Automation of Industrial Processes, Tecnatom, S.A. San Sebastian de los Reyes, Spain.

3.2. Additional notes

In the above paper a system is described that makes use of a first principles plant model or simulator as dynamic reference. In order for such a system to be realised, the plant model needs to adhere to a number of system requirements.

3.2.1. Modelling and simulation needs for advanced nuclear energy systems

In 2006, the “Workshop on Simulation and Modelling for Advanced Nuclear Energy Systems” identified a number of shortcomings in the current state of the simulations industry. The workshop also identified a number of research and development fields that should be pursued in order to address the shortcomings and enable better utilisation of simulators throughout the nuclear industry (Finc, 2006).

These themes are:

- Uncertainty quantification and error estimation in simulations,
- methods for systems that couple multiple models – movement away from empirical models toward physics-based first-principles models,
- methods for systems with multiple scales,
- algorithms and software that scale well on high-capability computational platforms, and
- simulation workflow management, including data archiving and automated discovery.

The following are some of the high-level findings of the workshop:

1. The code base currently used for advanced nuclear systems is insufficiently predictive to guarantee attainment of the ambitious technology stretch goals of the Global Nuclear Energy Partnership.
2. A significant opportunity exists to apply advanced modelling and simulation and high-performance computing to improve designs of future reactors, reduce uncertainty in facilities development and construction costs, improve safety, and reduce development times of new fuel types needed to close the nuclear fuel cycle.
3. Significant research challenges remain in developing and scaling multi-scale and multi-physics codes to the performance levels on advanced high-performance computers needed for fundamental studies, as well as for design and engineering use. These research challenges are similar (but not identical) to those faced in other science and engineering domains; thus, many methods can be leveraged from other disciplines.
4. The creation of new physics-based high-fidelity simulation codes offers the possibility of accelerating the licensing process if the regulatory process can be modified to incorporate first-principles simulations as a basis for risk analysis and design approvals.

From these findings, it is clear that a common belief exists that processing speed and parallel processing technology have advanced to such a stage that new simulation paradigms can be formed. The investment in these research areas promises to add much value to the current state of nuclear plant design, safety, and control. This research sets goalposts for simulator development that new simulator technologies need to attain to enable them to be used in the control and protection process of the nuclear plant.

3.2.2. Nuclear plant simulator requirements for fault identification

As the trends in simulation technology are known, additional requirements are defined to specify a state-of-the-art simulator, allowing not only online monitoring and plant diagnostics, but also improved design tools and safety verification tools.

We have developed a user requirement specification (URS) that includes all requirements to which a modern plant simulator should adhere, based on the findings of this research. This will enable traditional tasks associated with plant simulators as well as allow the simulator to be implemented in new tasks, such as the providing a dynamic reference for a dynamic operating envelope described in this thesis. The main requirements from the URS are described in the following paragraphs. It is important to note that not all requirements are essential for enabling the implementation of a dynamic reference, but are deemed important, since they form part of the envisioned tasks for which simulators will be used in future.

Simulator model requirements

To achieve the described improvements, an original approach to the integration level of solvers is required:

1. The simulator should adopt a first-principles approach, utilising advances in both hardware and software platforms, which will open the possibility to a new simulation system with advanced capabilities.
2. An integrated high-fidelity system of software tools should describe the overall nuclear plant behaviour, taking into account coupling among the different systems and physical phenomena during reactor operations and transients. The coupling should link neutronics, fuel behaviour, fluids and heat transfer, and structural mechanics, as well as radiation dose dispersion models during severe accident simulations. The system should also be coupled with the structural mechanics software model.
3. The new system should be able to perform sensitivity and uncertainty analyses to assess margins and be able to qualify, validate, and optimise designs (IAEA, 1999).
4. The plant fidelity should be scalable to enable high-resolution, high-accuracy calculations used for engineering design and specification applications or lower-resolution, lower-accuracy calculations optimised for real time and faster than real-time simulations used for transient analysis and training.
5. The simulator should be benchmarked to be able to quantify the accuracy of the plant model and mathematical solver combination in real time during the simulation process. The simulation accuracy should be available to plant diagnostic systems at all times.

The V&V of simulation software is very challenging because of the difficulties associated with uncertainty propagation through multi-physics multi-scale simulators and lack of integral experiments. It remains a very important requirement before implementation as a full-scale engineering and training simulator (Common Position of Seven European Nuclear Regulators and Authorised Technical Support Organisations, 2010).

Simulator functional requirements

The full-scope NPP simulators shall incorporate detailed first-principles modelling of systems and components of the NPP as base architecture for both control room simulated environment and the engineering simulator. The simulator will be used to interface with the operator in the simulated control room, as well with the design engineer in the office environment.

1. The simulator shall calculate and demonstrate expected plant responses to normal and abnormal operating conditions, including malfunctions.
2. The simulator shall contain all systems and components necessary for complying with ANSI/ANS-3.5-2009, including, but not limited to:
 - o Plant simulator hardware and software,
 - o a comprehensive virtual model of the NPP,
 - o plant control software from the DCS vendors, where the controller algorithms can be compiled and executed on the simulator platform under the control of the simulator real-time executive,
 - o software modelling tools required to maintain and modify the simulator software models,
 - o a graphical interface allowing the configuration of operation scenarios, and
 - o a system for the recording, archiving, and playback of simulator operations and simulated transients.
3. In addition to the dynamic capabilities, the simulator tool shall have the capability to solve all models in steady state to provide a steady-state solution. This will be used for mass/energy/heat balance calculations as well as real time synchronisation with the actual nuclear plant.

Reactor response simulation

The objective of reactor core simulations is to predict a series of plant parameters (fluxes, temperatures, stresses, damages, etc.) during normal and abnormal events, during static and transient events, for short-term operational times up to and including plant end of life. These parameters are important for the plant efficiency and safety for single components, system reliability, and system lifetime.

Neutronics

A model allowing simulation and modelling of nuclear reactor physics shall be included. Most industrial modelling is specific to current reactor designs. Departures from these designs, such as using reprocessed fuel, will require higher-fidelity simulation tools, based more on first principles than on normalisation to current designs.

Fluids and heat transfer

A model simulating fluid flow and heat transfer shall be included for core modelling, as well as for the rest of the plant, including steam generators, pipes, pumps, and condensers. Because of the complexity of the phenomena and geometries involved, current codes often rely on empirical correlations. It is often not clear whether these correlations can be readily extrapolated to new

situations. The scientific challenges are in physical modelling, numerical methods, and computer science. The physical modelling must rely more on first-principles methods for single-phase and two-phase multi-fluid flows, for steady and unsteady flows, and with or without heat transfer. Numerical methods must be more robust and must provide the optimal mix between accuracy and stability. Codes must deal with a large number of mesh elements and enable easy multi-scale and multi-physics coupling.

Dose dispersion

A puff and plume model for projection of thyroid and total effective dose equivalent (TEDE) in 16 km should be included. The model should take into account geographic information of the site and allow for wind speed and direction changes.

Control and instrumentation

The control and instrumentation of the plant should be modelled based on the exact control philosophy and configurations of the plant design. It should also include the protection systems as described in the plant design.

Seismic analysis and design

Enabled by modern solution algorithms and high-performance computing, more rigorous and realistic seismic simulation models should be included. These models will significantly increase the understanding of seismic events, enable performance-based design for significant cost savings, and increase design efficiency. Also included in the model should be the philosophy behind the earthquake events, which spans from energy release at the causative fault, to energy transport through seismic wave propagation in a highly heterogeneous media, to ultimate shaking and response of the structure. The phenomenon is inherently three-dimensional, and the response occurs in two distinctly different, but closely coupled, domains: the earth and a structural system.

Structural mechanics

Modelling of advanced material constitutive models that can accurately represent the time-dependent behaviour of materials in extreme environments should be possible. These models should address the effects of high irradiation levels, extreme temperatures, and chemical interactions on material behaviour. Advanced materials models should account for fully 3D, multi-axial states of stress both at low strain rates (normal operations) and at high strain rates (accident scenarios). Graphical information on structural damage due to accidents shall be shown.

3D models should also allow for the design of the following:

- Radiation shielding: areas of high radiation should be indicated on the 3D model and allow for the insertion of proper shielding for use in engineering analysis and specifications.
- Provide real-time navigation through the 3D-rendered environment.
- Allow highlighting components and seamlessly provide information on components from the simulator platform database – should also update changes to the simulator database.

3.2.3. Conclusion

In this chapter we described the principles when using a real-time plant simulators running in parallel with a nuclear plant to predict the control system behaviour and highlighting unexpected plant behaviour. The basis of the theory is established together with preliminary results. The control and protection architecture for implementation is developed and described and the system requirements of a nuclear plant simulator that would enable the proposed system were described.

In the following chapter the method to adapt plant measurements that isolates the control actions on the fault and re-introduces it into the measurement data, thereby improving plant diagnostic performance will be developed and described.

4. Article 2: Adapting plant measurement data to improve hardware fault detection performance in Pressurised Water Reactors.

By A.C. Cilliers and E.J. Mulder

School of Nuclear and Mechanical Engineering

North West University

This peer-reviewed paper was published in *Annals of Nuclear Energy* 49 (2012) pp. 81 - 87, after being presented at the Predictive Maintenance of South Africa (PdMSA), Johannesburg, South Africa, October 2011.

4.1. Relative contributions by authors

E.J. Mulder acted as study leader during this stage of the research with the task to provide guidance and support to A.C. Cilliers whilst also evaluating the academic soundness and strength of the research. All research was conducted and documented by A.C. Cilliers.



Adapting plant measurement data to improve hardware fault detection performance in pressurised water reactors

A.C. Cilliers*, E.J. Mulder

North West University, School for Mechanical and Nuclear Engineering, Hoffman Street, Potchefstroom, North West Province 2530, South Africa

ARTICLE INFO

Article history:

Received 28 February 2012

Received in revised form 28 May 2012

Accepted 29 May 2012

Keywords:

Nuclear plant safety

Diagnostics

Fault detection

Predictive maintenance

ABSTRACT

With the fairly recent adoption of digital control and instrumentation systems in the nuclear industry a lot of research now focus on the development expert fault identification systems. The fault identification systems enable detecting early onset faults of fault causes which allows maintenance planning on the equipment showing signs of deterioration or failure. This includes valve and leaks and small cracks in steam generator tubes usually detected by means of ultrasonic inspection.

Detecting faults early during transient operation in NPPs is problematic due to the absence of a reliable reference to compare plant measurements with during transients. The distributed application of control systems operating independently to keep the plant operating within the safe operating boundaries complicates the problem since the control systems would not only operate to reduce the effect of transient disturbances but fault disturbances as well.

This paper provides a method to adapt the plant measurements that isolates the control actions on the fault and re-introduces it into the measurement data, thereby improving plant diagnostic performance.

© 2012 Elsevier Ltd. All rights reserved.

1. Introduction

All online plant diagnostic approaches rely on the availability of a reference to compare the measured plant output to. With the use of plant training simulators in the nuclear industry since the 1980s and the continual improvement of computational speed and mathematical modelling methods, with increasing processing speed and improving model accuracies a full scope engineering simulator running in real time becomes the ideal reference to indicate faulty plant behaviour and degradation of plant hardware.

With this availability and advances in nuclear power plant simulation technology, a research project was initiated to make use of simulators to provide a deterministic dynamic reference for in-transient fault detection (Cilliers et al., 2011).

The primary objectives of the research were to:

1. Develop an early fault detection system by using real time simulators of nuclear power plants, continuously monitoring and comparing simulated measurement data and control outputs of the model reference adaptive control negative feedback system with the actual measured data and control outputs from the plant. The fault detection system should detect small faults that would normally go undetected as well as detect faults during plant operating transients.

2. Develop a fault characterisation method, making use of measured and simulated data together with the actual and simulated control system response. The fault characterisation system should provide information on the magnitude and location of the fault.
3. Develop a control and protection framework that allows NPP licensing within the existing licensing framework, but is still able to uncover the benefits of expert control and protection systems.

This paper introduces a section of the first objective, with following papers presenting the second and third objectives.

Petersen and McFarlane (2004) define the requirements for process fault detection and diagnosis as the following:

- the availability of well defined, accurate first principles models (with any modelling errors also suitably represented),
- clearly identified fault modes and models to represent these, and
- appropriately located sensors (often with levels of redundancy).

We have found these requirements to also be generic requirements applicable to the fault identification system developed as part of this research.

Plant diagnostics in the Instrumentation and Control discipline has been researched and developed over the last 40 years with various methods of providing dynamic reference models. In 1976, Willsky (1976) examined statistical techniques for the detection

* Corresponding author. Tel.: +27 829202954; fax: +27 866648796.

E-mail address: cilliean@eskom.co.za (A.C. Cilliers).

Adapting plant measurement data to improve hardware fault detection performance in Pressurised Water Reactors.

ABSTRACT

With the fairly recent adoption of digital control and instrumentation systems in the nuclear industry a lot of research now focus on the development expert fault identification systems. The fault identification systems enable detecting early onset faults or fault causes which allows maintenance planning on the equipment showing signs of deterioration or failure. This includes valve and leaks and small cracks in steam generator tubes usually detected by means of ultrasonic inspection.

Detecting faults early during transient operation in NPPs is problematic due to the absence of a reliable reference to compare plant measurements with during transients. The distributed application of control systems operating independently to keep the plant operating within the safe operating boundaries complicates the problem since the control systems would not only operate to reduce the effect of transient disturbances but fault disturbances as well.

This paper provides a method to adapt the plant measurements that isolates the control actions on the fault and re-introduces it into the measurement data, thereby improving plant diagnostic performance.

1. Introduction

All online plant diagnostic approaches rely on the availability of a reference to compare the measured plant output to. With the use of plant training simulators in the nuclear industry since the 1980's and the continual improvement of computational speed and mathematical modelling methods, with increasing processing speed and improving model accuracies a full scope engineering simulator running in real time becomes the ideal reference to indicate faulty plant behaviour and degradation of plant hardware.

With this availability and advances in nuclear power plant simulation technology, a research project was initiated to make use of simulators to provide a deterministic dynamic reference for in-transient fault detection (Cilliers et al, 2011).

The primary objectives of the research were to:

1. Develop an early fault detection system by using real time simulators of nuclear power plants, continuously monitoring and comparing simulated measurement data and control outputs of the model reference adaptive control negative feedback system with the actual measured data and control outputs from the plant. The fault detection system should detect small faults that would normally go undetected as well as detect faults during plant operating transients.
2. Develop a fault characterisation method, making use of measured and simulated data together with the actual and simulated control system response. The fault characterisation system should provide information on the magnitude and location of the fault.

3. Develop a control and protection framework that allows NPP licensing within the existing licensing framework, but is still able to uncover the benefits of expert control and protection systems.

This paper introduces a section of the first objective, with following papers presenting the second and third objectives.

Petersen and McFarlane (2004) define the requirements for process fault detection and diagnosis as the following:

- the availability of well defined, accurate first principles models (with any modelling errors also suitably represented),
- clearly identified fault modes and models to represent these, and
- appropriately located sensors (often with levels of redundancy).

We have found these requirements to also be generic requirements applicable to the fault identification system developed as part of this research.

Plant diagnostics in the Instrumentation and Control discipline has been researched and developed over the last forty years with various methods of providing dynamic reference models. In 1976, Willsky (1976) examined statistical techniques for the detection of failures in dynamic systems revealing key concepts, similarities and differences in problem formulations, system structures, and performance. Specifically, they discussed the problem of detecting abrupt changes in dynamic systems.

Chen and Howell (2001) notes that statistical and learning methods are fast and do not require a plant model, but are comparatively brittle because they cannot handle situations that are not explicitly anticipated. The 'brittleness' referred to makes the implementation of heuristic methods particularly problematic in the nuclear industry where deterministic proof of system dependability is required.

Simani and Fantuzzi (2000) notes that Fault Detection Systems have been widely developed during recent years with model-based methods, fault tree approaches and pattern recognition techniques amongst the most common methodologies utilized in such tasks with neural networks used in Fault detection problems for model approximation and pattern recognition.

Iserman (2004) presented an introduction into the fault detection field by describing how model-based methods of fault detection were developed by using input and output signals and applying dynamic process models. These methods are based on amongst others, parameter estimation, parity equations or state observers. Also signal model approaches were developed with goal is to generate several symptoms indicating the difference between nominal and faulty status. Based on different symptoms fault diagnosis procedures follow, determining the fault by applying classification or inference methods.

The development of steady state fault detection systems making use of the steady state references to detect control operation deviations in the nuclear industry has been done since 2000 with Chen and Howell (2001) commenting:

“Little has been written about distributing diagnostic tasks presumably because traditionally, the diagnostic engineer’s view of feedback control is that it complicates, rather than aids, diagnostic reasoning. Feedback control adds to the complexity of fault detection in process plants by masking measurement deviations that might indicate a fault”.

Also, Hamelin and Sauter (2000) realised that most of the developed algorithms make many idealised assumptions such as steady state conditions which are very often not satisfied, since in reality the system parameters may either be uncertain or time dependent, resulting in a mismatch between the actual system and the associated mathematical model used for reference. They state that even though the problem of uncertain parameters is of crucial importance to the industrial implementation of fault detection methods, it has however received little attention with only a handful of works so far devoted to it. Hamelin and Sauter (2000) also state that future developments should concern the incorporation of the proposed approach into a closed-loop system stating that: “Clearly, in a closed-loop system, the controller gain will also have an effect on the residual output.”

This fault masking effect is compounded during expected plant transients when the various control systems are operating to return the plant to steady state. The fault masking effect of the control system prevents making plant diagnostics very difficult when small slow acting faults occur.

To address the fault masking effect of the feedback control system, not only are the measurements and simulated measurements compared, but also the simulated and actual control operations. With the primary objective being to improve plant performance and fault detection dependability, a secondary benefit was achieved when early onset faults are detected while the control system manages to mask the fault completely. These faults often take a long time to develop large enough for conventional plant protection systems to detect the fault condition.

The benefits from detecting early onset faults are the ability to execute online maintenance on the affected systems when possible or plan maintenance on these systems during outages. This results in increased uptimes as well as the reduction of efficiency losses due to faults.

This was also used by Roy et al. (1998) who developed a fault characterisation system to address the need to have improved predictive maintenance techniques in an operating plant. Guidance into the methodology came from one of the earliest applications of state estimation based fault detection methods in nuclear plants. Roy et al.’s (1998) primary objective was to provide an early warning to the human operator regarding the failing health of control equipment, in the process averting major breakdown with its associated large plant downtime.

2. Fault masking by the control system

It is important to keep in mind that the purpose of the control system is to control the output of the nuclear plant, thus continuously providing control variables to steer the plant to reach the reference value. The only reasonable method of control in nuclear plants is closed-loop negative feedback control as opposed to an open-loop system as depicted in Fig. 1. The closed-loop is depicted in Fig. 2

using a block diagram. A block diagram representation of the system relationships is prevalent in control system engineering. The control diagrams are analysed in the 's' domain, this allows analysing steady state and transient conditions in state-change domain, rather than the time domain. This is used to model linear time-invariant systems and responses as a function of the input and output (transfer function) of the system.

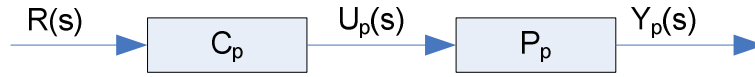


Fig. 1. Open-loop system

The closed-loop control system compares output values with a reference. This reference indicates a desired value, and the difference between the reference and measured values is used to set the control variable. This is not done to raise alarms or identify faults; in fact, the difference between the reference and the measured value is expected, since the reference value is set to the value the operator wants the plant to reach.

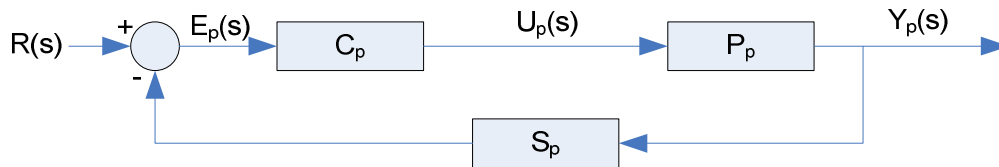


Fig. 2. Closed-loop control system

With:

- $R(s)$ representing the reference the output is compared to,
- $C_p(s)$ representing the control system,
- $P_p(s)$ representing the plant,
- $S_p(s)$ representing the sensor or measurement equipment, and
- $E_p(s)$ represents the error between the reference value and the output from the measurement equipment.

In the case of the Model Reference Adaptive Control (MRAC) system introduced by H Whitaker in 1958, the plant is controlled to follow a reference model provided by a lookup table. The reference value $R(s)$ would change to allow various plant conditions. In many cases, such a variable reference is used with the reference value sourced from a lookup table, as in the case of a typical Generation II PWR we consider in this research. When the reference is changed the control system should follow to produce an output as close as possible to the reference. Analysing the feedback control loop confirms this:

$$E_p(s) = R(s) - S_p(s)Y_p(s) \quad (1)$$

and

$$Y_p(s) = C_p(s)P_p(s)E_p(s) \quad (2)$$

thus

$$E_p(s) = R(s) - S_p(s)C_p(s)P_p(s)E_p(s) \quad (3)$$

resulting in

$$E_p(s) = \frac{1}{1+S_p(s)C_p(s)P_p(s)} R(s) \quad (4)$$

To ensure a steady state error as close as possible to 0, $S_p(s)C_p(s)P_p(s)$ needs to be selected as large as possible over the operating range of s . Since $P_p(s)$ is the model of the plant, only $S_p(s)$ and $C_p(s)$ can be selected by the control system designer. The effect of the control system designed to follow a changing reference also affects the system's response to disturbances or faults.

Making use of a closed loop negative feedback configuration has specific benefits that make its use attractive to the control system engineer:

- disturbance effect rejection,
- guaranteed performance even with model uncertainties, when the model structure does not match the real process perfectly,
- unstable processes can be stabilised,
- reduced sensitivity to parameter variations, and
- improved reference-tracking performance.

These benefits of the closed-loop negative feedback control system which is implemented behind the measured outputs of the plant reduces the effect of a fault introduced (disturbance effect rejection) into the system. For this reason a system designed to detect small faults or faults during transients cannot only compare the measured output of the plant with the simulated output, as the control system in the plant is working behind the measurements to maintain certain operating levels.

3. Measurement adaptation process

To develop a measurement adaptation process method that will cancel the fault masking and transient effect in order to have a meaningful plant measurement as reference with the simulated measurements, we make use of the primary functionality of any control system – to react to any external disturbance with an opposite response. For an ideal zero steady state error system, the eventual response is the negative equivalent of the external disturbance in order to keep certain variables within the allowed limits. This allows us to treat any faulty operation the same as a plant control system input (with the opposite effect) resulting in moving the various operating points away from the design value. The principle is formalised by stating that the objective of an effective plant control system is that:

For every possible movement of the operating point, expected or unexpected, a control and instrumentation (I&C) system is in place to counteract the movement until the I&C system is operating at maximum capacity and is unable to counteract the movement.

The implication: for every possible movement a fault induces in an operating point, a corresponding control function could counteract the movement. Since a control system is designed to move the operating point in any direction, a control operation should also exist that could replicate the movement that the fault induces in the system. This is made possible by the use of real time engineering simulators in the nuclear industry. In other words, having access to all plant inputs, except

the fault input, and having access to all outputs, expected and measured, as well as the expected and actual actuation signals, allows the calculation of the fault disturbance as a control input.

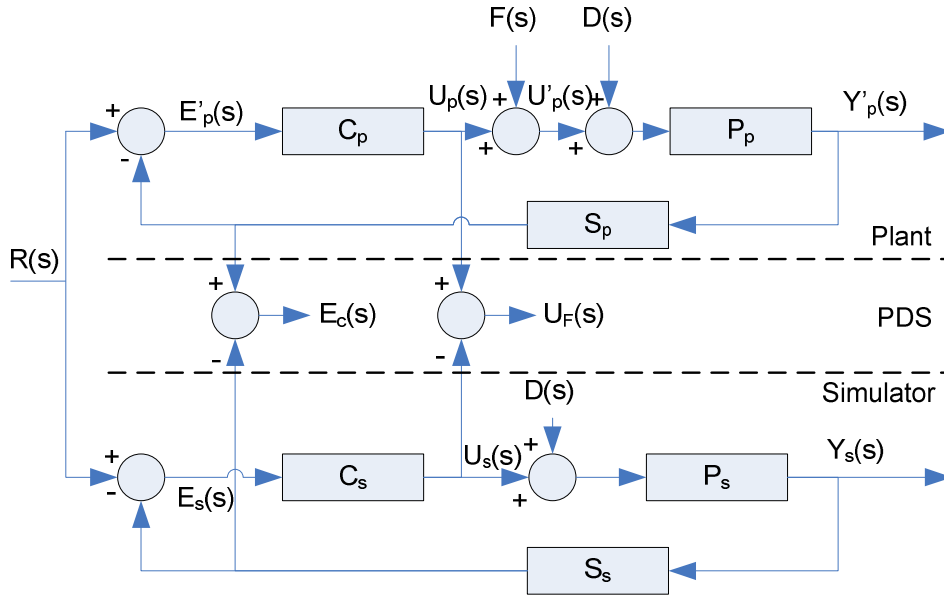


Fig. 3. Fault identification control diagram

In Fig. 3, the system to compare control variables as well as measured outputs is depicted. Since $E_c(s)$ does not provide enough information to detect small faults, we introduce an additional comparison point $U_F(s)$ comparing the controller outputs. For an acceptably accurate plant simulation model the measured and simulated measurements and control variables should be the same for all non-fault plant operating conditions and transients, since the simulator would be provided with the same reference input $R(s)$ as well as expected disturbances $D(s)$ due to changing operating conditions. The simulator would not be supplied with unexpected disturbances or faults $F(s)$ since a fault is an unpredictable event.

$U_F(s)$ can be calculated from Fig. 1 when $D(s) \neq 0$.

$$U_F(s) = U_p(s) - U_s(s) \quad (5)$$

And

$$U_p(s) = C_p(s)E'_p(s) \quad (6)$$

while

$$U_s(s) = C_s(s)E'_s(s) \quad (7)$$

$$E'_p(s) = R(s) - S_p(s)Y'_p(s) \quad (8)$$

Substituting (8) into (6) produces:

$$U_p(s) = C_p(s) \left(R(s) - S_p(s)Y'_p(s) \right) \quad (9)$$

and

$$U_p(s) = C_p(s)R(s) - C_p(s)S_p(s)Y'_p(s) \quad (10)$$

To solve the unknown plant output we write from Fig. 3:

$$Y'_p(s) = C_p(s)P_p(s)E'_p(s) + P_p(s)F(s) \quad (11)$$

and substituting (8) into (11) we get:

$$Y'_p(s) = \frac{C_p(s)P_p(s)}{1+C_p(s)P_p(s)S_p(s)}R(s) + \frac{P_p(s)}{1+C_p(s)P_p(s)S_p(s)}F(s) \quad (12)$$

and so, by substituting (8) into (6) we produce:

$$U_p(s) = \left(C_p(s) - \frac{S_p(s)C_p(s)^2P_p(s)}{1+C_p(s)P_p(s)S_p(s)} \right) R(s) - \frac{C_p(s)S_p(s)P_p(s)}{1+C_p(s)P_p(s)S_p(s)} F(s) \quad (13)$$

Then, if $C_p(s)S_p(s)$ is selected to be much greater than 1 over the designed range of s to achieve a zero steady state error, we obtain the approximate result:

$$U_p(s) \approx (C_p(s) - C_p(s))R(s) - F(s) \quad (14)$$

and subsequently

$$U_p(s) \approx -F(s) \quad (15)$$

In the same way we derive that for the simulator under the same conditions:

$$U_s(s) = \left(C_s(s) - \frac{S_s(s)C_s(s)^2P_s(s)}{1+C_s(s)P_s(s)S_s(s)} \right) R(s) - \frac{C_s(s)S_s(s)P_s(s)}{1+C_s(s)P_s(s)S_s(s)} D(s) \quad (16)$$

Thus, if $C_s(s)S_s(s)$ is selected to be much greater than 1 over the designed range of s to achieve a zero steady state error, we obtain the approximate result:

$$U_s(s) \approx -D(s) \quad (17)$$

and since

$$U_F(s) = U_p(s) - U_s(s) \quad (18)$$

then

$$U_F(s) \approx -F(s) \quad (19)$$

The result is valid as long as the control instrumentation remains in designed operating region and is not expected to operate beyond the maximum capabilities (for all small faults). If the control system is operating close to the limits of its linear region due to the $D(s)$ disturbance, the plant will be unable to compensate for the combination of $D(s) + F(s)$ disturbance and only a partial masking of the fault by the control system will occur. Thus, the result of (19) will only show the partial fault that was masked.

The fault information now available to the fault detection system provides a more realistic presentation as to the state of the plant. While the control system is keeping the plant within the accepted operating region the fault detection system has access to the expected plant measurements from the simulator as well as the measurements from the plant if the fault effect was allowed to move the operating point beyond the safe plant limitations. From these two sets of information fault detection is realised in two ways:

1. If the expected and simulated plant measurements drift away from each other beyond the known accuracy of both the measurement equipment and the simulation the plant can be said to be behaving unexpected and a fault is detected.
2. Since the control system maintains the operating point within the safe operating region, the conventional protection system will only detect a fault once the control system is unable to compensate for the effect of the fault and a trip set point is reached. Having access to the adapted

measurements information these conventional trip set points will react much sooner as a fault is detected earlier.

4. Reintroducing the fault information into the measurement data

Comparing the control operation of the plant with the control operation of the simulator as derived in (19), provides the inverse of the unexpected (fault) input to the plant. With the fault input to the system known, it would be useful to use this fault information to calculate the effect it would have on the plant if the control system did not compensate for the fault, while still compensating for expected disturbances. This would produce measured values from the plant with the full effect of the fault visible.

This is achieved by introducing the effect of the fault back into the plant measurements $Y'_p(s)$ outside the closed loop as depicted Fig. 4.

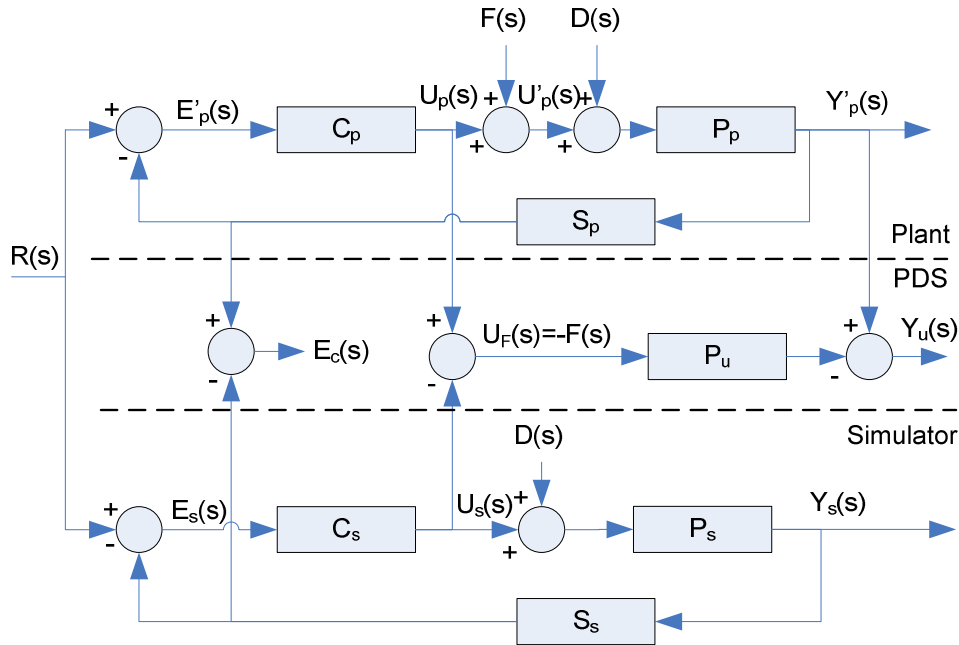


Fig. 4. Unmasked measurement generation diagram

We have shown in that:

$$Y_p(s) = \frac{C_p(s)P_p(s)}{1+C_p(s)P_p(s)S_p(s)}R(s) + \frac{P_p(s)}{1+C_p(s)P_p(s)S_p(s)}F(s) + \frac{P_p(s)}{1+C_p(s)P_p(s)S_p(s)}D(s) \quad (20)$$

and from Figure 2 the $Y_u(s)$ becomes:

$$Y_u(s) = \frac{C_p(s)P_p(s)}{1+C_p(s)P_p(s)S_p(s)}R(s) + \frac{P_p(s)}{1+C_p(s)P_p(s)S_p(s)}F(s) + \frac{P_p(s)}{1+C_p(s)P_p(s)S_p(s)}D(s) + P_u(s)F(s) \quad (21)$$

Since $C_p(s)S_p(s)$ is selected to be much greater than 1 over the designed range of s to achieve a zero steady state error, we obtain the approximate result:

$$Y_u(s) \approx \frac{1}{S_p(s)}R(s) + \frac{1}{C_p(s)S_p(s)}F(s) + \frac{1}{C_p(s)S_p(s)}D(s) + P_u(s)F(s) \quad (22)$$

With $\frac{1}{C_p(s)S_p(s)}F(s) + \frac{1}{C_p(s)S_p(s)}D(s)$ approaching 0 for large values of $C_p(s)S_p(s)$ and results in:

$$Y_u(s) \approx \frac{1}{S_p(s)}R(s) + P_u(s)F(s) \quad (23)$$

The resulting equation (23) provides a result resembling the reference output with the effect of the expected disturbance ($D(s)$) and unexpected fault reduced ($F(s)$) by the closed loop and the effect of the unexpected fault reintroduced outside the control loop. The result includes the complete effect of the fault since the portion of the fault that was masked by the control system is reintroduced into the system in an open loop.

It is important to note that although the control system response is linear, the plant itself, and the plant model might have a non-linear response to disturbance inputs. As such, care should be taken in implementing the described equations only as small incremental changes around operating point of the previous time step. In the following example, the equations were implemented in this way. The result was benchmarked against a simulation where the same expected and faulty disturbance was introduced, but the control system was limited to only responding to the expected transient disturbance and not the fault disturbance. The exact same results were obtained.

5. In-transient fault example

During a transient operation with $D(s) \neq 0$ it is difficult to detect a fault $F(s)$ since the plant operating point is in transition as well as the control systems are actively operating to reduce the effect of $D(s)$.

By making use of a typical example (small primary system coolant leak during load change), the two sets of information are depicted in Fig. 5. Here the measured and simulated pressures are depicted during the load change transient and a loss of coolant accident fault. By comparing the expected and actual control system operations, the compensating effect of the actual control system is removed from the measured data and plotted as uncompensated pressure. This pressure line shows us what the reactor coolant system pressure would have been, if the control system only attempted to control the disturbance due to the expected transient $D(s)$ and not the unexpected fault input $F(s)$.

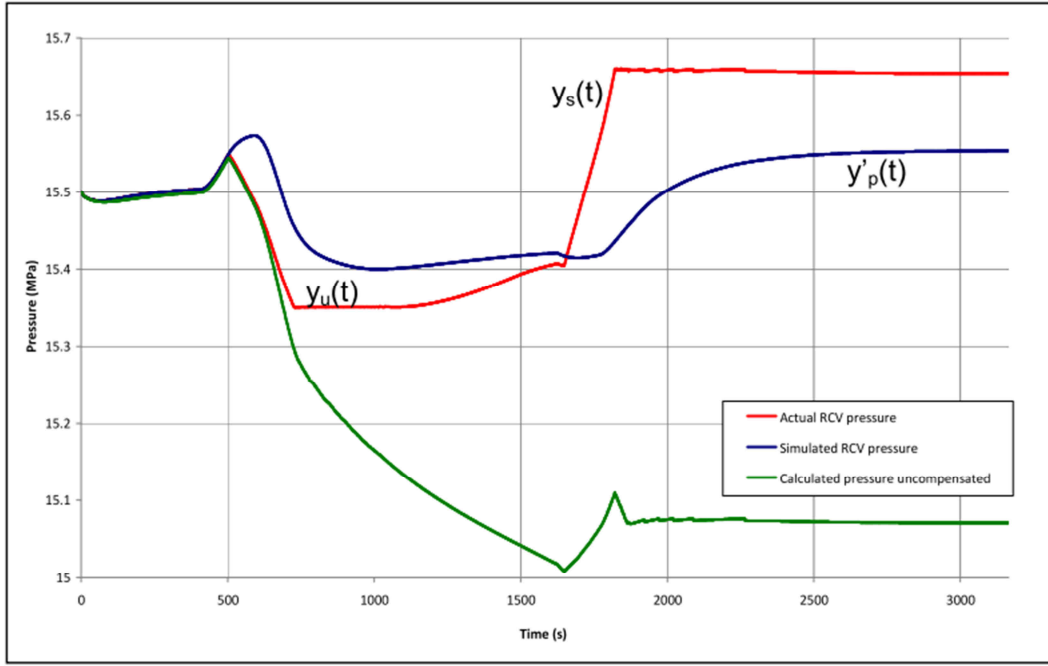


Fig. 5. In-transient pressure measurement and adapted measurement

This adapted measurement can now be used as against a reference to detect faults as soon as they start having an effect on the plant output or the control system. The method is based on first principles plant modelling and as such provides a deterministic measurement adaptation that starts deviating from the reference as soon as the plant hardware start to degrade in operation.

6. Inaccuracies in the plant model or measurement equipment

When using plant models to adapt the plant measurement output, the effect of inaccuracies in the model need to be evaluated. The accuracy of the model is affected by the numerical method used as well as the level of discretisation. These inaccuracies can always be known throughout the simulating process. Since the inaccuracies in the process and in the measuring equipment are known, an error band can be created around the adapted measurement to prevent faulty trips. The effect of a magnitude error in the plant model however does not directly correlate to the error of the output. To evaluate this effect we introduce an inaccuracy factor (ϵ) into the simulator physics and instrumentation model and we set:

$$(1 + \epsilon)P_p(s)S_p(s) = P_s(s)S_s(s) \quad (24)$$

and so (19) becomes:

$$\begin{aligned} U_F(s) = & \left(\frac{1 + \epsilon_1}{1 + (1 + \epsilon_1)C(s)P_p(s)S_p(s)} - \frac{1}{1 + C(s)P_p(s)S_p(s)} \right) S_p(s)P_p(s)C(s)^2R(s) \\ & - \left(\frac{1}{1 + C(s)P_p(s)S_p(s)} - \frac{1 + \epsilon_2}{1 + (1 + \epsilon_2)C(s)P_p(s)S_p(s)} \right) S_p(s)P_p(s)C(s)D(s) \\ & - \frac{C(s)S_p(s)P_p(s)}{1 + C(s)P_p(s)S_p(s)} F(s) \end{aligned} \quad (25)$$

Writing the terms in brackets over a common denominator:

$$\begin{aligned}
U_F(s) = & \left(\frac{\varepsilon_1}{(1 + \varepsilon_1 C(s)P_p(s)S_p(s) + C(s)P_p(s)S_p(s))(1 + C(s)P_p(s)S_p(s))} \right) S_p(s)P_p(s)C(s)^2 R(s) \\
& + \left(\frac{\varepsilon_2}{(1 + C(s)P_p(s)S_p(s))(1 + \varepsilon_2 C(s)P_p(s)S_p(s) + C(s)P_p(s)S_p(s))} \right) S_p(s)P_p(s)C(s)D(s) \\
& - \frac{C(s)S_p(s)P_p(s)}{1 + C(s)P_p(s)S_p(s)} F(s)
\end{aligned} \tag{26}$$

Equation 26 results in a multiplication factor of both the reference input $R(s)$ and the disturbance input $D(s)$, both of which should reduce to zero for the error to have a minimal effect on the resulting $U_F(s)$.

In Fig. 6 the resulting multiplication factors are depicted for different errors and changing values of $C(s)P_p(s)S_p(s)$. From the control system design objectives we know that $C(s)P_p(s)$ is designed to be much larger than 1 for all anticipated frequencies, and so both the disturbance and the reference input should reduce to values very close to zero. This division of fault effect can be attributed to the effect of the closed loop control system to adapt to model uncertainties.

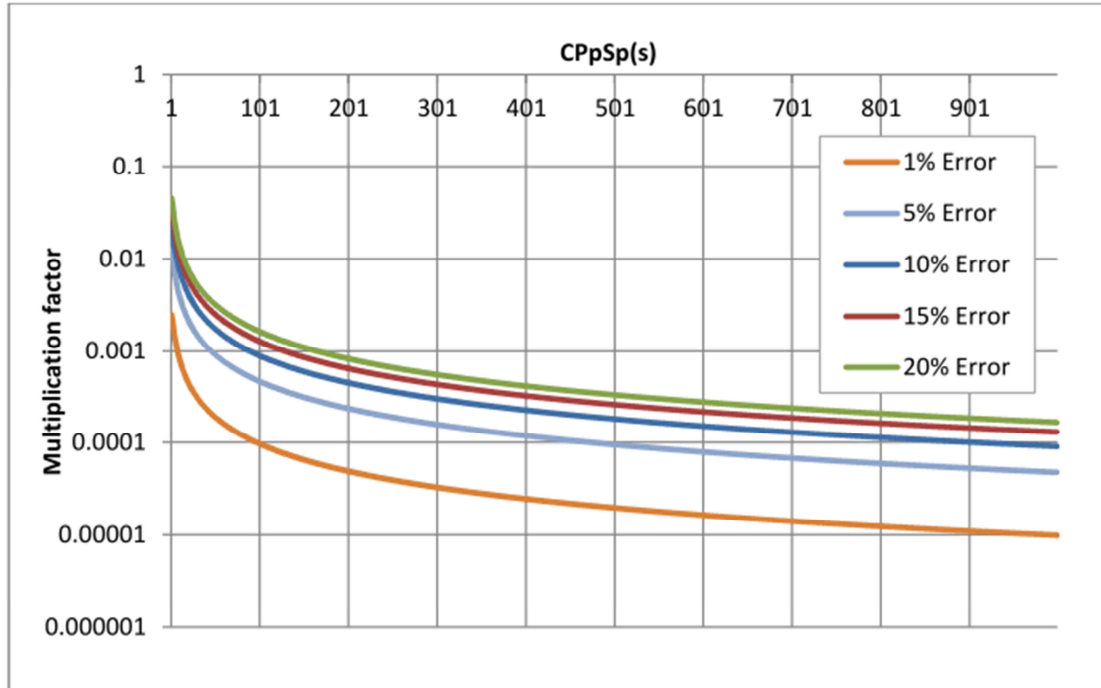


Fig. 6. Multiplication factor for changing values of $C(s)P_p(s)S_p(s)$ due to inaccuracy

7. Conclusion

We have shown that having an accurate first principles real time simulator available aid in fault detection and characterisation.

The methods developed in this research are applicable to all industries, unfortunately not all industries could benefit from this right away, as the nuclear industry are unique in a few instances:

Plant operation simulators as a dynamic reference as Nuclear power plants can easily be implemented as nuclear power plants have rather slow dynamics, with control systems using transfer functions with time constants in the order of seconds or even minutes. This allows a first principles approach in plant

operations modelling to be done to a high level of accuracy, and in real time. Other industries might find that developing a model of a plant based on first principles to be used as a dynamic reference is expensive and time consuming (Chen and Howell, 2001). Nuclear plants, on the other hand are required to be equipped with engineering and training simulators. This can now be used to provide a first principles dynamic reference for a fault detection system.

Fault detection systems based on neural networks are effective but brittle. The implementation of such systems will be difficult in the nuclear industry because of the uncertainties associated with such systems (Embrechts, 2004). The possibility of developing a fault detection system based on neural networks is eliminated, whereas this type of fault detection method could serve other industries very well.

The problems addressed in this research are applicable to all industries, but especially effective in the nuclear industry as described above, the problems addressed were:

The effectiveness of fault detection systems are diminished by the closed loop response of the control system to disturbances (Hamelin and Sauter, 2004). A method is developed in this research to measure the effect of the fault on the system without the closed loop response of the control system.

During expected transients the effect of the fault is hidden further due to the operation of the control system on both the fault and the expected disturbance. A method is developed in this research to measure only the fault effect on the system outside the closed loop control system.

Fault characterisation methods rarely make use of distributed control systems due to the fault hiding effect of the control system. Having a method that produces the full effect of the fault on each subsystem allows distributed control systems to be used in fault characterisation. It should prove effective in the sense that each subsystem responds differently to the fault disturbance and each should reveal a part of the nature and cause of the fault.

The results in this research are made possible by having access to real time plant data and being able to perform manipulations on the data. The method of using a real time plant simulator to provide expected measurement and control data produce a clear picture of the component and system health is only one example of making effective use of available plant data.

8. References

- Chen, J., Howell, J., 2001. A self-validating control system based approach to plant fault detection and diagnosis. *Computers and Chemical Engineering*. 25, 337-358.
- Cilliers, A.C., Nicholls, D., Helberg, A.S.J., 2011. Fault detection and characterisation in Pressurised Water Reactors using real-time simulations, *Annals of Nuclear Energy*. 38, 1196-1205.
- Embrechts, M.J., 2004. Hybrid Identification of Nuclear Power Plant Transients With Artificial Neural Networks. *IEEE transactions on industrial electronics*. 51:3, 686-693.

- Hamelin, F., Sauter, D., 2000. Robust fault detection in uncertain dynamic systems. *Automatica*. 36, 1747-1754.
- Iserman, R., 2004. Model-based fault detection and diagnosis – status and applications. Institute of Automatic Control, Darmstadt University of Technology.
- Petersen, I.R., McFarlane, D.C., 2004. A methodology for robust fault detection in dynamic systems, *Control Engineering Practice*. 12, 123–138.
- Roy, K., Banavar, R.N., Thangasamy, S., 1998. Application of Fault Detection and Identification (FDI) Techniques in Power Regulating Systems of Nuclear Reactors. *IEEE Transactions on nuclear science*. 45:6, 3183-3201.
- Simani, S., Fantuzzi, C., 2000. Fault diagnosis in power plant using neural networks. *Information Sciences*. 127, 125-136.
- Willsky, A.S., 1976. A Survey of Design Methods for Failure Detection in Dynamic Systems. *Automatica*. 12, 601-611.

4.2. Additional notes

For more information on how the equations in the above article is utilised to generate the uncompensated fault, the additional notes is provided.

The calculation that as performed in Fig 4. is:

$$Y_u(s) = Y'_p(s) - P_u(s)(U_p(s) - U_s(s)) \quad (4.1)$$

with all variables known except $P_u(s)$.

The plant process model $P(s)$ is based on the physics of the actual process in the plant and implemented in the simulator, unfortunately $P(s)$ as it is used in the simulator is not available to implement separately outside the negative feedback control loop as the simulator code is proprietary. It is therefore required to model the effect of $P(s)$ for each process to enable the use of $P(s)$.

4.2.1. Deriving the plant process from the simulator

The process of deriving a model for $P(s)$ is described at the hand of the RCS pressure control system as depicted in Fig. 4-1.

The pressure control system uses measured pressure from the plant and compares it to the reference pressure. The error signal is fed into the control system that calculated a pressuriser heater operation to increase the pressure, or a coolant spray valve opening to reduce the pressure. In the case of RCS pressure $U(s)$ is a heater or valve operation. Subsequently $U_f(s) = -F(s)$ would also be heater or valve operation. $P(s)$ receives the heater or valve operation and translates it to a pressure increase or decrease.

To determine $P(s)$, the heater and valve operations are set to various values in turn, and then recording the effect it has on the pressure.

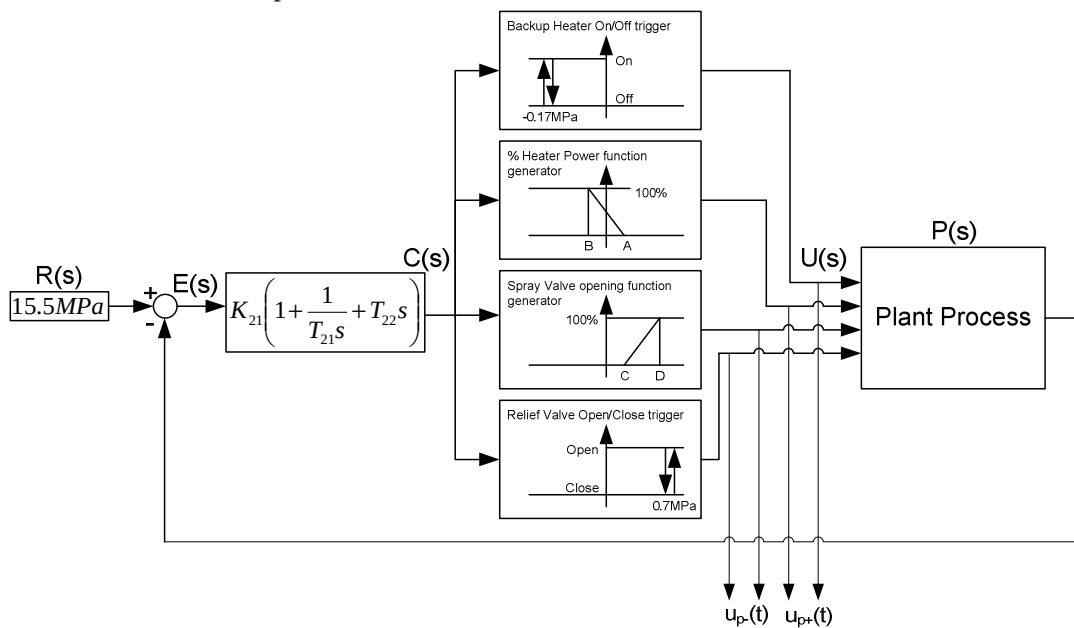


Fig. 4-1. Pressure control block diagram

In Fig. 4-2 4-2 it can be seen that, for example, if the heater is at 10% the pressure would increase at a rate of 0.3544 MPa per second and so it can be accepted that the effect of a fault is to reduce the RCS pressure at a rate of 0.35444 MPa per second.

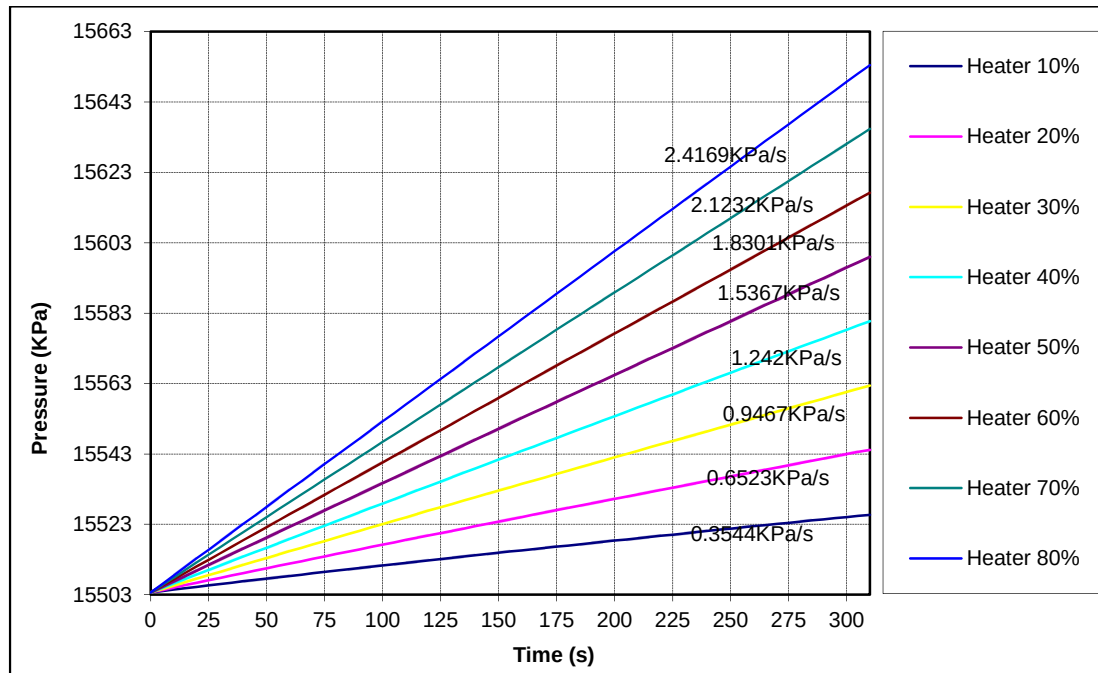


Fig. 4-2. Pressuriser heater effect on pressure in time

From Fig. 4-2 the rate of pressure change can be plotted against heater power as is done in Fig 4-3. Adding a trend line through the data points result in a straight line through all the points indicating a linear relationship between the rate of pressure change and the heater power. The gradient of the line indicates that for every 1% increase in heater power the pressure will increase at 0.2987KPa/s.

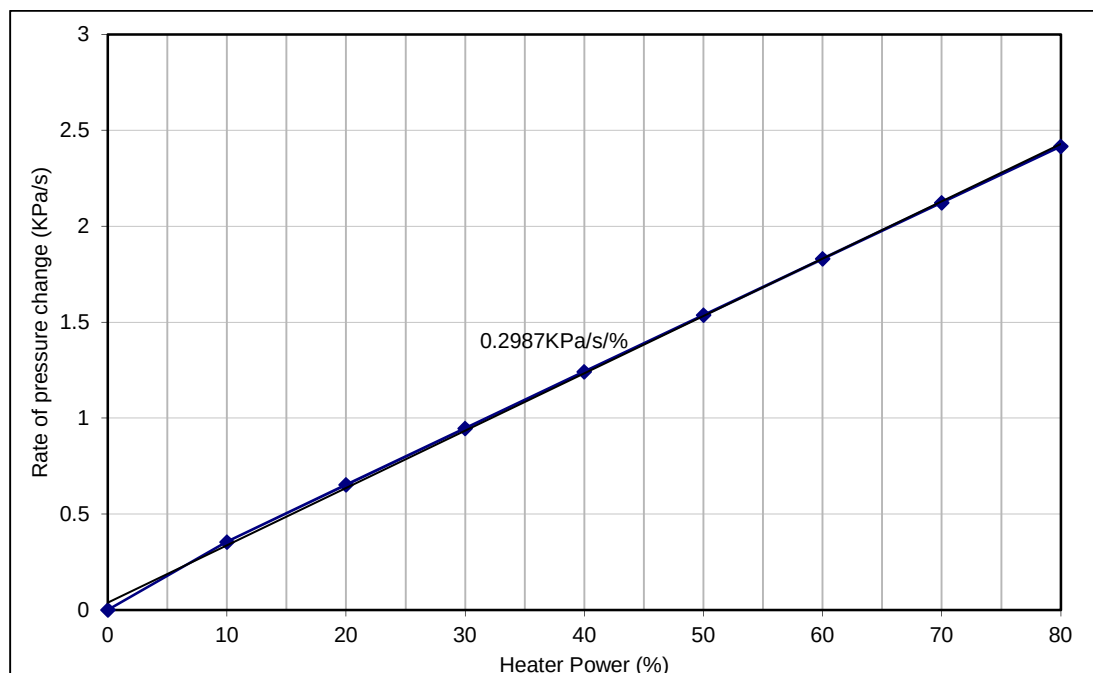


Fig. 4-3. Pressuriser heater power effect on pressure change rate

Having access to the simulator $P(s)$ models makes the process of removing the fault compensating effect of the control system less troublesome since the simulator calculates the measurements as well as the response of the plant. The described process of obtaining the plant process would thus be unnecessary.

With a model of the plant process $p(t)$ available in the time domain, and $U_f(s)$ calculated as $u_f(t) = u_p(t) - u_s(t)$ in real time as it is received from the simulator, the plant response can be calculated in the time domain as well.

The equivalent time domain calculation for the uncompensated pressure (4.1) taking a single sample at time $t = 0$:

$$y_u(0) = y'_p(0) - p_u(0)(u_p(0) - u_s(0)) \quad (4.2)$$

with:

- y_u the uncompensated pressure, $y_u(0)$ at time $= 0$,
- y'_p the pressure measurement from the plant and reference the effect is subtracted from, $y'_p(0)$ at time $= 0$,
- p_p the effect on the measured output due to the control system minimizing the effect of the fault, $p_u(0)$ at time $= 0$,
- u_p the control instrumentation operation on the faulty and expected disturbance input, and
- u_s the control instrumentation operation on the expected disturbance input only.

Since $y_u(t)$ is starting to deviate from the measured $y'_p(t)$ once the fault is introduced (for $t > 0$), to calculate $y_u(1)$ the reference is now not $y_p(1)$ as it would have been if using (4.1) but $y_u(1) - (y'_p(1) - y'_p(0))$ so the general formula for calculating the uncompensated measurement is:

$$y_u(t) = y_u(t-1) - (y'_p(t) - y'_p(t-1)) - p_u(0)(u_p(0) - u_s(0)) \quad (4.3)$$

The difference between up and us denotes the component of the control instrumentation operating to reduce the effect of the fault disturbance. This is then multiplied by the effect (p_u) of the control instrumentation on the measurement to produce the plant response to the fault disturbance.

In the case of the pressuriser heater $p_u(t) = 0.2987\text{KPa/s/Heater}\%$ which is a constant.

In some cases $p_u(t)$ would not be a constant linear relationship in change and $p_u(t)$ could also be piecewise constant depending on another parameter (in the case of the heater and pressure the relationship is constant between 13 MPa and 15.65 MPa), or any other relationship to the measured output could be used. The advantage of having a simulator code at hand is that these relationships have already been implemented in the simulator code.

Analysing (4.2) and (4.3) reveals that when $u_p(t) = u_s(t)$ the compensating effect in the system is 0. This is expected, since the control system is not compensating for any unexpected transients or fault Conditions.

By removing the masking of the fault effect of the control instrumentation from the measured data, we produce transient data with only the expected disturbance behaviour apparent. It should be mentioned that, up to this point, the actual plant is operating exactly as it normally would. All fault isolation calculations are made simply from data being fed to the PDS from the plant, with two sets of 'measured' data now available for diagnostic purposes.

4.2.2. Conclusion

In this chapter the method to adapt plant measurements that isolates the control actions on the fault and re-introduces it into the measurement data, thereby improving plant diagnostic performance was developed and described.

By using the improved fault detection information received from all distributed systems as in the plant control system described in this chapter we can and correlate the information to not only detect the fault, but also to diagnose it based on the location and magnitude of the fault cause as described in the following chapter.

5. Article 3: Correlating hardware fault detection information from distributed control systems to isolate and diagnose a fault in Pressurised Water Reactors.

By A.C. Cilliers

School of Nuclear and Mechanical Engineering

North West University

This peer-reviewed paper was published in Annals of Nuclear Energy 54 (2013) pp. 91 – 103.



Contents lists available at SciVerse ScienceDirect

Annals of Nuclear Energy

journal homepage: www.elsevier.com/locate/anucene



Correlating hardware fault detection information from distributed control systems to isolate and diagnose a fault in pressurised water reactors

Anthonie Christoffel Cilliers *

North West University, School for Mechanical and Nuclear Engineering, Hoffman Street, North West Potchefstroom 2530, South Africa

ARTICLE INFO

Article history:

Received 5 June 2012

Received in revised form 17 October 2012

Accepted 17 October 2012

Keywords:

Fault

Detection

Diagnose

Pressurised water reactor

Distributed control

Performance

ABSTRACT

Early fault identification systems enable detecting and diagnosing early onset faults or fault causes which allow maintenance planning on the equipment showing signs of deterioration or failure. This includes valve and leaks and small cracks in steam generator tubes usually detected by means of ultrasonic inspection.

We have shown (Cilliers and Mulder, 2012) that detecting faults early during transient operation in NPPs is possible when coupled with a reliable reference to compare plant measurements with during transients. The problem introduced by the distributed application of control systems operating independently to keep the plant operating within the safe operating boundaries was solved by re-introducing the fault information it into the measurement data, thereby improving plant diagnostic performance.

This paper introduces the use of improved fault detection information received from all distributed systems in the plant control system and correlating the information to not only detect the fault but also to diagnose it based on the location and magnitude of the fault cause.

© 2012 Elsevier Ltd. All rights reserved.

1. Introduction

With the availability and advances in nuclear power plant simulation technology, a research project was initiated to make use of simulators to provide a deterministic dynamic reference for in-transient fault detection (Cilliers et al., 2011; Cilliers and Mulder, 2012).

The primary objectives of the research were to:

1. Develop an early fault detection system by using real time simulators of nuclear power plants, continuously monitoring and comparing simulated measurement data and control outputs of the model reference adaptive control negative feedback system with the actual measured data and control outputs from the plant. The fault detection system should detect small faults that would normally go undetected as well as detect faults during plant operating transients.
2. Develop a fault characterisation method, making use of measured and simulated data together with the actual and simulated control system response. The fault characterisation system should provide information on the magnitude and location of the fault.
3. Develop a control and protection framework that allows NPP licensing within the existing licensing framework, but is still able to uncover the benefits of expert control and protection systems.

This paper introduces the second objective, with a following paper presenting the third.

Owing to the use of distributed control systems in nuclear plants, the same fault will affect a number of plant measurements during which the affected control systems will operate to counteract the effect of the fault on the system. The plant diagnostic system re-introduces this fault effect into the relevant measurement information (Cilliers and Mulder, 2012). As a result, the fault is detected early in more than one system, each system revealing something about the nature and possible cause of the fault.

Plant diagnostics in the instrumentation and control discipline has been well researched and developed over the last 40 years in with various methods of providing dynamic reference models. In 1976, Willsky (1976) examined statistical techniques for the detection of failures in dynamic systems revealing key concepts, similarities and differences in problem formulations, system structures, and performance. Specifically, they discussed the problem of detecting sudden changes in dynamic systems.

The development of steady state fault detection systems making use of the steady state references to detect control operation deviations in the nuclear industry has been done since 2000 with Chen and Howell (2001) commenting:

“Little has been written about distributing diagnostic tasks presumably because traditionally, the diagnostic engineer's view of feedback control is that it complicates, rather than aids, diagnostic reasoning. Feedback control adds to the complexity of fault detection in process plants by masking measurement deviations that might indicate a fault”.

* Tel.: +27 829202954; fax: +27 866648796.

E-mail address: cillican@cskom.co.za

Correlating hardware fault detection information from distributed control systems to isolate and diagnose a fault in pressurised water reactors.

ABSTRACT

Early fault identification systems enable detecting and diagnosing early onset faults or fault causes which allow maintenance planning on the equipment showing signs of deterioration or failure. This includes valve and leaks and small cracks in steam generator tubes usually detected by means of ultrasonic inspection.

We have shown (Cilliers and Mulder, 2012) that detecting faults early during transient operation in NPPs is possible when coupled with a reliable reference to compare plant measurements with during transients. The problem introduced by the distributed application of control systems operating independently to keep the plant operating within the safe operating boundaries was solved re-introducing the fault information it into the measurement data, thereby improving plant diagnostic performance.

This paper introduces the use of improved fault detection information received from all distributed systems in the plant control system and correlating the information to not only detect the fault but also to diagnose it based on the location and magnitude of the fault cause.

1. Introduction

With this availability and advances in nuclear power plant simulation technology, a research project was initiated to make use of simulators to provide a deterministic dynamic reference for in-transient fault detection (Cilliers et al, 2011; Cilliers and Mulder, 2012).

The primary objectives of the research were to:

1. Develop an early fault detection system by using real time simulators of nuclear power plants, continuously monitoring and comparing simulated measurement data and control outputs of the model reference adaptive control negative feedback system with the actual measured data and control outputs from the plant. The fault detection system should detect small faults that would normally go undetected as well as detect faults during plant operating transients.
2. Develop a fault characterisation method, making use of measured and simulated data together with the actual and simulated control system response. The fault characterisation system should provide information on the magnitude and location of the fault.
3. Develop a control and protection framework that allows NPP licensing within the existing licensing framework, but is still able to uncover the benefits of expert control and protection systems.

This paper introduces the second objective, with a following paper presenting the third.

Owing to the use of distributed control systems in nuclear plants, the same fault will affect a number of plant measurements during which the affected control systems will operate to counteract the effect of the fault on the system. The plant diagnostic system re-introduces this fault effect into the relevant measurement information (Cilliers and Mulder, 2012). As a result, the fault is detected early in more than one system, each system revealing something about the nature and possible cause of the fault.

The development of steady state fault detection systems making use of the steady state references to detect control operation deviations in the nuclear industry has been done since 2000 with Chen and Howell (2001) commenting:

“Little has been written about distributing diagnostic tasks presumably because traditionally, the diagnostic engineer’s view of feedback control is that it complicates, rather than aids, diagnostic reasoning. Feedback control adds to the complexity of fault detection in process plants by masking measurement deviations that might indicate a fault”.

We have shown that the fault masking problem described here can be overcome by re-introducing the fault information into the measurement data in an open loop (Cilliers and Mulder, 2012). The use of distributed diagnostics now becomes possible.

Once a fault is detected in a system, a trip can be initiated to shut the plant down and to keep it safe, whilst being able to characterise the detected fault to assist in repairing the plant. The characterisation of a fault could vary from indicating the sub-system in which the fault is located, to indicating the magnitude and spatial location of the fault.

Plant diagnostics in the Instrumentation and Control discipline has been well researched and developed over the last forty years in with various methods of providing dynamic reference models. In 1976, Willsky (1976) examined statistical techniques for the detection of failures in dynamic systems revealing key concepts, similarities and differences in problem formulations, system structures, and performance. Specifically, they discussed the problem of detecting sudden changes in dynamic systems.

Roy et al. (1998) developed a fault characterisation system to address the need to have improved predictive maintenance techniques in an operating plant. Guidance into the methodology came from one of the earliest applications of state estimation-based fault detection methods in nuclear plants. Roy’s primary objective was to provide an early warning to the human operator regarding the failing health of control equipment, in the process averting major breakdown with its associated large plant downtime. Further, an attempt was made to identify subcomponent faults, so as to carry out fault event sequencing and root cause analysis. They state that most fault detection and characterisation algorithms proposed up to 2000 have been essentially limited to the detection and identification of

global faults in a system and so, a further step to this would be to develop fault identification methods for identifying subcomponent faults in equipment, resulting in improved fault localization and providing better predictive maintenance aids.

The method used by Roy et al. (1998) is shown to be very effective to characterise faults although still being limited to only being able to identify faults during steady state conditions. The fault identification system developed in this research aims to detect and characterise faults during transient or operational mode change conditions when a plant tends to be exposed to higher stresses than under steady state conditions.

In other research Cheon et al. (1993) made use of neural networks to process alarms to aid in the diagnosis of nuclear power plants, while a lot of work has been done to detect and locate faulty sensors in plants, such as the work done by Dorr et al. (2007) and Ming et al. (2006). The research in this paper does not intend to detect faulty sensors although it could potentially aid in locating such faults.

As recently as 2008, Yan et al. (2008) developed a distributed fault identification system with the objective to address problems arising from the models that typically exhibit complex nonlinearity and compensates for the effects of the faults on the residuals that are hidden owing to noise, both of which can prevent an deterministic solution. The noise referred to in this case can also be equivalent to disturbances due to operational mode changes which makes this method come close to identifying faults during transient states of the plant although this is not shown.

To realise the proposed system Yan et al. (2008) made use of a fault tracking approximator to detect and identify system faults. A network of distributed estimators is constructed where the fault tracking approximator based on an iterative learning algorithm is embedded into each estimator. Compared with a neural network-based fault identification scheme, the approach proved to be more efficient although still based on approximation schemes that are very difficult to license in the nuclear industry.

Similar to Yan et al.'s (2008) approach, Hadad et al. (2008) used neural networks to detect and characterise faults occurring in the Russian VVER pressurised water reactor. Ming et al. (2006) made use of a hybrid approach to diagnose faults with neural networks. Ferrari et al. (2008) designed a fault isolation scheme in an input-output discrete-time framework and derived detectability and characterising properties making is of analytical methods.

In 2010 Villez et al. (2010) initiated a project to integrate diverse fault detection systems and automation into closed loop supervisory control systems to reduce the human interaction when a fault is detected. The integration approach in their research requires new control paradigms to be created which would make the nuclear licensing of the new systems difficult.

In the chemical process industry, Chillin et al (2010 and 2012) focuses their research on monitoring and reconfiguration of distributed model predictive control systems. Here the focus is not to detect and isolate faults, but rather to adapt the distributed control parameters of the control systems to maintain system stability when actuator faults occur.

Also in the process control industry a similar approach to this research was taken by Frank and Ding (1997) with the aim to research and design a residual generator that eliminates effect of process input signals and other disturbances, evaluate the results and where elimination of process input signals and disturbances are not fully possible, to optimise the process to achieve approximate results. In this case the reference model is created by estimating outputs of the process. The evaluation of the results is done by fuzzy logic. Similar work was also surveyed by Frank (1990). Although this research provides clear guidance to the problem at hand as well as the methodology to approach the problem, the nature of the nuclear industry requires that deterministic systems are used in both the reference model as well as the evaluation of the results.

The nuclear industry is in a unique situation in having access to first principle simulation models, developed and improved over the last 30 years that can be used as a reliable reference model in fault detection systems.

The system described in this research is deterministic in nature and makes use of conventional nuclear plant protection philosophies. This results in pragmatic fault identification system that can easily be adopted into any existing or new nuclear power plant protection approach.

2. Fault characterisation

For fault characterisation, it is possible to combine the isolated fault information from various measurements inside the plant and to correlate this information with various typical plant faults. This would identify the fault with an increasing level of certainty as the fault effects unfold over time and this information becomes available to the real-time system. The system does this in the following sequence:

1. The system detects that various control systems are behaving unexpectedly (Cilliers and Mulder, 2012).
2. The fault effect is reintroduced into the measurement data of each affected control system (Cilliers and Mulder, 2012).
3. The adapted measurements drift away from the expected measurements beyond the conventional trip set point and a fault is detected (Cilliers and Mulder 2012).
4. The unexpected behaviour is characterised by matching the behaviour with the known behaviour of certain fault categories.
5. The fault is characterised further, as the behaviour trend is identified.
6. The location of the fault is found by combining the measurement equipment that indicated the fault with the location and cause becoming more accurate as the fault is detected in other subsystems.
7. The magnitude of the fault is calculated from the magnitude of the variation from the expected transient.

The first three stages deals with detecting a fault condition early while the operating point has not yet shown any movement due to the fault condition as described by Cilliers and Mulder (2012). The following stages deals with fault characterisation or fault diagnosis. In order to develop a fault

characterisation method it is important to understand the conventional plant protection and operating envelope.

3. Conventional and adapted operating envelope

In Fig. 1 a typical conventional operating envelope is depicted with operating boundaries due to physical limitations in the plant.

A load change transient causes the 100% steady state operating point to move to a new steady state position following a path of large pressure and temperature changes. The static operating envelope is specified large enough to accommodate the various possible operating points as well as the paths that are followed during transient states. The result is that hardware degradation or failures that do not cause large enough changes in the operating point will go undetected until develop to an extent where the plant integrity is under threat, only then, the fault will be detected and a trip will be issued. In such a case an emergency shutdown procedure includes the actuation of safety features that results in extended downtime periods and costly start up procedures.

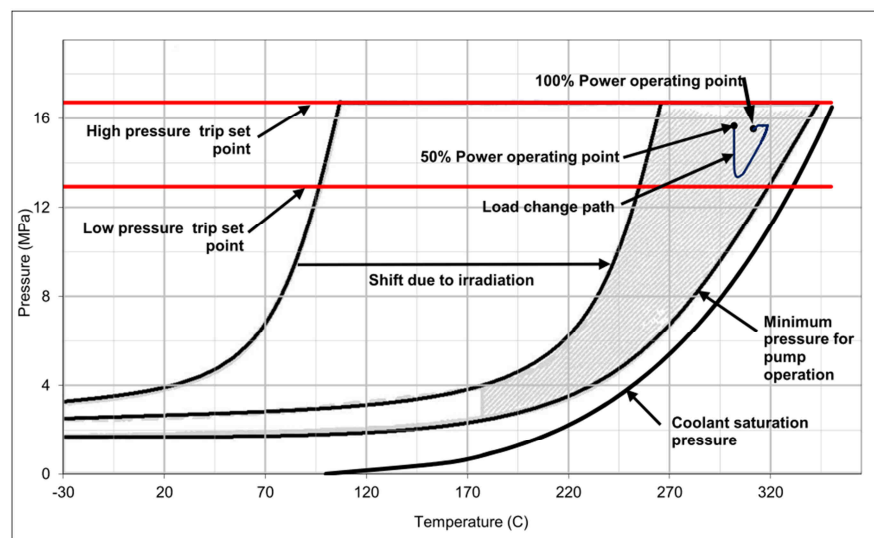


Fig. 1. Temperature – Pressure operating envelope

The effect of the process described by Cilliers and Mulder (2012) could be implemented in one of two ways:

1. The adapted data causes an increase in operating point movement due to a fault since the control system will not mask any unexpected movement. This results in the operating point moving outside the operating envelope much sooner when a hardware fault is present.
2. The adapted data creates a much smaller operating envelope with the size based on instrumentation and simulation tolerances. This operating envelope will move dynamically with the operating point during expected transients but will be static for unexpected transients due to hardware faults.

Both these methods rely on the same measurement data manipulations with only slight differences in the fault indication philosophy. The first method could use all the conventional plant trip indications,

the trip will only occur sooner as the fault effect is not masked. This is a benefit in the nuclear industry as extensive operating experience with conventional protection systems exists. The second method can be implemented to indicate a fault even sooner as the operating point will move beyond the tolerance limits of the instrumentation and dynamic reference before it moves outside the static operating envelope limits.

The operating envelope depicted in Fig. 1, is one of many operating envelopes each indicating an operating range in various independent systems. A fault causing the pressure to change for example could be detected due to the pressure moving outside the pressure boundary. The same fault would also cause another plant measurement to move outside its allowed operating range. Correlating these fault indications allows us to not only indicate a fault but also diagnose the fault cause as well.

4. Plant fault diagnosis

A combination of fault indications results in the defining the fault cause. Tab. 1 depicts the various combinations of measurements that would move outside the operating envelope when a certain hardware fault occurs. A steam tube rupture for example would cause the primary pressure to drop below the allowed pressure and would cause the steam generator level to increase above an allowed level. A loss of coolant accident (LOCA) would have similar effects although the steam generator level should be unaffected while the pressure in the containment would increase. This method of diagnosing the fault is possible using conventional plant protection philosophies since the same effects would be seen once the fault grows large enough that the control system is unable to mask the effect of the fault.

Strictly speaking it is not always necessary to have pre-simulated fault data such as that of Tab. 1 at hand, as the characterisation of the fault as a disturbance input as described by Cilliers and Mulder (2012) presents the analyst with information on which of the distributed control systems are affected.

The information might not in all cases reveal the exact fault, but based on the effects of the fault on the uncompensated system the fault location and magnitude of the effect can be deduced.

If the second approach is followed, the adapted measurement data is not compared to the fixed operating envelope boundaries, but rather with the expected operating point of the dynamic reference. In this way, the maximum and minimum limits from Tab. 1 are changes to dynamic expected values from the dynamic reference. Once the adapted measurement moves outside the reference and instrumentation tolerance boundary for all affected systems, a fault is detected and diagnosed.

Tab. 1. Fault groups with initiating measurements

Measurement indications	Fault group										
	Uncontrolled control assembly withdrawal in subcritical cold condition	Uncontrolled control assembly withdrawal in subcritical cold condition	Inadvertent reduction in RCS boron concentration	Loss of reactor coolant pumps	Primary loss of coolant	SG tube rupture	Leaks and breaks in the MS system	Leaks and breaks in the Feed Water system	Loss of off-site power	Loss of main heat sink	Inadvertent closure of secondary loop isolation valve
Intermediate range neutron flux > max	x										
Intermediate range neutron flux doubling time > max	x										
Power range neutron flux rate of change > max		x	x								
Reactor thermal power > max		x	x								
RCP speed < min for > 1 loop				x					x		
PRZ level > max	x	x	x	x				x	x	x	x
PRZ pressure > max	x	x	x	x				x	x	x	x
PRZ pressure < min					x	x					
SG pressure > max				x					x	x	x
SG pressure drop > max							x				
SG pressure < min							x		x		
SG level A < min							x	x	x		
SG level A > max						x					
Containment pressure > max					x		x	x			

To further diagnose the fault, the magnitude of the control system operation that attempts to mask the fault is analysed. During small faults, this magnitude is the opposite of the fault since the control system is attempting to cancel the effect of the fault on the system. This principle and the specific operation of some of the control systems are discussed in Cilliers et al (2011).

The above principles can be best explained at the hand of examples where the measurement data is adapted, and compared with the dynamic reference to provide detailed fault diagnostic information.

4.1. Fault diagnosis examples

The examples described in this section are a small break loss of coolant accident and a steam generator (SG) tube rupture. The cases are specifically selected as they provide good benchmarking in terms of fault detection, as well as a comparison of the two examples provides an indication as to the

effectiveness of the fault diagnostic process as the two accidents have many similarities. In the examples, and expected load change transient (100% to 80%) was used as with the fault disturbance adding additional stress on the control system. During a load change transient, the various systems are operating to stabilise the system and additional disturbances from the fault are difficult to isolate.

4.2. Loss of coolant accident

A typical fault, and one of the most documented types of accident causes, is the LOCA. LOCAs are categorised as large break and small break LOCAs, each with specific characteristics. A small break LOCA is defined as a break with an equivalent diameter between 0.95 cm and 0.25 cm; in other words, a break smaller than 0.95 cm translates into an opening surface area smaller than 0.709 cm². When the equivalent diameter of a break is less than 0.95 mm, the leakage can be compensated for by make-up flow from the reactor chemical and volume control/reactor boron and water make-up system (REA) systems, thereby maintaining the pressuriser level.

In this case, the fuel cladding is not damaged, and only radioactive products normally contained in the primary system are released into the containment. This also means that the conventional plant protection systems remain unaware of the fault for an extended period of time.

Tab. 2. Loss of coolant accident configuration

Accident configuration	
Description	Loss of coolant accident (cold leg)
Delay time	100 s
Ramp time	0 s
Failure fraction	0.5 cm ²
Transient configuration	
Description	Load change
Transient size	100-80%
Transient rate	5% per minute
Event sequence	
Action	Time (s)
PZR proportional heater capacity change	0.0
PZR proportional heater capacity change	22.0
PZR proportional heater capacity change	157.0
PZR back-up heater capacity change	241.0
PZR proportional heater capacity change	641.0
PZR spray valve #1 position change	702.5
HPSI start high RB press 1.30 psia	3 752.0
HPI pump #1 position change	3 752.0
HPI pump #2 position change	3 752.0

Letdown valve #1 position change	3 752.0
HPI pump #3 position change	3 752.0
Ctmt vent valve #1 position change	3 752.0
RBS pump #1 position change	3 752.0
Ctmt spray starts 1.3 kg/cm ²	3 752.0
Letdown valve #1 position change	3 752.5
Reactor SCRAM	3 753.0

The selected break size for the reference LOCA is 0.5 cm², which is smaller than a defined small break LOCA. Tab. 2 lists the LOCA configuration as well as the plant operation sequence. The primary protection system detects a fault after 60 minutes and 53 seconds, with the fault still unidentified. The trip is due to overpressure of 1.3 atmospheres (0.13 MPa) in the containment building.

When comparing the expected values with the measured values during the transient, a slight variation from the expected values is seen. This is, however, not large enough to detect or diagnose a fault using the primary protection system. In Fig. 2, the expected and measured RCS pressures are depicted, with the slight variation seen. When the expected pressuriser heater operation and the actual pressuriser heater operation are compared, it is clear that the proportional heater starts to compensate for the transient much earlier than expected, with the back-up heater switched on, and maximum heater operation is also reached before expected.

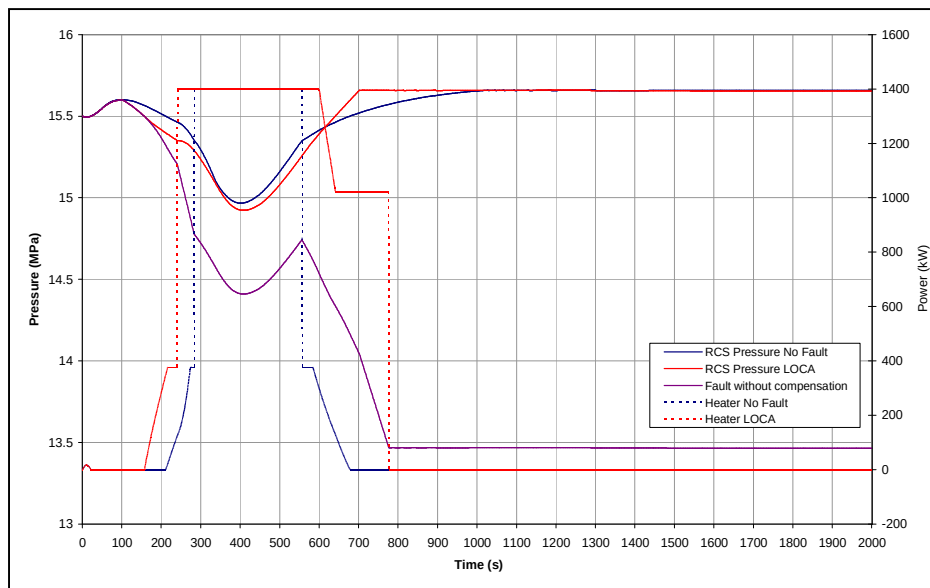


Fig. 2. RCS pressure and heater operation

With this information, it is possible to calculate the reduced pressure by removing the pressure increase caused by the additional heater operation as shown in Fig. 2. During the time that the expected and actual heater operation reached a maximum, the control systems were unable to compensate for the fault, and so no compensating pressure was removed from the measured pressure.

The uncompensated pressure drops to below 13.5 MPa, which is quite significant, since, at this pressure, the conventional protection system would have initiated a reactor SCRAM. Making use of the proposed system the trip would have occurred 11 minutes 14 seconds after the fault had started, 49 minutes and 39 seconds before a fault was detected by the existing system.

The analysis does not stop there. With the adapted pressure now moving much further away from the expected pressure, a fault condition can be detected before the plant system would have initiated a trip. In Fig. 3, the difference is depicted, with a 5% difference in pressure reached after 8 minutes 20 seconds and a 10% difference reached after 10 minutes. Depending on the specified simulator accuracy, the fault can be detected within these times. The information about the fault with the analysis so far already reveals more than the existing protection system, which only reveals containment overpressure.

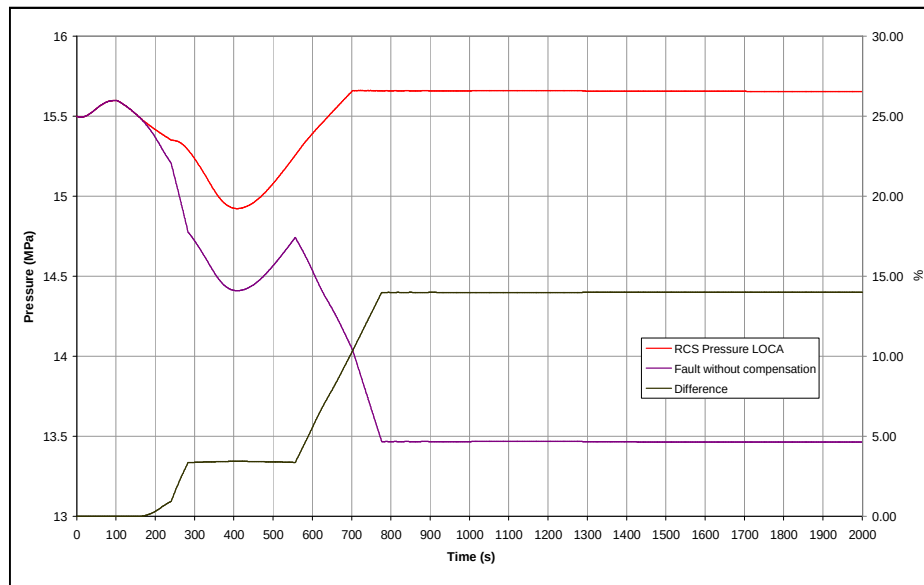


Fig. 3. RCS pressure and percentage difference

The information revealed by analysing other measured and simulated parameters should provide even more information as to the nature and cause of the detected fault. Comparing the RCS average temperature with the expected temperature in Fig. 4 reveals no significant variation as well as control rod reactivity and core power. The implication is that the average temperature control system has remained unaffected by the fault and is not compensating for any unexpected change in operation.

In Fig. 5, the actual pressuriser level is compared to the expected level, with a variation reaching a maximum of 5% during the transient. However, the residual inflow into the pressuriser to maintain the coolant level is substantially larger than expected, indicating a compensating effect from some unexpected cause. The RCS coolant volume is calculated by the plant control system from the pressuriser and pressure vessel levels. Since the volume is used in m³ and flow is measured in ton per hour, it is much easier to use the RCS volume in fault calculations. The discontinuities in the pressuriser level depicted in Fig. 5 are due to two phase flow as steam is released. This is depicted in other Figures as well, where coolant flow is present.

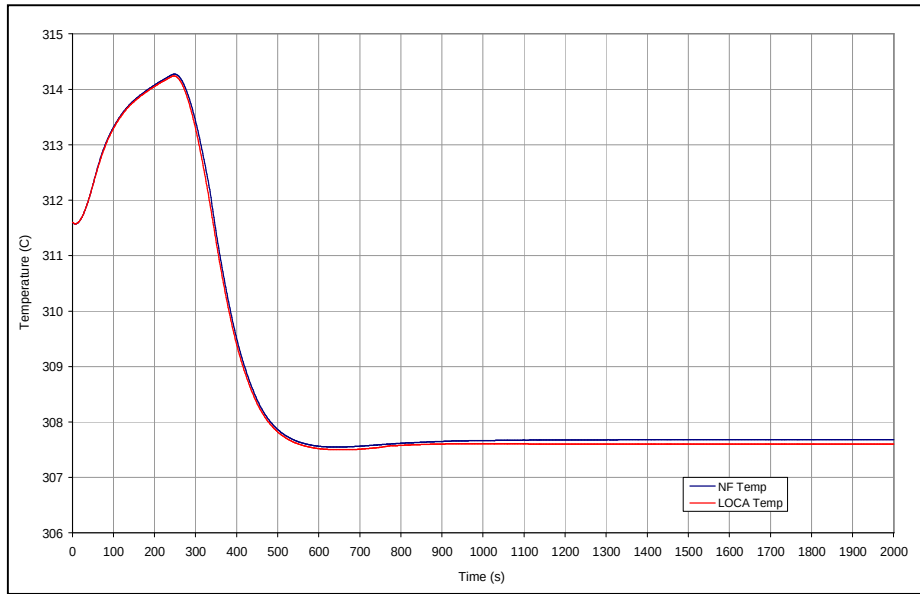


Fig. 4. RCS average temperature

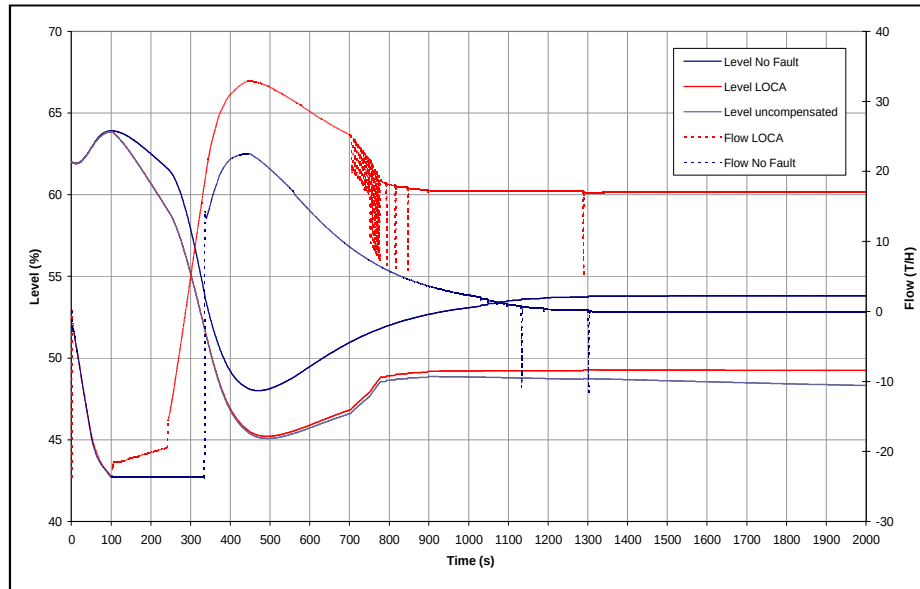


Fig. 5. Pressuriser level and residual inflow

The RCS coolant volume is depicted in Fig. 6. A reduced volume is calculated by removing the flow into the pressure vessel that compensates for the reduced level due to the fault. The volume without compensating flow provides us with an indication what reduction in volume the fault is causing, and thus, the actual effect of the fault. The loss in volume without the compensated flow produces more information on the nature of the fault. Since the inflow into the RCS is not fully reflected in the increase in volume or pressuriser coolant level, a resultant outflow of coolant could be the only cause.

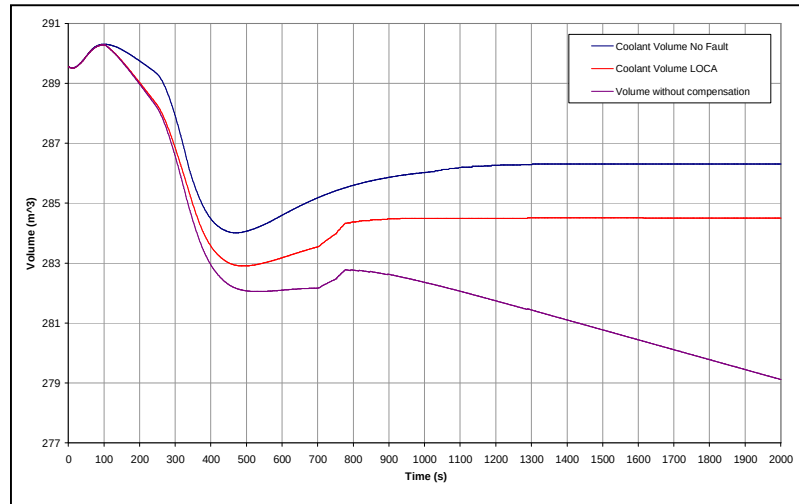


Fig. 6. RCS coolant volume

Since the charging and letdown flow is governed by a control transfer function, the inflow will eventually match the outflow out of the coolant and indicate the exact flow of coolant from the identified leak. In Fig. 7, the coolant inflow that compensates for the unknown outflow is shown.

The calculated flow stabilises after 20 minutes, resulting in an outflow of 17.06 ton per hour of coolant lost. At 17.06 ton per hour and at a pressure of 15.66 MPa, the break size is calculated as 0.5 cm² when it settles after 20 minutes. The pressure used to calculate the break size is that of the actual measured pressure, since the outflow through the break is a direct result of the actual pressure in the system.

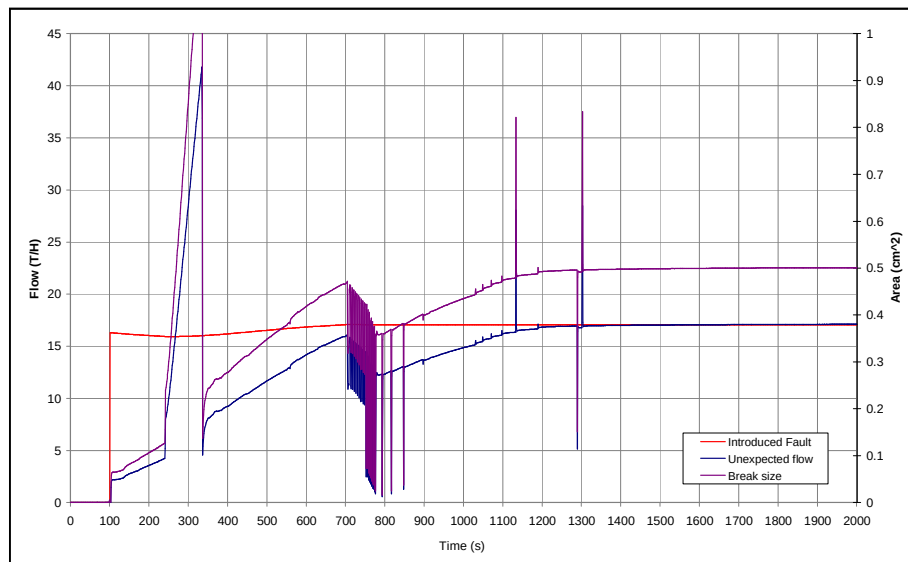


Fig. 7. Unexpected flow and introduced fault flow

Fig. 8 depicts the pressure change in the containment where the fault is eventually detected and the SCRAM is issued.

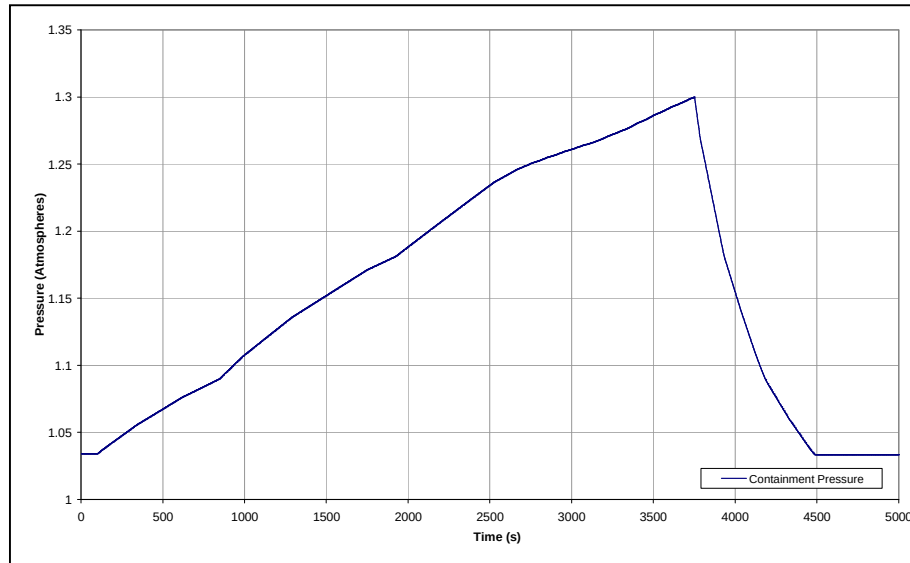


Fig. 8. Containment pressure

By combining all of these effects, the fault can be derived as a LOCA from Tab. 1 as the fault was detected in the following control systems:

- Pressuriser level control
 - Control: Pressuriser makeup flow larger than expected,
 - Measurement: Pressuriser level lower than expected.
- RCS Pressure control
 - Control: Pressuriser heater operation larger than expected,
 - Measurement: Pressuriser pressure lower than expected.
- Containment pressure monitoring
 - Measurement: Containment pressure larger than maximum allowed pressure.

The diagnostic system results are summarised in Tab. 3.

Tab. 3. Loss of coolant accident diagnostic system results

Accident results		
	Proposed fault diagnostic system	Conventional protection system
Categorised as	Loss of coolant from RCS to containment	Containment over pressure
Time faulty operation detected	700 seconds	3650 seconds
Time fault diagnosed	1 200 seconds	3650 seconds
Failure fraction 1	17.06 ton per hour	NA
Failure fraction 2	0.5 cm ²	NA

4.3. Steam generator tube rupture

An SG tube rupture is quite common, with the SG secondary side being exposed to water and steam during the steam generating process. When an SG tube ruptures, a path between the primary and secondary coolant systems is created. Since the primary coolant system is at a higher pressure (15.5 MPa) than the secondary coolant system (6.9 MPa), the coolant would flow out of the RCS into the steam generator secondary loop. When looking at the RCS, we expect to see the same results as we see in a LOCA, since coolant is lost. In the secondary system, we should see some indication that unexpected coolant is entering the system, for which the control system is compensating. Tab. 4 lists the SG tube rupture configuration as well as the plant operation sequence.

Tab. 4. SG tube rupture configuration

Accident configuration	
Description	SG tube rupture
Delay time	100 s
Ramp time	0 s
Failure fraction	10% of 1 tube
Transient configuration	
Description	Load change
Transient size	100-80%
Transient rate	5% per minute
Event sequence	
Action	Time (s)
PZR proportional heater capacity change	0.0
PZR proportional heater capacity change	21.0
PZR proportional heater capacity change	165.0
PZR back-up heater capacity change	251.5
HPI pump 3 position change	309.0
PZR proportional heater capacity change	633.5
PZR spray valve 1 position change	691.0
PZR back-up heater capacity change	727.0
PZR spray valve 1 position change	730.0
PZR spray valve 1 position change	949.5
PZR spray valve 1 position change	950.0

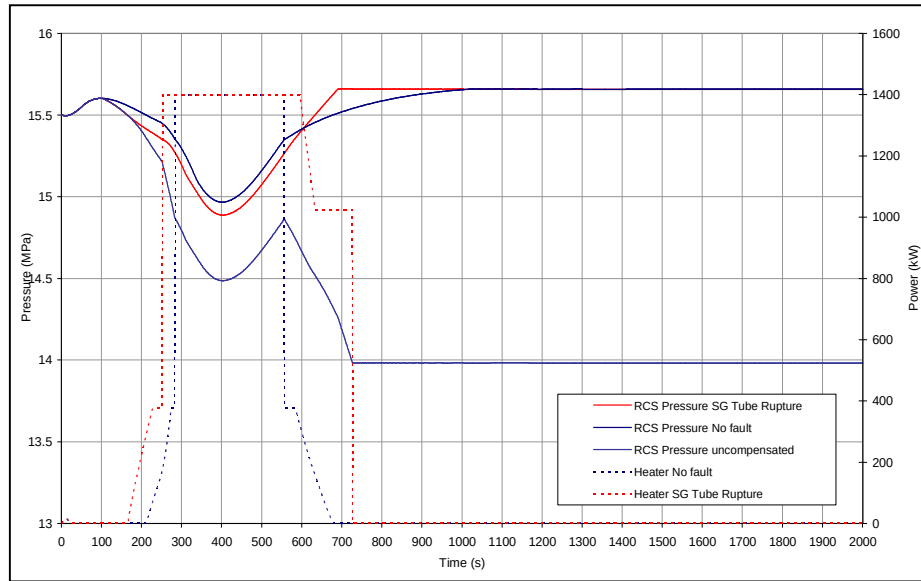


Fig. 9. RCS pressure and heater operation

When comparing the expected values with the measured values during the transient, a slight variation from the expected values is seen. This is, however, not large enough for the reactor protection system to detect or categorise a fault. In Fig. 9, the expected and measured RCS pressure is depicted, with the slight variation seen. When the expected pressuriser heater operation and the actual pressuriser heater operation are compared, it is clear that the proportional heater starts to compensate for the transient much earlier than expected, with the back-up heater switched on, and maximum heater operation is also reached before expected.

With this information, it is possible to calculate the reduced pressure by removing the pressure increase caused by the additional heater operation as shown in Fig. 9. It is clear that, during the time that the expected and actual heater operation reached a maximum, the control systems were unable to compensate for the fault, and as a result no compensating pressure was removed from the measured pressure.

The uncompensated pressure drops to below 14 MPa for a 10% crack in one SG tube. In Fig. 10, the difference is depicted, with a 5% difference in pressure reached after 8 minutes 20 seconds and a 10% difference reached after 10 minutes. Depending on the specified simulator accuracy, the fault can be detected within these times. The information about the fault with the analysis so far appears to reveal a fault condition, with the existing protection system unaware of any changes in the plant health.

The information revealed by analysing other measured and simulated parameters should provide even more information as to the nature and cause of the detected fault. Comparing the RCS average temperature with the expected temperature in Fig. 11 reveals no significant variation as well as control rod reactivity and core power. The implication is that the average temperature control system has remained unaffected by the fault and is not compensating for any unexpected change in operation, similar to a LOCA.

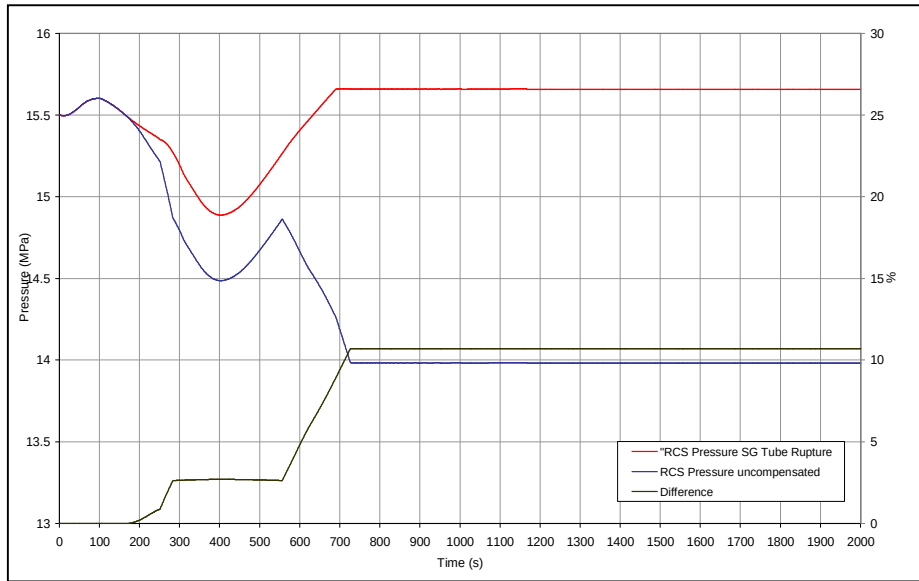


Fig. 10. RCS pressure and percentage difference

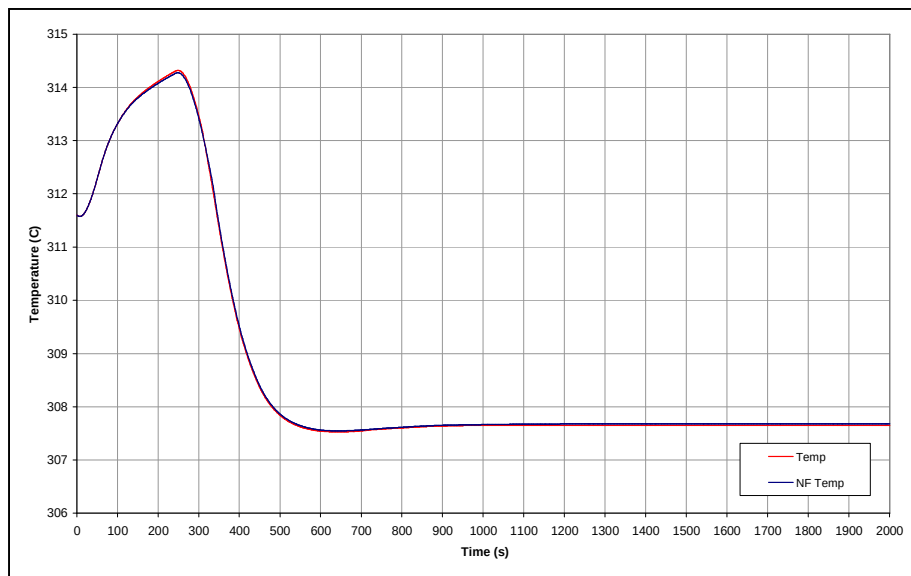


Fig. 11. RCS average temperature

In Fig. 12, the actual pressuriser level is compared to the expected level, with the variation reaching a maximum of 5% during the transient. However, the residual inflow into the pressuriser to maintain the coolant level is substantially larger than expected, indicating a compensating effect from some unexpected cause. The RCS coolant volume is calculated by the plant control system from the pressuriser and pressure vessel levels. Since the volume is used in m³ and flow is measured in ton per hour, it is much easier to use the RCS volume in fault calculations.

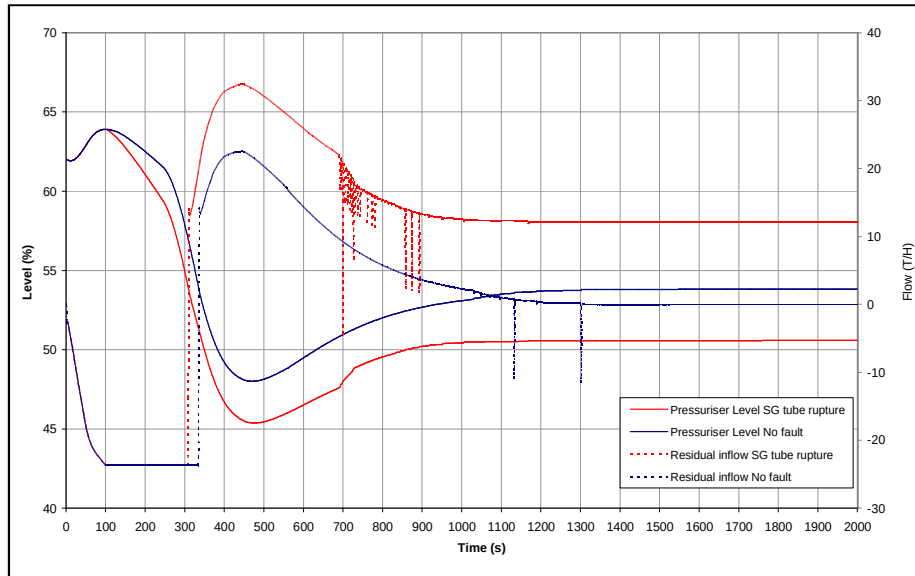


Fig. 12. Pressuriser level and residual inflow

The RCS coolant volume is depicted in Fig. 13. Removing the compensating flow into the pressure vessel produces reduced volume if the control system did not compensate for a loss of coolant.

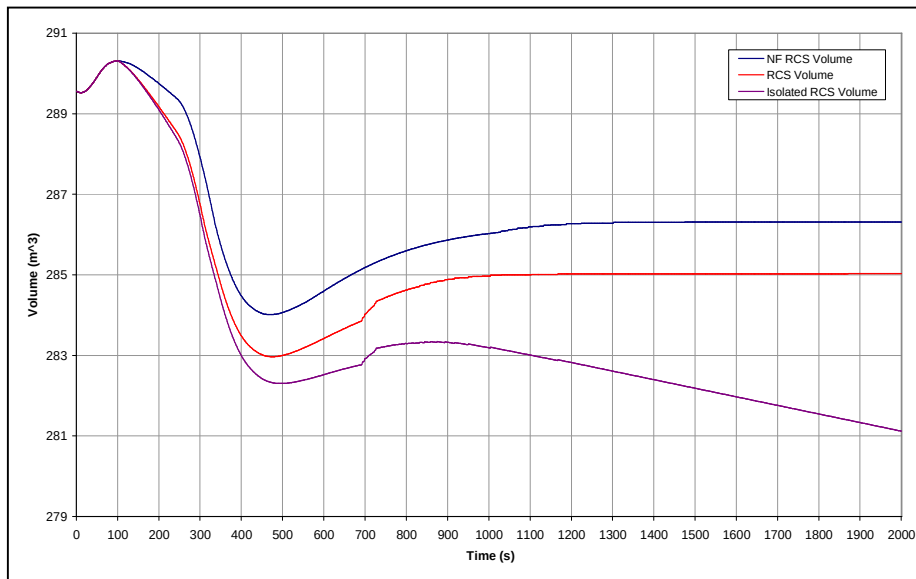


Fig. 13. RCS volume

Before the RCS volume drop is analysed, the results of comparing the secondary system parameters also indicate the control system compensating for some unexpected behaviour. This was not the case for the LOCA, since the fault was limited to a leak from the RCS to the containment building. In Fig. 14, the variation in SG level is seen, with the reduced feed water inflow into the SG to compensate for the increased level due to the tube rupture.

The difference between the expected feed flow into the SG and the actual inflow into the SG should provide us with the amount of flow coming from the unexpected source. In the RCS, the increased

flow into the pressuriser compared to the expected flow would result in the expected outflow to an unexpected sink.

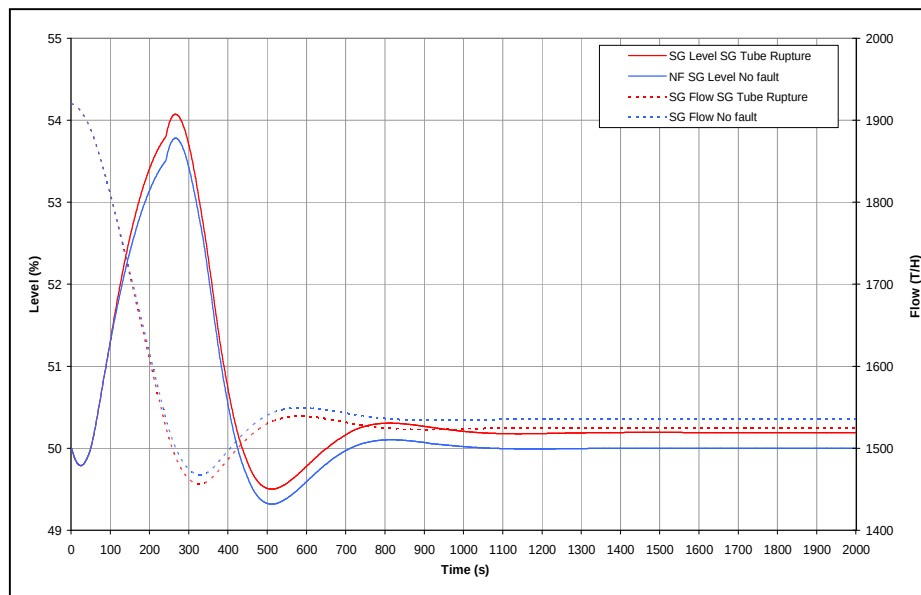


Fig. 14. Steam generator level and inflow

The unexpected outflow from the RCS and the unexpected inflow to the SG should be in the same order, with slight variations due to the dead bands of both level controls expected and steam accumulating in the top of the pressuriser.

In Fig. 15, the comparison is made with the size of the actual fault flow. The actual flow from the RCS to the SG secondary system is 12.1 ton per hour.

The results from the diagnostic system indicate 12.1 ton per hour from the RCS and 11 ton per hour into the SG.

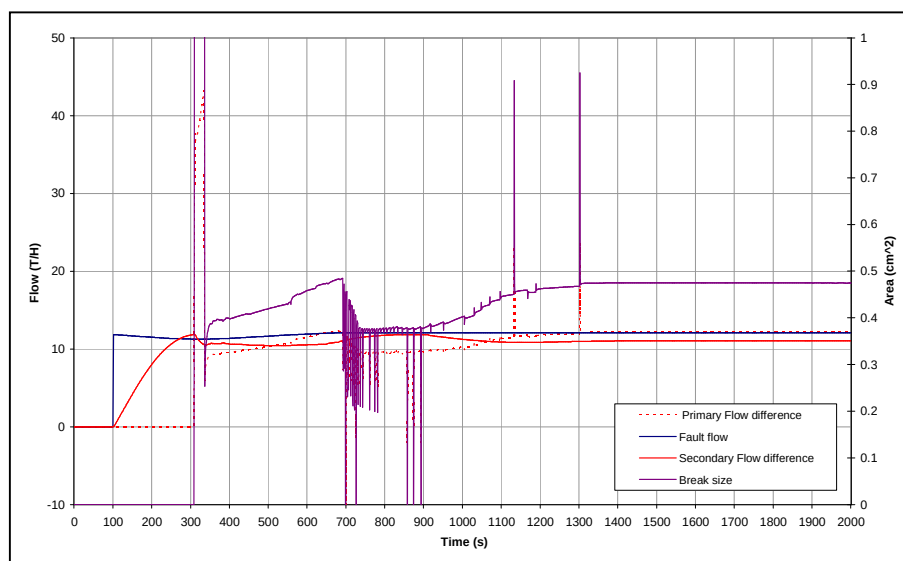


Fig. 15. Primary and secondary flow compensation for fault

With the pressure difference between the primary and secondary coolant loops as well as the flow through the break, the break size is calculated as 0.47 cm^2 . It is interesting to note that the break size is very similar to that of the LOCA in the previous example, although the flow through the break is less. This is simply due to the lower pressure differential when the break is into the secondary loop instead of into the containment building.

Since the break does not feed into the containment building, no pressure change is seen inside the containment building. For this reason, the fault is never detected, and no SCRAM is issued. The diagnostic system allows the identification of the fault within 10 minutes.

By combining all of these effects, the fault can be derived as a SG tube rupture from Tab. 1 as the fault was detected in the following control systems:

- Pressuriser level control
 - Control: Pressuriser makeup flow larger than expected,
 - Measurement: Pressuriser level lower than expected.
- RCS Pressure control
 - Control: Pressuriser heater operation larger than expected,
 - Measurement: Pressuriser pressure lower than expected.
- SG Level control
 - Control: SG Let down flow larger than expected,
 - Measurement: SG level higher than expected.

In Tab. 5, the diagnostic system results are summarised.

Tab. 5. SG tube rupture accident diagnostic system results

Accident results		
	Proposed fault diagnostic system	Conventional Protection system
Categorised as	Loss of coolant from RCS to secondary coolant loop	Not categorised
Time faulty operation detected	700 seconds	Not detected
Time fault diagnosed	1 200 seconds	Not categorised
Failure fraction 1	12 ton per hour	NA
Failure fraction 2	0.47 cm^2	NA

5. Conclusion

The difference between a LOCA and a steam tube rupture is merely the location of the damage to the primary system. In the case of the LOCA the primary system leak is directly into the containment whilst the leak of a tube rupture is into the secondary coolant loop. The pressure and level controls of the reactor primary coolant system should be similarly affected by both faults. In the case of LOCA the pressure measurement in the containment would be affected, and for the steam tube rupture, the

steam generator flow, and level controls are affected. The combination of magnitude of additional control at measured pressures and temperatures allow us to calculate the magnitude of the damage to the system.

We have shown that fault detection and diagnoses in this manner is indeed possible without relying on statistical models of fault signatures. The effectiveness of the system lies in the use of accurate mathematical models of the plant combined with conventional deterministic reactor protection principles. The described technique is somewhat limited as it cannot be applied to unstable systems stabilised by the closed loop control systems. It does however make it an ideal technique to use when the aim is to detect small faults that would normally go undetected as well as to detect faults during expected plant operating transients as described by Cilliers and Mulder (2012).

In follow on work a case study is done on the Three Mile Island accident. To implement this system a control and protection architecture is also developed to enable separation of systems while still being able to benefit from control information in plant diagnostics.

6. References

- Chen, J., Howell, J., 2001. A self-validating control system based approach to plant fault detection and diagnosis. *Computers and Chemical Engineering*. 25, 337-358.
- Cheon, W., Chang, S.H., Chung, H.Y., Bien, Z.N., 1993. Application of Neural Networks on Multiple Alarm Processing and Diagnosis in Nuclear Power Plants. *IEEE Trans Nucl. Sci.* 40:1, 11-20.
- Chilin, D., Liu, J., Chen, X., 2012. Fault detection and isolation and fault tolerant control of catalytic alkylation of benzene process. *Chemical Engineering Science*, 78, 155-166.
- Chilin, D., Liu, J., de la Pena, D.M., 2010. Detection, isolation and handling of actuator faults in distributed model predictive control systems. *Journal of Process Control*, 20:9, 1059-1075.
- Cilliers, A.C., Mulder, E., 2012. Adapting plant measurement data to improve hardware fault detection performance in Pressurised Water Reactors. *Annals of Nuclear Energy*, 49, 81-87.
- Cilliers, A.C., Nicholls, D., Helberg, A.S.J., 2011. Fault detection and characterisation in Pressurised Water Reactors using real-time simulations. *Annals of Nuclear Energy*. 38, 1196-1205.
- Dorr, R., Kratz, F., Ragot, J., Loisy, F., Germain, J., 2007, Detection, Isolation, and Identification of Sensor Faults in Nuclear Power Plants. *IEEE Trans Control Syst. Technol.* 5:1, 42-60.
- Ferrari, R.M.G., Parisini, T., Polycarpou, M.M., 2008. A Robust Fault Detection and Isolation Scheme for a Class of Uncertain Input-output Discrete-time Nonlinear Systems. *American Control Conference*, Seattle, Washington, USA, 2804-2809.
- Frank, P.M., 1990. Fault diagnosis in dynamic systems using analytical and knowledge based redundancy – a survey and some new results. *Automatica*, 26, 459-474.
- Frank, P.M., Ding, X., 1997. Survey of robust residual generation and evaluation methods in observer-based fault detection systems. *Journal of Process Control*. 7:6, 403-424.

- Hadad, K., Mortazavi, M., Mastali, M., Safavi, A.A., 2008. Enhanced Neural Network Based Fault Detection of a VVER Nuclear Power Plant With the Aid of Principle Component Analysis. *IEEE Trans Nucl.* 55:6, 3611-3619.
- Ming, Y., Jianfei, L., Minjun, P., Shengyuan, Y., Zhijian, Z., 2006. A Hybrid Approach for Fault Diagnosis based on Multilevel Flow Models and Artificial Neural Network. *International Conference on Computational Intelligence for Modelling Control and Automation, Web Technologies and Internet Commerce.*
- Roy, K., Banavar, R.N., Thangasamy, S., 1998. Application of Fault Detection and Identification (FDI) Techniques in Power Regulating Systems of Nuclear Reactors. *IEEE Transactions on nuclear science.* 45:6, 3183-3201.
- Villez, K., Venkatasubramanian, V., Spinner, T., Rengaswamy, R., Garcia, H., Rieger, C., 2010. Achieving resilience in critical infrastructure: A case study for a nuclear power plant cooling loop. *IEEE*, 49-52.
- Yan, B., Tian, Z., Shi, S., 2008. A novel distributed approach to robust fault detection and identification. *Electrical Power and Energy Systems.* 30, 343-360.
- Willsky, A.S., 1976. A Survey of Design Methods for Failure Detection in Dynamic Systems. *Automatica.* 12, 601-61.

5.1. Additional notes

5.1.1. Conclusion

In this chapter we introduced the use of improved fault detection information received from all distributed systems in the plant control system and correlating the information to not only detect the fault, but also to diagnose it based on the location and magnitude of the fault cause.

We have shown that fault detection and diagnoses in this manner is indeed possible without relying on statistical models of fault signatures. The effectiveness of the system lies in the use of accurate mathematical models of the plant combined with conventional deterministic reactor protection principles. The described technique is somewhat limited as it cannot be applied to unstable systems stabilised by the closed loop control systems. It does however make it an ideal technique to use when the aim is to detect small faults that would normally go undetected as well as to detect faults during expected plant operating transients.

In the next chapter we will make use of the techniques and processes developed in this and previous chapters and apply it to a case study of the Three Mile Island nuclear power plant accident. In this way we can determine and showcase how the improved information available could present the operator with a better idea to the state of the plant during situations where a combination of faults and transients prevents the operator and conventional systems to recognise the abnormal behaviour.

6. Article 4: Benchmarking an expert fault detection and diagnostic system on the Three Mile Island accident event sequence.

By A.C. Cilliers

School of Nuclear and Mechanical Engineering

North West University

This peer-reviewed paper was submitted to Annals of Nuclear Energy on 14 June 2012.

Benchmarking an expert fault detection and diagnostic system on the Three Mile Island accident event sequence.

ABSTRACT

Early fault identification systems enable detecting and diagnosing early onset faults or fault causes which allow maintenance planning on the equipment showing signs of deterioration or failure. This includes valve and leaks and small cracks in steam generator tubes usually detected by means of ultrasonic inspection.

We have shown (Cilliers and Mulder, 2012) that detecting faults early during transient operation in NPPs is possible when coupled with a reliable reference to compare plant measurements with during transients. We have also shown (Cilliers, 2012) that by correlating the fault detection information as received from distributed systems it is possible to diagnose the faults in terms of location and magnitude.

This paper makes use of the techniques and processes developed in the previous papers and apply it to a case study of the Three Mile Island accident. In this way we can determine how the improved information available could present the operator with a better idea to the state of the plant during situations where a combination of faults and transients prevents the operator and conventional systems to recognise the abnormal behaviour.

1. Introduction

With the availability and advances in nuclear power plant simulation technology, a research project was initiated to make use of simulators to provide a deterministic dynamic reference for in-transient fault detection and diagnosis (Cilliers et al, 2011; Cilliers and Mulder, 2012; Cilliers, 2012).

The primary objectives of the research were to:

1. Develop an early fault detection system by using real time simulators of nuclear power plants, continuously monitoring and comparing simulated measurement data and control outputs of the model reference adaptive control negative feedback system with the actual measured data and control outputs from the plant. The fault detection system should detect small faults that would normally go undetected as well as detect faults during plant operating transients.
2. Develop a fault characterisation method, making use of measured and simulated data together with the actual and simulated control system response. The fault characterisation system should provide information on the magnitude and location of the fault.
3. Develop a control and protection framework that allows NPP licensing within the existing licensing framework, but is still able to uncover the benefits of expert control and protection systems.

This paper functions as a benchmark of the first objective described by Cilliers and Mulder (2012) and the second objective described by Cilliers (2012), with a following paper presenting the third objective. In these papers we have shown that fault detection and diagnoses in this manner is indeed possible without relying on statistical models of fault signatures. The effectiveness of the system lies in the use of accurate mathematical models of the plant combined with conventional deterministic reactor protection principles. In this paper a case study is done on the Three Mile Island (TMI) accident.

The TMI accident can be considered as a watershed moment in the nuclear industry which led to numerous safety analyses and advances following. The event itself has been studied to determine the exact sequence of events (Hochreiter and Robinson, 2004) as well as the cause and mistakes made (Cummings, 1980). Other research was done on preventing the deterioration of the situation in the direct aftermath of the accident (Gonzalez and Gagliardo, 1980).

The event has also been used as case studies such as that of Le Bot (2004) that illustrated their point of view through the analysis of the TMI accident in 1979. Analysis of this accident allowed them to validate their positions regarding the need to move, in the case of an accident, from the concept of human error to that of systemic failure in the operation of systems such as a nuclear power plant. Their retrospective analysis of the TMI accident showed that the operators' mode of operation resulted from an overall logic, reflecting emergency operation logic upon which the design of the operating system was based. It helps to get out of the deadlock reducing the TMI accident either to a commissioning error of the type 'Inappropriate shutdown of the safety injection' or to an error of diagnostic and misrepresentation of the situation. The main theme of the research is acknowledging that although operator actions were to blame for the accident after a minor plant fault occurred, the real problem was the limited information available to the operators and that automated actions would have resulted in the same effect. They conclude by stating:

“The operating system did not foresee the means that were actually necessary to fulfil the mission required by the situation.”

The work by Le Bot (2004) is very relevant to the research in this paper as we focus on manipulating measurement data combined with detailed models of the plant to increase the available information to the operator or system.

2. The TMI accident sequence of events

The event occurred at 04:00 on 28 March 1979. At the time, routine maintenance was being carried out on the ion-exchange system for feed water polishing. The accident was caused as a result of two block valves in the auxiliary feed water pump pressure lines that had been left closed after maintenance work had been conducted on the lines two days prior to the accident. The fault was initiated when the primary auxiliary feedwater pump failed. This should not have caused an accident as the secondary feedwater supply system should continue to supply feedwater to the steam

generators. With the two block valves closed, the feedwater supply was cut off completely (Cummings, 1980).

This prevented feed water from entering one of the steam generators and so reduced the plant's ability to evacuate heat from the core. Because of the rise in temperature in the core, the Reactor Coolant System (RCS) pressure increased, which caused the power-operated relief valves (PORV) to open. Once the pressure had been reduced, the pressure relief valve failed to reseal and a leak occurred corresponding to a small break LOCA.

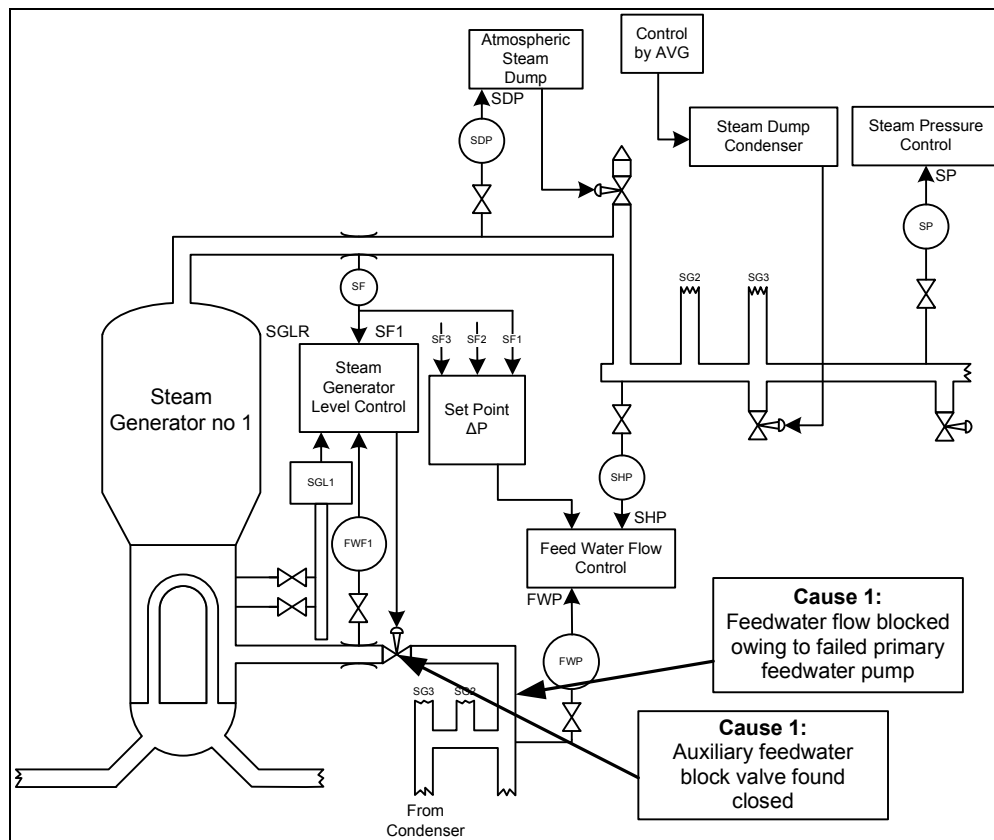


Fig. 1. Three Mile Island faulty valves (Cause 1)

The closed auxiliary feed water block valves were discovered closed after eight minutes and opened. This should have enabled the steam generators (SGs) to evacuate the heat correctly from the core, and the accident would have been prevented.

The small break LOCA caused by the leaking PORV was only discovered two and a half hours later, by which time the accident was well under way. Due to fault trigger (the closed block valves in the auxiliary feed water pressure lines) being corrected and the PORV indication light in the control room indicating that it had been de-energised, the operators did not expect a small break LOCA, and since the plant was already in a recovery transient from the accident, it was difficult to recognise unexpected behaviour of the plant. In fact, when the safety injection system started operating automatically after two minutes, the operators switched it off, believing that it would overfill the pressuriser (Hochreiter and Robinson, 2004)

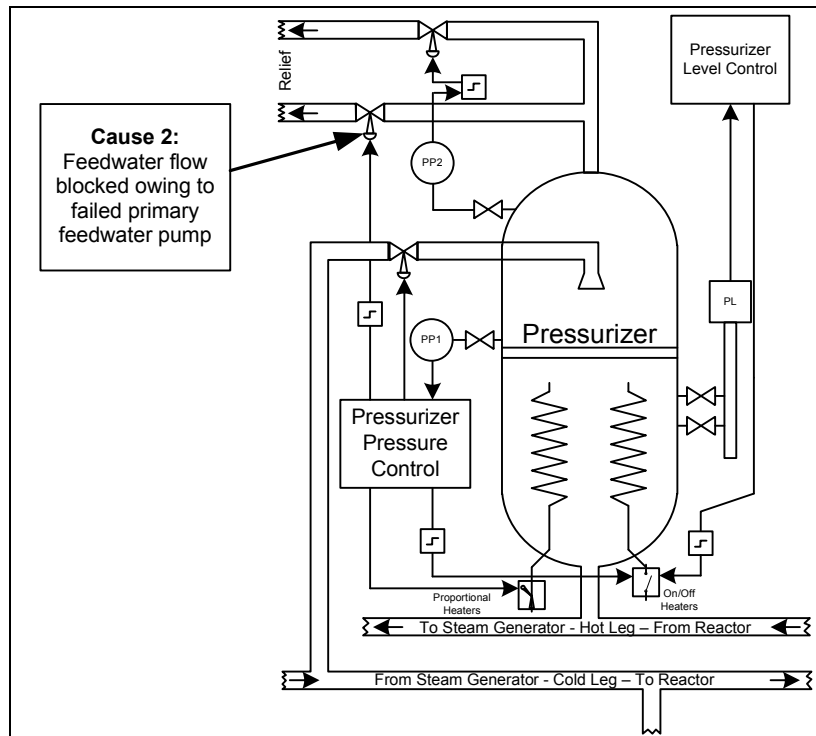


Fig. 2. Three Mile Island faulty valves (Cause 2)

It would be valuable to test the plant diagnostic system in these conditions. The event can be split into two distinct phases. The first phase is the blocking of feedwater flow to one SG, and the second phase the PORV stuck open after relieving pressure. The valves involved in these two causes are depicted in Fig. 1 and Fig. 2.

3. Cause 1: Feedwater supply block to Steam Generator

The closed feed water block valves caused a large fault that was detected within 114 seconds on the RCS high pressure setpoint by the conventional plant protection system. The affected control systems during this phase of the accident were the:

- Pressuriser level control
 - o Control: Pressuriser letdown flow larger than expected,
 - o Measurement: Pressuriser level higher than expected.
- RCS Pressure control
 - o Control: Pressuriser spray operation larger than expected,
 - o Measurement: Pressuriser pressure higher than expected.
- SG Pressure control
 - o Measurement: SG pressure increase larger than expected,
 - o Measurement: SG pressure higher than expected.
- SG Level control
 - o Measurement: SG level lower than expected.

Making use of dynamic setpoints and control operations operating beyond the expected operations the fault is detected within 4 seconds, with the combination of systems correlating to an “Inadvertent

closure of secondary loop isolation valve” in Table 1 reached within 56 seconds as depicted the following figures.

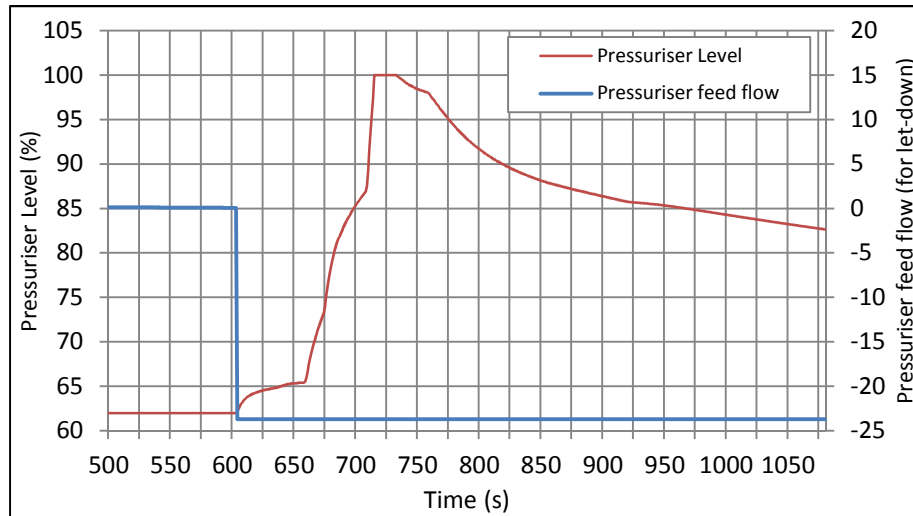


Fig. 3. Pressuriser level and feed flow

Figure 3 depicts the pressuriser level and feed flow, indicating an almost immediate rise in level with the pressuriser level control system following with increased letdown flow in an attempt to reduce the pressuriser level. The increase in pressuriser level is a direct effect of the reduced heat evacuation capability of the steam generators which resulted in increased pressure in the RCS and subsequent increased pressuriser level. Figure 4 depicts the increase in RCS pressure and the activation of the pressuriser spray after 35 seconds in an attempt to reduce the pressure.

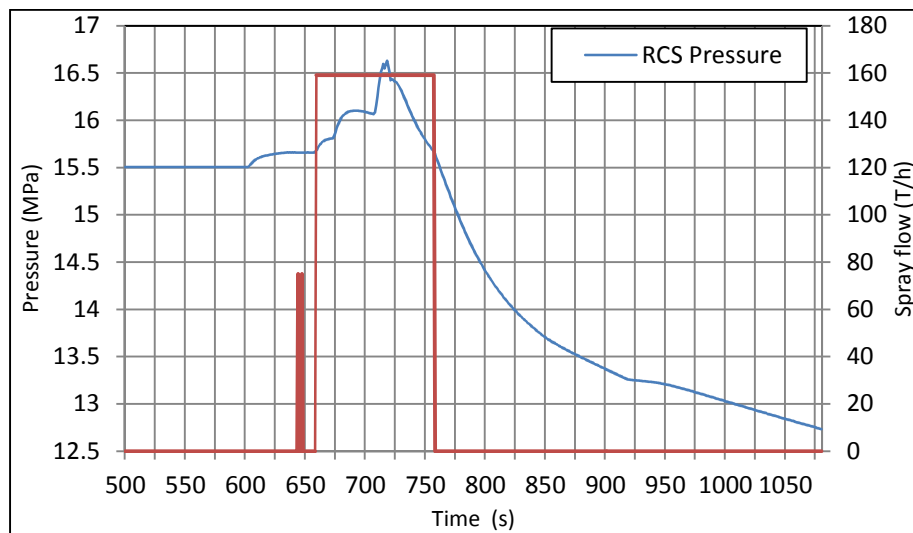


Fig. 4. RCS pressure and spray

In the secondary coolant loop the effect of the blocked auxiliary feedwater flow resulted in an immediate drop in SG level due to the continuation of steam being removed from the SG without the coolant being replaced. The reduced capacity for heat evacuation caused an increase in coolant temperature and pressure. The reduced level and increased pressure in the affected SG is depicted in Figure 5.

During the accident the closed auxiliary feedwater block valves were discovered after 8 minutes (480 seconds) and opened by which time the reactor was already tripped. Although the use of the PDS would detect and characterise the fault within 56 seconds, it is accepted that closing of the valve could still take some time. For this reason we assume that even with the use of the plant diagnostic system the opening of the valve could have occurred 480 seconds after the fault was initiated.

The reactor SCRAM event due to high RCS pressure after 114 seconds coincided with the opening of the power-operated relief valve (PORV) with the intention of reducing the RCS pressure. The PORV should have remained open only temporarily until the pressure was sufficiently reduced, but after the PORV was de-energised it remained stuck open. The stuck open PORV is considered to be the start of the second phase of the accident.

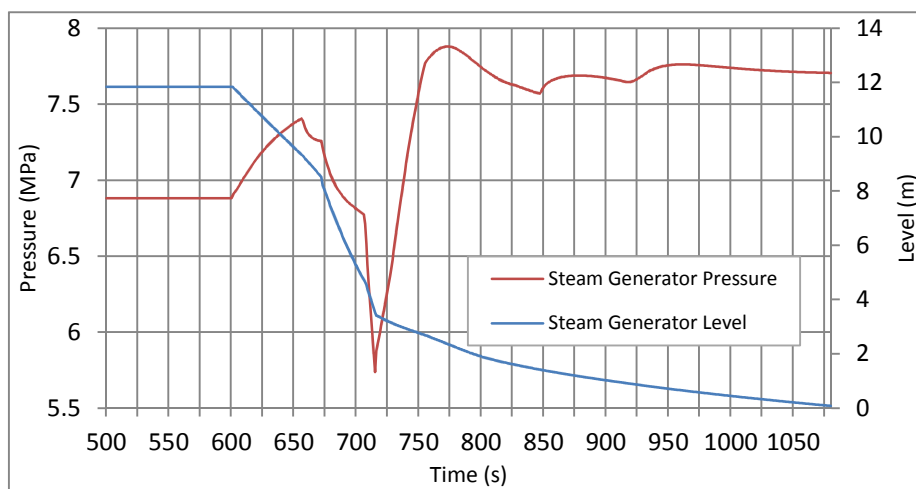


Fig. 5. SG pressure and level

4. Cause 2: Power-operated relief valve failure

When the auxiliary feedwater block valves were opened and since the reactor was already tripped the plant was expected to continue with the automated safety actuation functions that would put the plant in a safe shutdown state. The plant was now in a safety actuation transient which coincides with various operations. These operations make it difficult for the operator to know if what he is observing in the plant is what he should be observing and so, the effect of the failed stuck-open PORV went unnoticed.

The exact size of the stuck-open PORV could not be found in literature, so a size of 10% of maximum was used for the case study purposes.

Since the plant diagnostic system is specifically designed to detect small faults early, it should prove effective in guiding the operators to the leaking PORV. In Table 1, the basic configuration and event sequence are listed.

Tab. 1. Three Mile Island accident configuration

Accident configuration	
Description	Three Mile Island accident
Delay time	0 s
Ramp time	Variable
Failure fraction	Variable
Transient configuration	
Description	Steady state
Transient size	
Transient rate	
Event sequence	
Action	Time (s)
SG feed water block valves closed (Initiating event)	600
PZR safety relief valve auto open	714
Reactor SCRAM	716
PZR safety relief valve fail open	716
SG feed water block valves opened	1080
Safety injection system auto start-up	1139
Safety injection system shutdown	1259
Main coolant pumps 1 and 2 shutdown	4 200
Main coolant pumps 3 and 4 shutdown	6 600
Fuel cladding oxidation, fuel melt	8 700
Close pressure relief block valve	9 600
Safety injection system start-up	12 600

The first parameter to analyse is typically the RCS pressure. The RCS pressures depicted in Figure 6 are those of the TMI plant with the auxiliary feed water block valves closed and opened after eight minutes (480 seconds) in all instances. The expected pressure line represents the simulated information that recognises the closed/opened auxiliary feed water block valves, but does not predict the failure of the PORV.

In this case, the plant still SCRAMs, but since no valve leak is expected, the high-pressure injection (HPI) system is not activated. Incidentally, this is what the operators believed was happening, and when the HPI system was activated, it was turned off. With the PORV leaking an additional drop in pressure is seen until the HPI system is activated, which returns the pressure to normal. Since the pressuriser heater is working at maximum capacity without being able to return the pressure to normal in both cases, the HPI system is seen as the control system compensating for the fault.

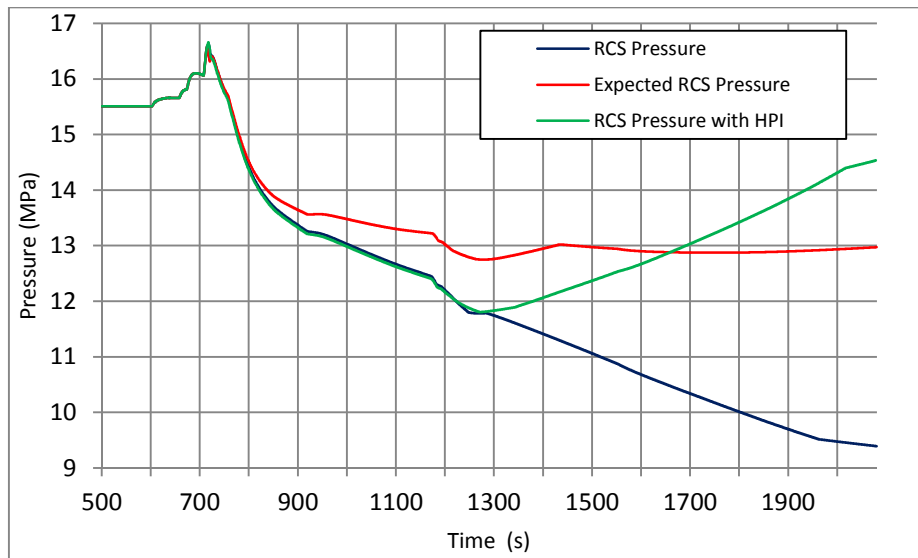


Fig. 6. RCS pressure

If the compensating effect of the HPI is removed, a clear pressure drop is witnessed. Again, since the operators turned off the HPI system, this is the pressure line as it actually occurred in the plant. When the question is raised why this did not alert the operators to a possible leak in the RCS, it should be noted that the operators did not have the luxury of having a correctly operating plant simulation as reference, and if the PORV valve closed as expected the pressure should have decreased due to the safety actuation, just not at the rate it did. Since the events at TMI were not limited to a single fault, it would be very difficult to recognise a fault from a transient without the simulated reference.

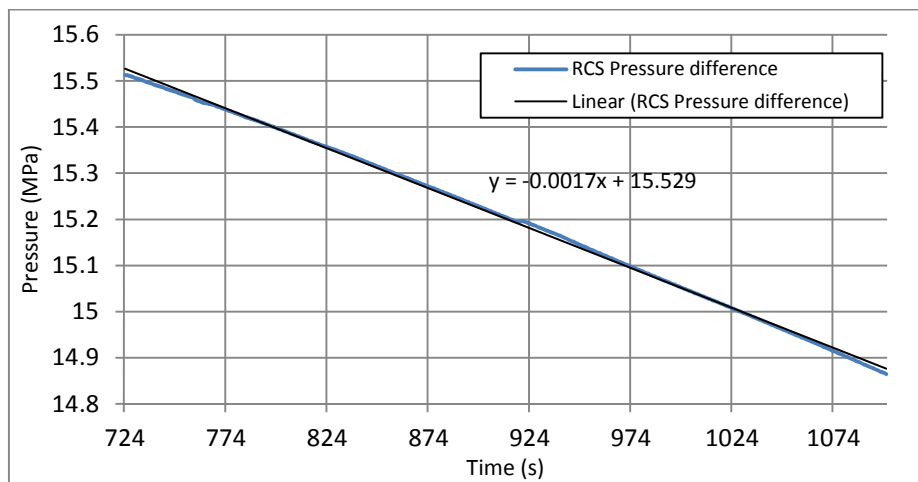


Fig. 7. Actual and expected pressure difference

In Figure 7 the difference between the expected and actual measured pressure is depicted. The difference produces a straight line with a 1,7kPa pressure drop per second. This pressure drop rate corresponds with a 10% valve open leak as modelled using the simulator model. This difference is seen at 724 seconds, 8 seconds after the PORV was stuck open. This would have provided the operators with an immediate and accurate indication of the additional fault that occurred in the system.

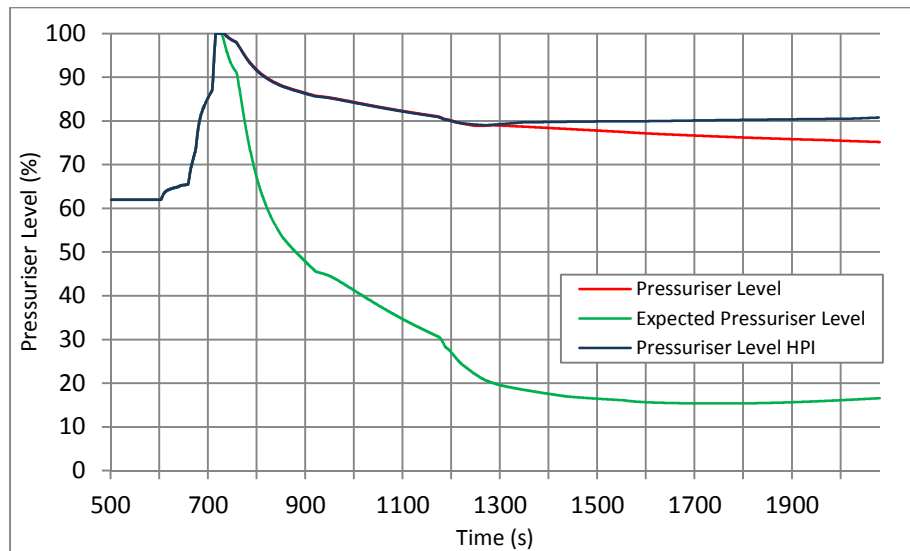


Fig. 8. Pressuriser level and residual inflow

In Figure 8, the pressurised levels of both the PORV fail scenario at TMI and the simulation without the PORV failing are depicted. It is interesting to note that, with the PORV failing, the pressuriser level is at a much higher level than without it failing, this without the control system actually having started to compensate for the fault yet. This is consistent with the events at TMI, as the steam flowing out of the open PORV located more water in the pressuriser, causing voids in other areas of the RCS.

With the effect of the HPI system seen after 600 seconds, the high pressuriser level is maintained, although the operators shut the HPI down in order to prevent the pressuriser being filled solid with coolant.

The calculated RCS volume is depicted in Figure 9. Here the volume with the PORV failing and the reference volume without the PORV failing are shown. With the HPI system being activated, the slight reduction in volume is compensated for, and the reactor is kept safe. With the compensating effect of the HPI being switched off, the volume is reduced significantly. The fact that the HPI was, indeed, switched off was one of the primary reasons that meltdown occurred. The effect was exacerbated by the coolant pumps that had to be shut down due to vibrations caused by pumping a two-phase coolant mixture.

The average rate of change of the RCS volume shows a coolant loss of 18 ton per hour. This is consistent with the PORV leak and indicates an equivalent break with surface area of 0.6 cm² (or 10% valve opening). The 0.6 cm² break is smaller than the area of 0.709 cm² defined for a small break LOCA. The implication of this is that if the control system had not already been responding to the closed auxiliary feed water valves, the fault would have gone unnoticed for a much longer time.

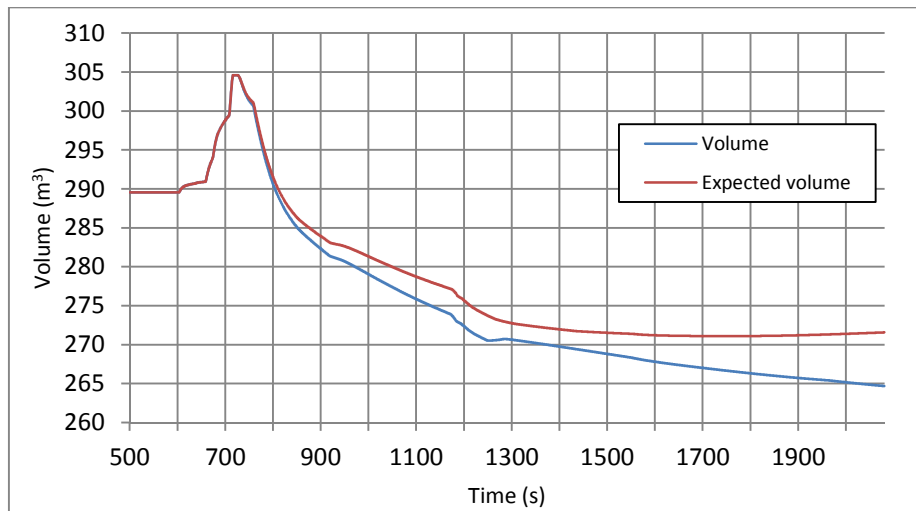


Fig. 9. RCS volume

Figure 10 depicts the flow out of the stuck-open PORV. At first, the PORV opens to relieve the overpressure in the RCS and releases steam at a rate of 196 ton per hour. When it closes, it does not seat properly and keeps on releasing steam in the region of between 15 and 18 ton per hour.

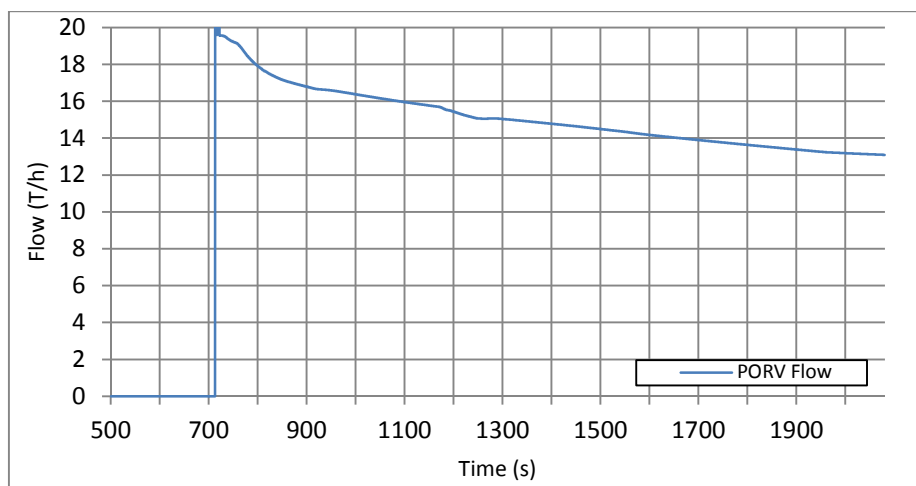


Fig. 10. Flow out of open PORV

The fact that the operators literally shut down the control system that would have allowed the plant to shut down safely – the system that would have also managed to hide the effect of the leaking valve – provides us with a very interesting case study. While the HPI system was operating, the operators had no way of knowing whether the plant was shutting down correctly or not. When the HPI system had been shut down, it should have been clear from the plant-measured parameters that coolant was leaking out of the system – as it is with the use of the PDS. This was not the case, since the operators had no reference transient with which to compare the plant measurements. The PDS provides this reference as well as information on the compensating effect of the HPI, which enables much better interpretation of the same information that the operators had in front of them.

5. Summary and conclusions

From the above results, it can be argued that implementing a plant diagnostic system will result in detecting faults that would otherwise take a long time to detect or would not be detected at all. It can also be argued that the manipulated information sets provided by the plant diagnostic system, which exclude the control system compensating effect, could be very effective in providing information on the nature of the fault. In the case of TMI, the plant could have been stabilised immediately, with the effect of the fault seen in the uncompensated information leading to a clear small loss of coolant event inside the containment.

In conclusion, it is important to combine all methods developed in this research to recommend an acceptable and licensable control and protection architecture in which the plant diagnostic system and other specialised fault identification and control systems can be implemented whilst maintaining separation of systems. This will be presented in a following paper.

6. References

- Cilliers, A.C., 2012. Correlating hardware fault detection information from distributed control systems to isolate and diagnose a fault in Pressurised Water Reactors. *Annals of Nuclear Energy*, in Press.
- Cilliers, A.C., Mulder, E., 2012. Adapting plant measurement data to improve hardware fault detection performance in Pressurised Water Reactors. *Annals of Nuclear Energy*, in Press.
- Cilliers, A.C., Nicholls, D., Helberg, A.S.J., 2011. Fault detection and characterisation in Pressurised Water Reactors using real-time simulations. *Annals of Nuclear Energy*. 38, 1196-1205.
- Cummings, G.E., 1980. Operator/Instrumentation interactions during the Three Mile Island Incident. *IEEE Transactions on Nuclear Science*. 27:1, 931-934.
- Gonzalez, L.C., Gagliardo, R.S., 1980. Electrical modifications to Three Mile Island – Unit 2 during the initial stages of the accident. *IEEE Transactions on Power Apparatus and Systems*, 99:6, 2327-2333.
- Hochreiter, L.E., Robinson, G.E., 2004. *Elements of Nuclear Reactor Design*. Department of Mechanical and Nuclear Engineering, The Pennsylvania State University, University Park, Pennsylvania, USA.
- Le Bot, P., 2004. Human reliability data, human error and accident models – illustration through the Three Mile Island accident analysis. *Reliability Engineering and System Safety*. 83, 153-167.

6.1. Additional notes

6.1.1. Conclusion

In this chapter we made use of the techniques and processes developed in the previous chapters and applied it to a case study of the Three Mile Island nuclear power plant accident. In this way we determined and showcased how the improved information available could present the operator with a better idea to the state of the plant during situations where a combination of faults and transients prevents the operator and conventional systems to recognise the abnormal behaviour.

From the results, it can be argued that implementing a plant diagnostic system will result in detecting faults that would otherwise take a long time to detect or would not be detected at all. It can also be argued that the manipulated information sets provided by the plant diagnostic system, which exclude the control system compensating effect, could be very effective in providing information on the nature of the fault.

7. Conclusion

7.1. Introduction

As discussed in Chapter 1, the main concern of the thesis is to develop a novel dynamic operating envelope used for fault identification together with an implementation framework that would allow the implementation of the system in existing and new NPPs without negatively impacting the existing licensed systems.

Chapter 2 through Chapter 6 examined the pillars used to build the original contribution on, each pillar being studied in terms of recent research done in the field, technological advances and the applicability of using the gained knowledge as a tool in the development of a dynamic operating envelope. Specific problems associated with the application of the field in realising a dynamic operating envelope is identified to be solve, or disqualify the field as a supporting pillar.

In **Chapter 2** a study on existing and proposed fault detection and characterisation methods was done. In particular, fault identification research papers were selected that highlight the limitations and needs at the time of conducting this project. These papers provided a basis on which to develop the proposed fault identification system. **Chapter 3** described the principles when using a real-time plant simulators running in parallel with a nuclear plant to predict the control system behaviour and highlighting unexpected plant behaviour. The control and protection architecture is also developed and described together with the simulator requirements to enable the realisation of the system. In **Chapter 4** the method to adapt plant measurements that isolates the control actions on the fault and re-introduces it into the measurement data, thereby improving plant diagnostic performance is described. **Chapter 5** introduced the use of improved fault detection information received from all distributed systems in the plant control system and correlating the information to not only detect the fault, but also to diagnose it based on the location and magnitude of the fault cause. **Chapter 6** makes use of the techniques and processes developed in the previous papers and apply it to a case study of the Three Mile Island accident. In this way we can determine how the improved information available could present the operator with a better idea to the state of the plant during situations where a combination of faults and transients prevents the operator and conventional systems to recognise the abnormal behaviour.

The research process as described in the abovementioned chapters, combines work on real-time simulator codes with fault identification system advances as well as the ever-present nuclear industry licensing process.

The study of simulator technologies and capabilities in the nuclear industry allows the development of a functional requirement specification for a full scope simulator that can be used as a dynamic reference model in fault detection systems. The survey and study of existing and proposed fault identification systems allow the identification of possible limitations and problems needed to be overcome to achieve the objectives of our proposed fault identification system. By selecting possible

solutions to researched limitations and combining it with the real-time simulator requirements a fault detection method is derived and analytically evaluated. A method is also derived to re-introduce the fault that is masked by the control system outside the closed loop. The combination of the fault re-introduction into all subsystems and the analysis of the conventional distributed control systems in a nuclear plant enable the development of a fault characterisation method.

The methods are tested by setting up a virtual implementation with one simulator representing the plant with the fault introduced and another simulator representing the dynamic reference model. A number of typical faults are tested on the system, as well as a Three Mile Island case study.

Finally, the control plant knowledge, combined with the conventional control and protection architecture and nuclear licensing requirements, allows the development of a revised control and protection architecture framework. This framework would enable the introduction of expert systems such as the fault identification system developed in this thesis without impacting the licensing process of nuclear control and instrumentation.

7.2. Conclusions

The conclusions presented are grouped according to the following thesis objectives:

1. *Develop an in-transient fault detection system by using real-time simulators of nuclear power plants, continuously monitoring and comparing simulated data with the actual measured data from the plant.*
2. *Develop a fault characterisation method, making use of measured and simulated parameters together with actual and simulated control system response. The fault characterisation system should provide information on the magnitude and location of the fault.*
3. *Develop a control and protection framework that allows nuclear power plant licensing within the existing licensing framework, but is also able to exploit the benefits of the latest available control and protection technologies.*

7.3. Simulation-based fault detection system

The fault detection system developed in this thesis is the primary objective of the research.

The system was required to improve on the existing plant **dependability** by:

1. Detecting faults that are of such a small magnitude that they would go undetected when comparing plant measurements to a reference such as expected operating points or even a simulator predicting the expected operating point.
2. Detecting faults during transients when operating point references are unavailable.

3. Detecting and characterising faults that have not been preconceived and simulated to provide a reference fault signature.

The research presented in this thesis was initiated based on the premise that changes between measured parameters in a nuclear power plants and parameters predicted by a simulator simulating the same transient would point to faulty plant behaviour if and when it occurred. This proved to be true in cases where the faulty behaviour was larger than the maximum counteraction of which the control system was capable. In most such cases, the fault was so large that the traditional protection system would have detected the fault and tripped the plant. This is caused by the fault-masking effect of the control system that counteracts a small fault disturbance to maintain a reference operation point.

To work around the fault-masking effect of the control system, we present a method to also compare the control system operations of the simulator and the nuclear plant. This allowed the calculation of a new set of ‘measured’ parameters that did not include the compensating effect of the control system on the fault. The controlling effect of the system on expected transients was not removed and so, allowed the identification of small faults during steady state and transient conditions thus satisfying the abovementioned **dependability** criteria 1 and 2.

The effectiveness of the system was proven experimentally using a plant simulator representing the real-world system as well as the plant simulator. Ultimately, the method was tested on a recreation of the Three Mile Island accident, with the plant diagnostic system predicting the non-fault behaviour and providing a non-fault reference to the plant operators.

7.4. Fault characterisation method

Once a fault has been detected, it is necessary to decide upon an action to be taken in preventing an accident developing from the fault. In order to do this the fault needs to be characterised. The primary method developed in this thesis is not completely novel, it uses known methods of identifying the parameters affected by the fault, then, based on typical fault patterns, it predicts the cause of the fault. It also adds additional control system operations as fault indications. It builds on the novel fault detection system which provides a much better indication to the extent of which the fault affected the specific parameters. In this way better predictions to the cause of and in particular the magnitude of the fault can be made.

The proposed method satisfies the **dependability** criteria 3 by providing uncompensated information of all plant measurements to produce information on the source of the unexpected fault transient as well as the location and magnitude.

7.5. Control and protection implementation framework

The development of the nuclear power plant control and protection implementation framework provides a key to add practical value to the nuclear industry by the seamless addition of expert fault identification systems.

To ensure the effective implementation of such a plant diagnostic system, the I&C philosophies used in the nuclear industry were studied, with variations being recommended and changed as the research progressed. Finally, a complete I&C implementation framework with probabilistic risk assessment requirements was set, which should prove acceptable with international regulators and allow the implementation of digital control systems as well as other sophisticated fault identification systems. The concern of cyber security was discussed, with the advantages the I&C implementation platform as well as the diagnostic system allowed in preventing and detecting cyber threats.

The additional implementation of other existing fault identification systems or the development of more fault identification theories into the platform is made possible by the way the framework is structured: all the plant diagnostic modules have access to the measured plant information without affecting the operation of any other diagnostic modules or the operation of the primary protection system.

The IAEA (1999) mentions that:

“Digital I&C systems are expected to continue as an area of rapid technological development. Future designs of nuclear power plants will require new solutions both in sensing technologies and in digital control. Advanced sensors, detectors, transmitters, and data transmission lines are needed to meet the requirements imposed by the operating conditions of new designs (e.g. high temperatures and high flux) and the harsh environment of ‘beyond design basis’ conditions. Additional monitoring and diagnostic systems will need to be developed, making use of on-line condition monitoring techniques, reactor noise analysis for incipient failure identification, wireless sensor networks and communication, and integrated remote operation.”

The research contained in this thesis provides a platform on which these technological developments can be implemented, as well as providing a specific novel online diagnostic technique. The successful implementation of the system on an existing or new nuclear power plants should be pursued in order to demonstrate the effectiveness in practice. This can be done without impacting the existing plant safety systems.

7.6. Recommendations for future research

The ultimate goal of this research is the implementation of the fault identification system to be implemented as a supervisory system in the Koeberg nuclear power plant as well as including it into the control and instrumentation systems to be implemented in Eskom’s proposed new build program. In order to achieve successful implementations further research needs to be done, in particular:

- The fault identification system needs to be validated on actual plant transient and fault data. This would require logged transient data of start-up, load change, and other transients as well as similar data while a fault occurred. The validation in this thesis was done under controlled conditions with specific known faults being used. Proving the system on actual plant data would add to the validity of the system.
- Implementation of a background supervising system. As with the testing of the system on logged data, a lengthy implementation on the actual plant using real-time measurement and control parameters from the plant without being included as a protection system, will ensure complete validation as well as build the trust in the system. The interaction of control personnel with the system should also be tested and further developed.

8. Bibliography

- Areva, 2006. General EPR Safety Analysis Report. Areva NP, France.
- Barhen, J., Nageswara, S., Rao, V., 2000. Information Fusion Method For System Identification Based On Sensitivity Analysis. International Society of Information Fusion, Proceedings of the Third International Conference on Information Fusion, pp. MoC5 11-17.
- Carrasco, J.A, 2005. Simulation Aids in the Automation of Industrial Processes, Tecnatom, S.A. San Sebastian de los Reyes, Spain.
- Chen, J., Howell, J., 2001. A self-validating control system based approach to plant fault detection and diagnosis. Computers and Chemical Engineering. 25, 337-358.
- Cheon, W., Chang, S.H., Chung, H.Y., Bien, Z.N., 1993. Application of Neural Networks on Multiple Alarm Processing and Diagnosis in Nuclear Power Plants. IEEE Trans Nucl. Sci. 40:1, 11-20.
- Chilin, D., Liu, J., Chen, X., 2012. Fault detection and isolation and fault tolerant control of catalytic alkylation of benzene process. Chemical Engineering Science, 78, 155-166.
- Chilin, D., Liu, J., de la Pena, D.M., 2010. Detection, isolation and handling of actuator faults in distributed model predictive control systems. Journal of Process Control, 20:9, 1059-1075.
- Committee on Application of Digital Instrumentation and Control Systems to Nuclear Power Plant Operations and Safety, 1997. Digital Instrumentation and Control Systems in Nuclear Power Plants: Safety and Reliability Issues, National Academy of Sciences, Washington, D.C, United States of America.
- Common Position of Seven European Nuclear Regulators and Authorised Technical Support Organisations., Licensing of Safety Critical Software for Nuclear Reactors, Europe, 2010.
- Dorr, R., Kratz, F., Ragot, J., Loisy, F., Germain, J., 2007, Detection, Isolation, and Identification of Sensor Faults in Nuclear Power Plants. IEEE Trans Control Syst. Technol. 5:1, 42-60.
- Eskom, 1997. Process instrumentation channel accuracy. Koeberg, South Africa.
- Embrechts, M.J., 2004. Hybrid Identification of Nuclear Power Plant Transients With Artificial Neural Networks. IEEE transactions on industrial electronics. 51:3, 686-693.
- Ferrari, R.M.G., Parisini, T., Polycarpou, M.M., 2008. A Robust Fault Detection and Isolation Scheme for a Class of Uncertain Input-output Discrete-time Nonlinear Systems. American Control Conference, Seattle, Washington, USA, 2804-2809.
- Finc, P, et al., 2006. Workshop in Simulation and Modelling for Advanced Nuclear Energy Systems, Office of Advanced Scientific Computing Research, U.S. Department of Energy, Washington. D.C. USA.
- Frank, P.M., 1990. Fault diagnosis in dynamic systems using analytical and knowledge based redundancy – a survey and some new results. Automatica, 26, 459-474.
- Frank, P.M., Ding, X., 1997. Survey of robust residual generation and evaluation methods in observer-based fault detection systems. Journal of Process Control. 7:6, 403-424.
- Hadad, K., Mortazavi, M., Mastali, M., Safavi, A.A., 2008. Enhanced Neural Network Based Fault Detection of a VVER Nuclear Power Plant With the Aid of Principle Component Analysis. IEEE Trans Nucl. 55:6, 3611-3619.

- Hamelin, F., Sauter, D., 2000. Robust fault detection in uncertain dynamic systems. *Automatica*. 36, 1747-1754.
- Hu K., Yuan J., 2008. Multi-model predictive control method for nuclear steam generator water level. *Energy Conversion and Management*, vol. 49, pp. 1167-1174.
- International Atomic Energy Agency, 1999. Modern Instrumentation and Control for Nuclear Power Plants: A Guidebook. Technical Report Series No. 387. IAEA, Vienna, Austria.
- Iserman, R., 2004. Model-based fault detection and diagnosis – status and applications. Institute of Automatic Control, Darmstadt University of Technology.
- Koeberg, 1997. Koeberg Safety Analysis Report, Revision 4b, Eskom (Pty) Ltd., South Africa.
- Ming, Y., Jianfei, L., Minjun, P., Shengyuan, Y., Zhijian, Z., 2006. A Hybrid Approach for Fault Diagnosis based on Multilevel Flow Models and Artificial Neural Network. *International Conference on Computational Intelligence for Modelling Control and Automation, Web Technologies and Internet Commerce*.
- Paz, R.A, 2002, Model Reference Design Technique, New Mexico State University: Klipsch School of Electrical and Computer Engineering. Las Cruces, USA.
- Petersen, I.R., McFarlane, D.C., 2004. A methodology for robust fault detection in dynamic systems, *Control Engineering Practice*. 12, 123–138.
- Roy, K., Banavar, R.N., Thangasamy, S., 1998. Application of Fault Detection and Identification (FDI) Techniques in Power Regulating Systems of Nuclear Reactors. *IEEE Transactions on nuclear science*. 45:6, 3183-3201.
- Simani, S., Fantuzzi, C., 2000. Fault diagnosis in power plant using neural networks. *Information Sciences*. 127, 125-136.
- Villez, K., Venkatasubramanian, V., Spinner, T., Rengaswamy, R., Garcia, H., Rieger, C., 2010. Achieving resilience in critical infrastructure: A case study for a nuclear power plant cooling loop. *IEEE*, 49-52.
- Wall, R.W, 2005. Power Systems Protection, University of Idaho, USA.
- Westinghouse, 2007. AP1000 Safety Analysis Report. Westinghouse, USA.
- Willsky, A.S., 1976. A Survey of Design Methods for Failure Detection in Dynamic Systems. *Automatica*. 12, 601-611.
- Yan, B., Tian, Z., Shi, S., 2008. A novel distributed approach to robust fault detection and identification. *Electrical Power and Energy Systems*. 30, 343-360.
- Zhang, X., Polycarpou, M., Parisini, T., 2001. Fault Isolation in a Class of Nonlinear Uncertain Input-Output Systems. *Proceedings of the American Control Conference Arlington, Virginia*.

A. Appendix

A.1. General nuclear plant control and protection systems

This section describes the distributed control and protection systems used in Generation II pressurised water reactors and stipulates the relevant operating conditions. The understanding of each of the control systems is required for the development of a fault characterisation method.

A.2. The protection operating window of a pressurised water reactor

The reactor trip system monitors process variables that are directly related to equipment mechanical limitations, such as pressure, pressuriser water level (to prevent water discharge through safety valves and uncovering heaters), and variables that directly affect the heat transfer capability of the reactor (for example, flow and reactor coolant temperatures). Other parameters utilised in the reactor trip system are calculated from various process variables. Whenever a direct process or calculated variable reaches a set point, the reactor will be shut down in order to protect against gross damage to fuel cladding or loss of system integrity that could lead to release of radioactive fission products into the containment.

The following parameters are monitored for direct reactor trips:

1. Nuclear flux
2. Reactor coolant temperature (“ T_{avg} ” and “ ΔT ”)
3. Reactor coolant pressure (pressuriser pressure)
4. Pressuriser water level
5. Reactor coolant flow rate and reactor coolant pump breaker position
6. Reactor coolant pump speed
7. Steam generator steam and feed water flow rates
8. Steam generator water level
9. Operating status of the turbo-alternator set
10. Safety injection, containment spray, or Phase B containment isolation

These parameters have specific set points on which an automatic direct trip is initiated; these set points are depicted in Tab.A.1 from the Koeberg Safety Assessment Report (Koeberg, 1997).

Tab.A.1. Trip set points and time delays of a reference PWR (Koeberg, 1997)

Trip function	Trip set point		Trip time delay (seconds)
	Limiting trip set point	Nominal trip set point	
Power range			
• High neutron flux	118%	109%	0.6
• Low neutron flux	35%	25%	0.6
• High neutron flux rate of			

increase	-6.7% with T = 2 s	-5%	0.6
• High neutron flux rate of decrease	+6.7% with T = 2 s	+5%	0.6
Overtemperature ΔT	Variable $\Delta T_{nom} = 38\text{ }^{\circ}\text{C}$ $T_{nom} = 295.9\text{ }^{\circ}\text{C}$ $P_{nom} = 15.51\text{ MPa}$ $K1 = 1.31$ $K2 = 0.105\text{ MPa}^{-1}$ $K3 = 0.026\text{ }^{\circ}\text{C}^{-1}$ $K7 = 0.35$ $T1 = 4\text{ s}$ $T2 = 4\text{ s}$ $T3 = 30\text{ s}$ $T4 = 4\text{ s}$	Variable	Variable
Overpower ΔT	Variable $K4 = 1.181$ $K5 = 0.0308\text{ (}^{\circ}\text{C)}^{-1}$ $K6 = 0.00338\text{ (}^{\circ}\text{C)}^{-1}$ $K8 = 1.154$ $T1 = 4\text{ s}$ $T5 = 11\text{ s}$ $T7 = 8\text{ s}$	Variable	Variable
Pressuriser			
• High pressure	16.72 MPa	16.66 MPa	1
• Low pressure	12.93 MPa	13.1 MPa	1
Reactor coolant			
• Low flow in one or two loops	85.8%	88.8%	1
• Pump low rotational speed	91.8%	91.9%	0.7
Steam generator			
• Lo-lo level	0%	15%	2
• High level – isolation of main feed water system and turbine trip	85%	75%	2
• Low level coincident with steam/feed water flow mismatch	15%	25%	2

In the case of variable set points such as ΔT at the overtemperature and overpower set points, a number of formulas are derived for changing set points with changing conditions. These formulas translate to Fig.A-1, which displays the trip set points under varying conditions.

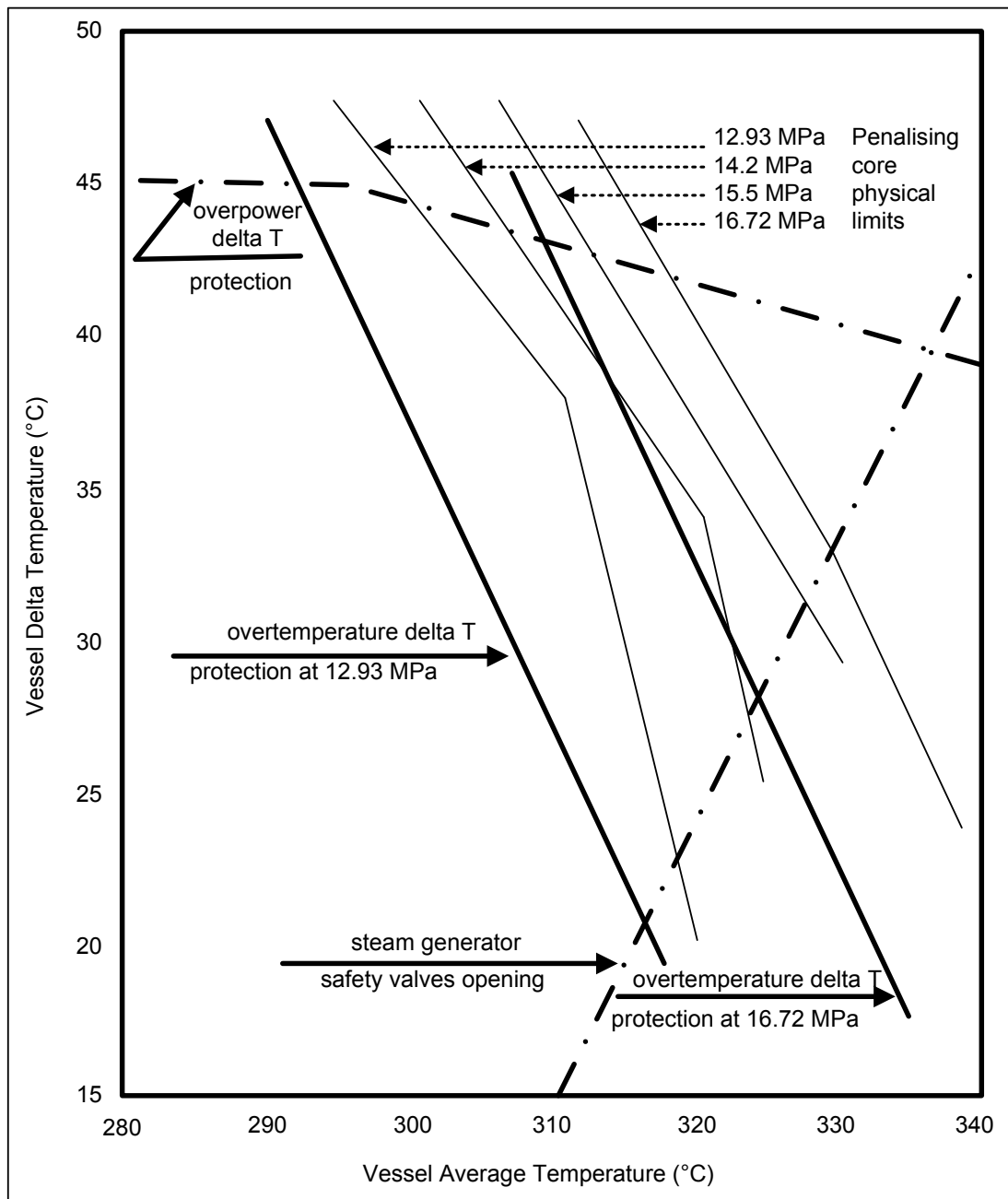


Fig.A-1. Overtemperature and overpower ΔT protection (Koeberg, 1997)

The fixed high-pressure and low-pressure trip set point can be displayed on a pressure temperature graph such as Fig.A-2.

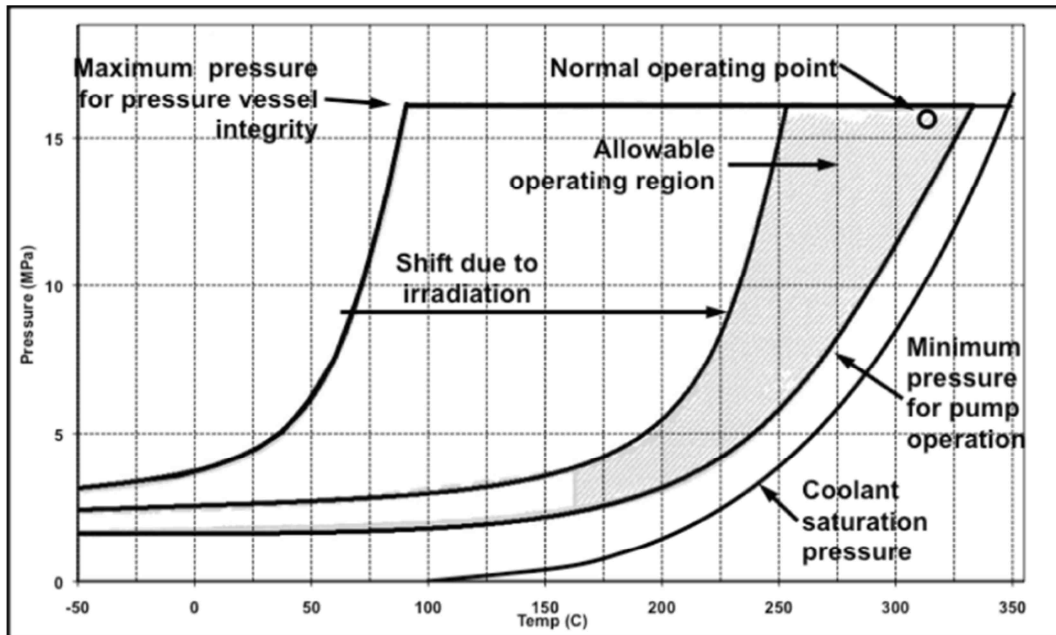


Fig.A-2. Pressure temperature curve for pressure protection

Input signals to the reactor trip system are derived from signals that are direct measurements of unit operating parameters. The signals are generated by analogue channels, which include the input sensors, the associated circuitry, and the set point relays. Each unit operating parameter is monitored by two, three, or four redundant channels, depending on the nature or importance of the parameter measured. For additional redundancy, the logic signals generated by the set point relays are processed identically by two logic trains, A and B. Each of the two trains, A and B, is capable of opening a separate and independent reactor trip breaker. The two trip breakers in series initiate reactor trip by interrupting the power supply to each of the control rod drive mechanisms, thereby unlatching the rods.

A.3. The PWR primary circuit control system

The main parameters to be adjusted and controlled in a typical PWR are:

- Steam flow, adjusted by the turbine governor valves,
- reactor power, controlled by the control rods, and
- feed water flow, controlled by feed water pump speed and feed water valves.

The primary purpose of the PWR control system is to maintain the reactor coolant flow rate constant under all operating conditions to evacuate heat generated in the core at a constant rate. To match the reactor power with the turbine load, the heat generated in the core needs to be varied. This is achieved by moving the control rods in or out of the reactor (Areva, 2006). A typical Generation II (GEN II) PWR can operate between 15 and 100% P_n (unit rated power) with the following capabilities (Koeberg, 1997):

- Steps of $\pm 10\%$ P_n of turbine load.
- ramps of $\pm 5\%$ P_n/minute of load variation without dumping steam to the condenser, and

- load rejection from 100% P_n to the auxiliary power level (5% P_n) with the use of the steam dump to the condenser.

A typical PWR uses seven primary control systems to keep the plant operating at the requested power level and within the designed safety margins (Koeberg, 1997). Each system operates independently of the others with some shared information. These control systems are as follows:

- Power control
 - Reactor average temperature control
 - Rod cluster control
- Pressuriser control
 - Pressure control
 - Level control
- Steam pressure control
 - Condenser steam dump control
 - Atmospheric steam dump control
- Steam generator level control
- Condenser level control
- Turbine speed and load control
- Generator voltage control

The general PWR control schematic with all primary control systems is depicted in Fig.A-3.

The control systems that directly impact the primary coolant system of the PWR are those of the pressuriser pressure and level control and reactor average temperature control. It is also influenced, to a lesser extent, by atmospheric steam dump control, level control, feed water flow control, and steam pressure control (Westinghouse, 2007).

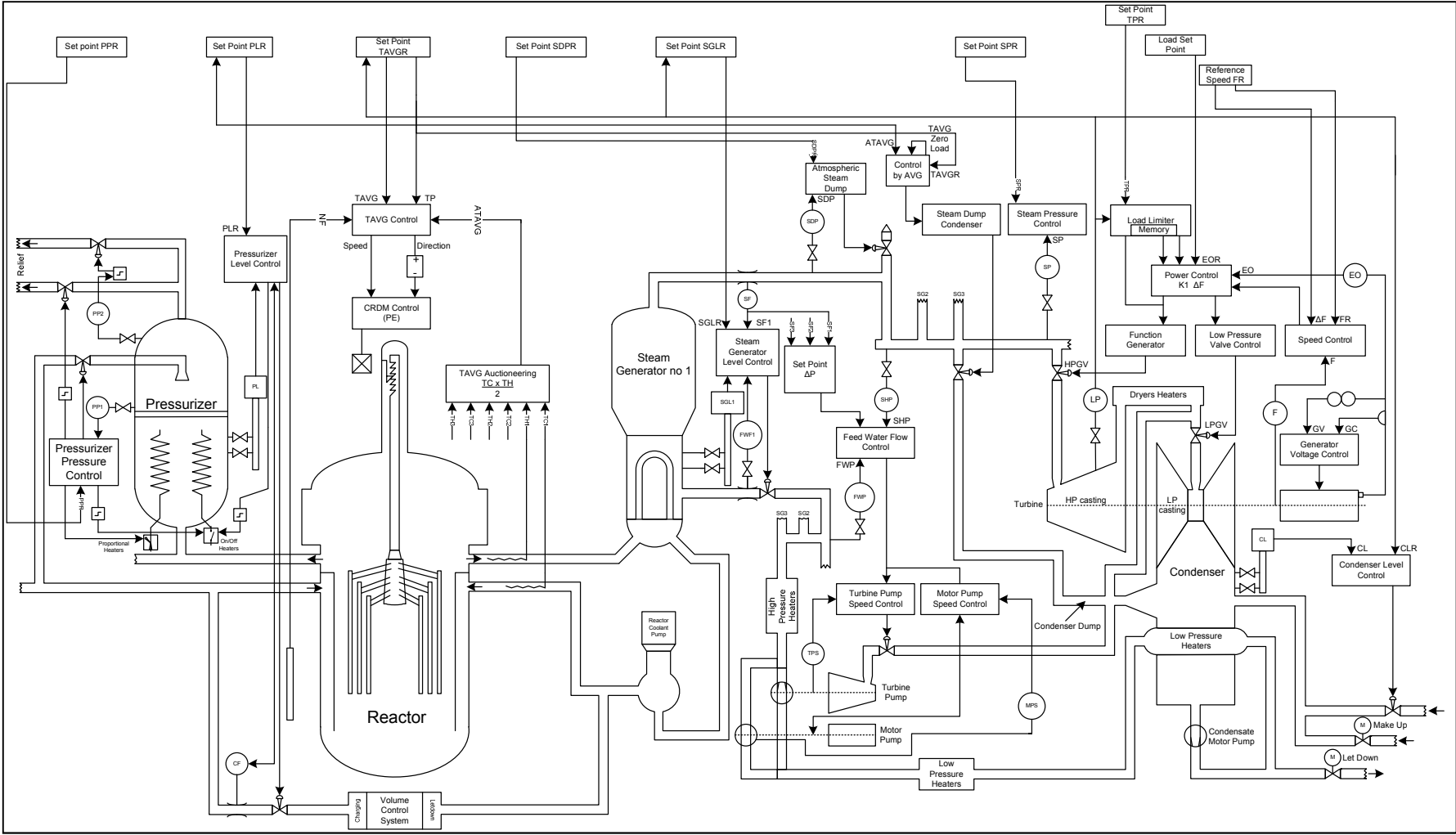


Fig.A-3. PWR general control schematic (Koeberg, 1997)

A.4. Power control

The reactor power is controlled by controlling the reactor average temperature; this, in turn, is controlled by inserting or removing control rods into or from the reactor core (Areva, 2006), (Westinghouse, 2007). In the long term, the reactor power is also controlled by the reactor chemical and volume control system (RCS) changing the boron concentration in the coolant. The slow-acting control does not affect the parameters used to improve the control and protection used in this research.

A.5. Average temperature control

Temperature control depicted in Fig.A-4 is achieved by control rod movement inside the reactor. It is designed to maintain the average temperature within $\pm 1.8^\circ\text{C}$ of the set point. This includes accepted measurement error and a dead band. It is designed to allow for expected operating transients, during which time the control margin is extended beyond the $\pm 1.8^\circ\text{C}$, after which the control system is expected to return the measured temperature to within 0.8°C of the specified set point (Koeberg, 1997).

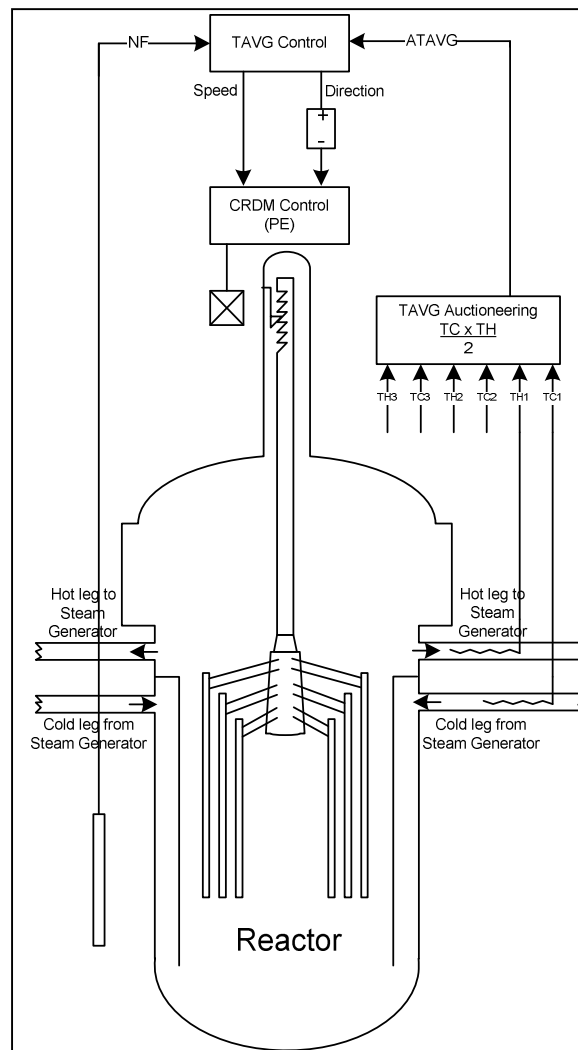


Fig.A-4. Average temperature control

The average temperature is obtained by calculating the average temperature from the cold- and hot-leg thermocouples.

$$T_{avg} = \frac{1}{2}(T_{cold} + T_{hot}) \quad (A-1)$$

Three separate average temperature values are received from three independent channels; from these, the highest value is selected.

The control function is generated by combining measured average temperature, neutron flux, and turbine power. The control system calculates the difference between the reactor power and the turbine load, followed by a derivative controller, whose output increases with the time derivative of this power/load difference and decreases with the turbine load. The result is passed on to a summing module with a single output passed to the control rod speed and direction controller (rod cluster control system) (Koeberg, 1997). The control diagram of the average temperature control by control-rod movement depicted in Fig.A-5 compensates for any expected or unexpected disturbance to the average temperature by moving of the control rods inside the reactor.



A.6. Rod cluster control system

The rod cluster control system uses the information received from the average temperature controller to move the control rods in or out of the reactor core. This position is determined by the difference between the average temperature and set point temperature being positive or negative. The control rod speed is determined by a function generator table (Areva, 2006).

Any unexpected movement of the control rods inside the reactor can be attributed to unexpected changes in core power, turbine power, or average temperature. Since these changes are fully controlled by simply adjusting the speed and position of the control rods, any unexpected disturbance can be modelled as a control rod movement in the opposite direction of the control rod operation.

The control rod clusters consist of four control banks – A, B, C, and D – and two shutdown banks – SA and SB. Each bank contains two sub-banks, consisting of four rods each. The control banks are operated in sequence with an overlap of 100 steps to minimise axial flux asymmetry in the reactor core. The rod cluster control system is capable of varying the control rod speed from six to 72 steps/minute (Koeberg, 1997).

In addition to the control capabilities, the system includes monitoring and interlocking systems to prevent inadvertent control rod operations. These include the following:

- Rod cluster position monitoring system to:
 - know at any specific time the position of any rod cluster,
 - detect incorrect positioning of a control rod cluster in relation to the required configuration at the time,
 - notify by means of alarm signals once insertion and withdrawal limits have been reached, and
 - give warning that either a control or shutdown rod cluster has unexpectedly been dropped into the core.
- Rod stop interlocks to:
 - inhibit inadvertent rod withdrawal (not insertion), since this could result in unsafe plant operations.

A.7. Pressuriser control

The pressuriser's main function is to maintain the primary coolant system pressure constant at all times. The two parameters within the pressuriser that are controlled are pressuriser pressure and level (Westinghouse, 2007).

Pressure control

Pressure control measurements of the pressuriser are used, while the pressure is controlled by a proportional heater and back-up heater for low pressure.

For high pressure, the pressuriser spray and relief valves are used as depicted in Fig.A-6. These control parameters are able to control the pressure level for any disturbance until it reaches maximum operational capacity. Any unexpected disturbance to the pressuriser pressure can, therefore, be modelled as a heat source, for high pressure, and cooling spray or opening of relief valves, for low pressure. Disturbances due to expected transients would be predicted by the real time simulator with no unexpected operations identified.

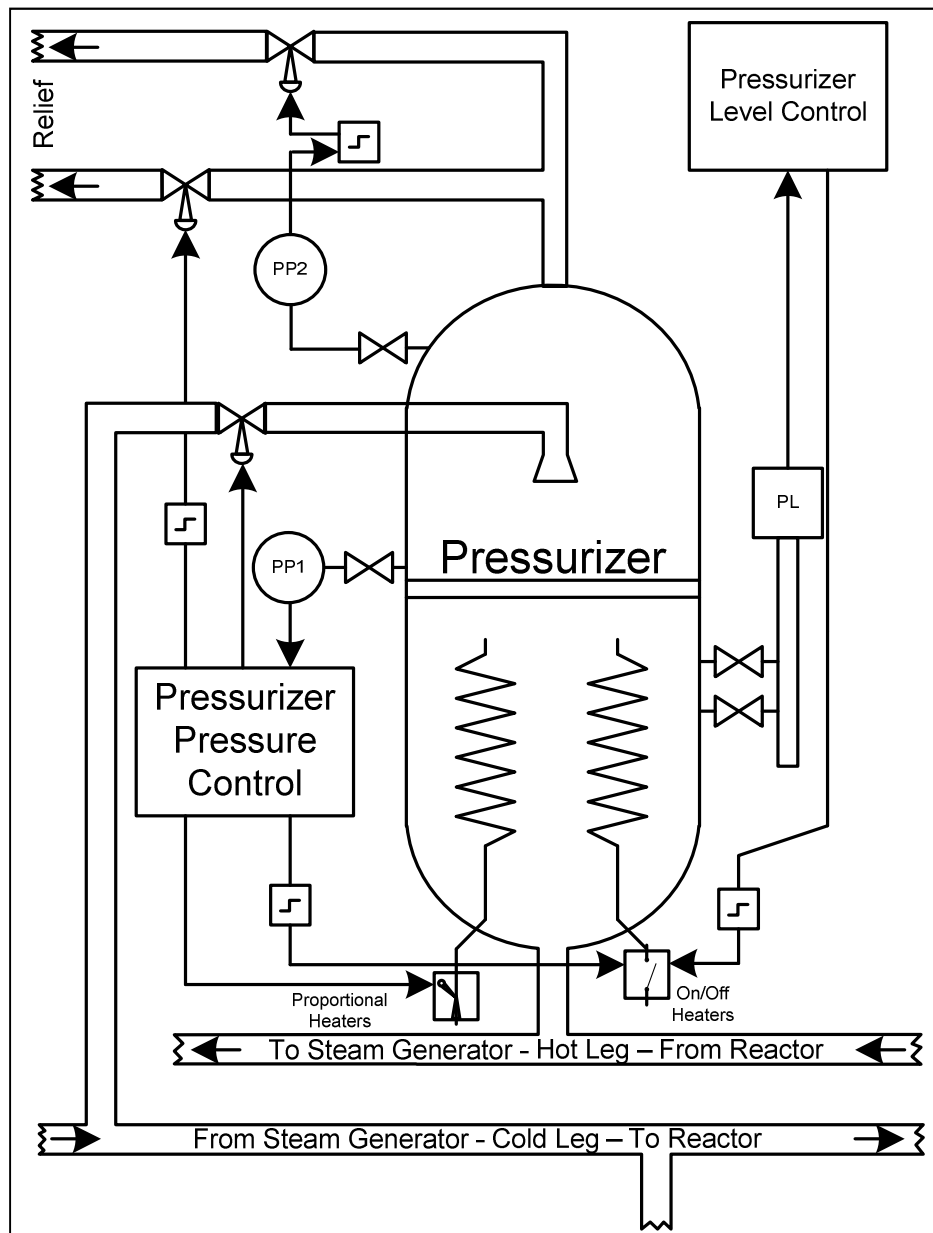


Fig.A-6. Pressuriser pressure and level control

Fig.A-7 depicts the logic used to control the instrumentation. Under steady-state conditions, very few control actions take place, since equilibrium will be reached at some point with a stable control system. A disturbance is introduced into the plant due to certain expected transients or due to an

unexpected fault introduced into the system. In such a case, the control actions will counteract the effect of the disturbance.

In all cases, a real time simulator can predict the effect of each control instrument as well as the expected transient. The unexpected fault, however, cannot be predicted, but affects the operation of all the other control instruments acting on the same operating point. The operating speed is characterised by the PI+D transfer equation:

$$K_{21} \left(1 + \frac{1}{T_{21}s} + T_{22}s \right) \quad (\text{A-2})$$

that is the response the system will have to a disturbance attempting to move the operating point from the reference (typically, 15.5 Mpa).

The response output is passed on to four channels controlling the:

- Pressuriser spray valve,
- proportional heaters,
- on/off switches for the back-up heaters, and
- on/off channel controlling the pressuriser relief valves.

The pressuriser level is controlled by opening letdown and charging valves to and from the cold leg of the coolant loops. The logic that controls the level is discussed in the following section 0.

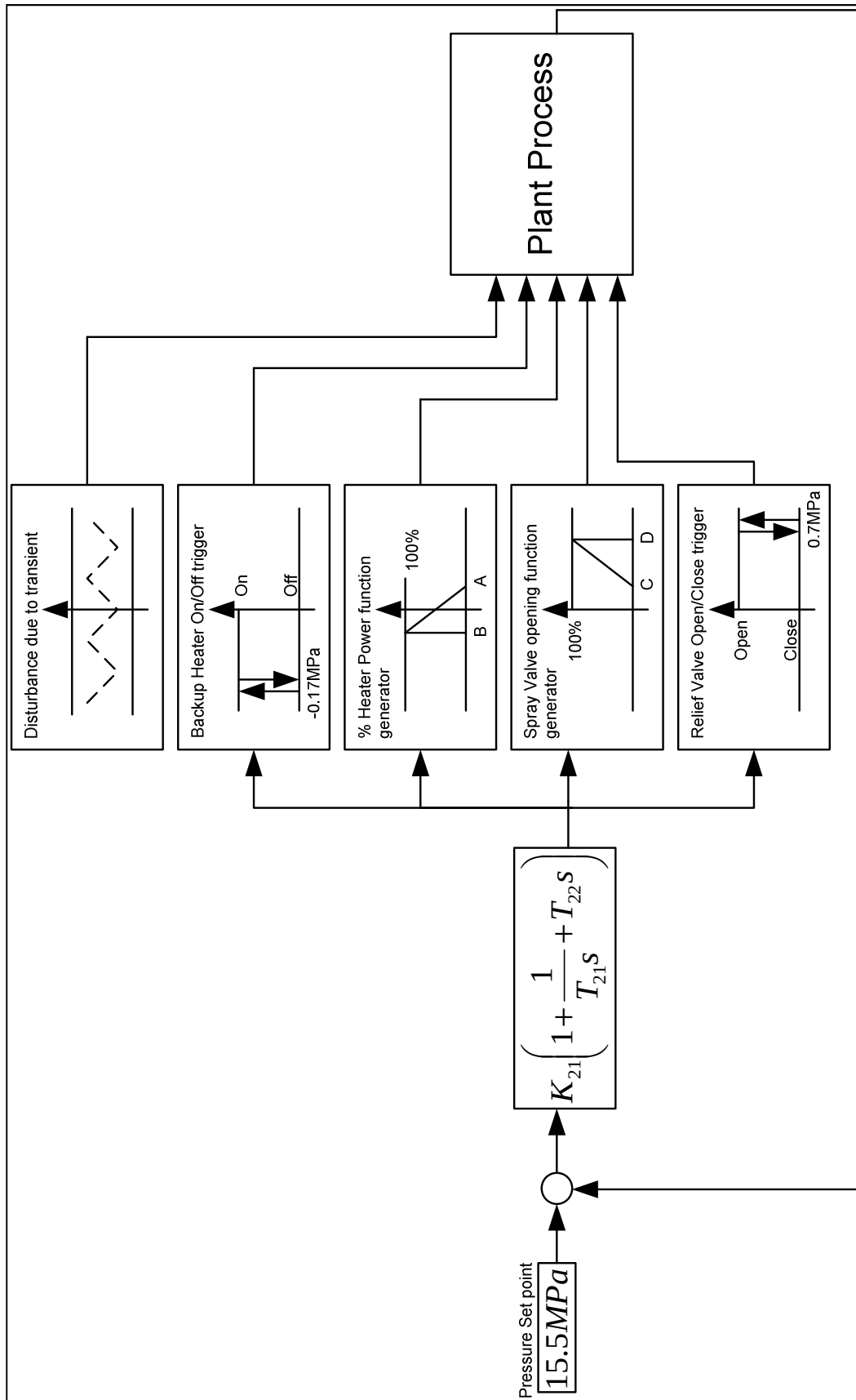


Fig.A-7. Pressuriser pressure control diagram

Level control

The pressuriser level control logic depicted in Fig.A-8 controls the timing and size of the letdown and charging flow valves. The level set point is a function of the average reactor coolant temperature. It includes a dead band that allows for natural temperature-induced level variations. This allows the restriction of charging flow variations during slight power variations. Once the dead band threshold has been breached, the letdown and charging valve opening is controlled by the proportional-integral (PI) transfer function:

$$K_{25} \left(1 + \frac{1}{T_{24}s} \right) \quad (A-3)$$

dictating the disturbance response.

The effect of an expected or unexpected disturbance is compensated for by the feedback control system. This would result in a return to the reference pressure within the control system's designed time. Since the pressuriser level can be controlled fully by the letdown and charging flow, any unexpected operation in the pressuriser level control can be modelled as a letdown or charging flow action for which the pressuriser level control is compensating.

The pressuriser level set point is dependent on the coolant temperature, with higher temperatures resulting in a higher acceptable pressuriser level, since the coolant temperature varies continually, the dead operating band is created to prevent the pressuriser level control from continually operating. In the case of the pressuriser level remaining in the dead region between ± 0.8 °C on either side of the full power reference and $+2$ °C and -3 °C on either side of the no-load reference temperature, the control system would not interject and, thus, would have no unexpected operation acting on the pressuriser level. In such a case, the information from the level-measurement input is clean and can be compared to the expected pressuriser level from the simulator. During expected transients, the behaviour of the level control system could be predicted by a real time simulator with an unexpected operation detected when it occurs (Koeberg, 1997).

At this point, it should be mentioned that many of the parameters being controlled are interdependent, and as such, during expected or unexpected transients, a number of parameters would need to be controlled to return to the reference value. This implies that unexpected faulty plant operation would have a number of control systems operating on it to reduce its effects. The unexpected disturbance would then be modelled as a number of control operations opposed to a single control operation. The benefit obtained from such a combination of modelled control operations is that it describes the nature of the fault completely, resulting in effective fault characterisation.

In 2007 Hu K and Yuan attempted to optimise the SG water level control method by implementing a multi-model predictive control method since the dynamics of a nuclear SG vary according to the power levels and changes as time goes on. In their research, a robust model predictive control (RMPC) method was developed for the level control problem (Hu and Yuan, 2008).

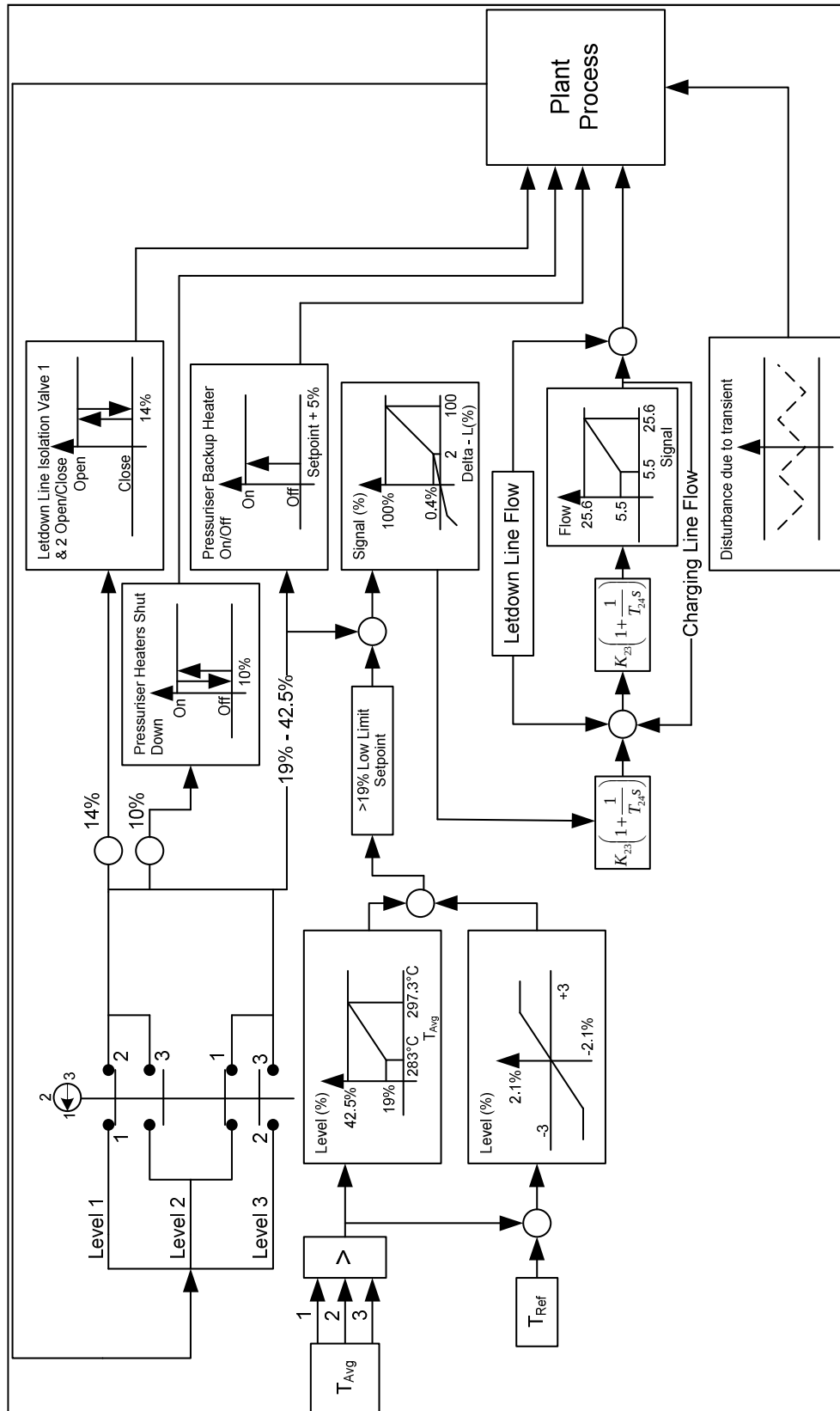


Fig.A-8. Pressuriser level control diagram

When implementing the fault identification method described in this thesis, an optimised method such as that of Hu and Yuan (2008), would not affect the effectiveness of the fault identification system. In

fact, being able to control the pressuriser level within a narrower band would increase speed of the fault identification system in detecting unexpected control system operations. It is, however required that the simulator includes an exact model of the control system in use in the plant.

A.8. Steam pressure control

The secondary circuit steam dump system is used to create a temporary artificial load during certain transients by releasing steam from upstream of the turbine inlet valves to the condenser, as back-up steam can be dumped to the atmosphere. The steam generator with relevant control systems is depicted in Fig.A-9.

Condenser steam dump control

The condenser steam dump is actuated during turbine instantaneous load reductions higher than 10% Pn or continuous reductions greater than 5% Pn/minute (Koeberg, 1997).

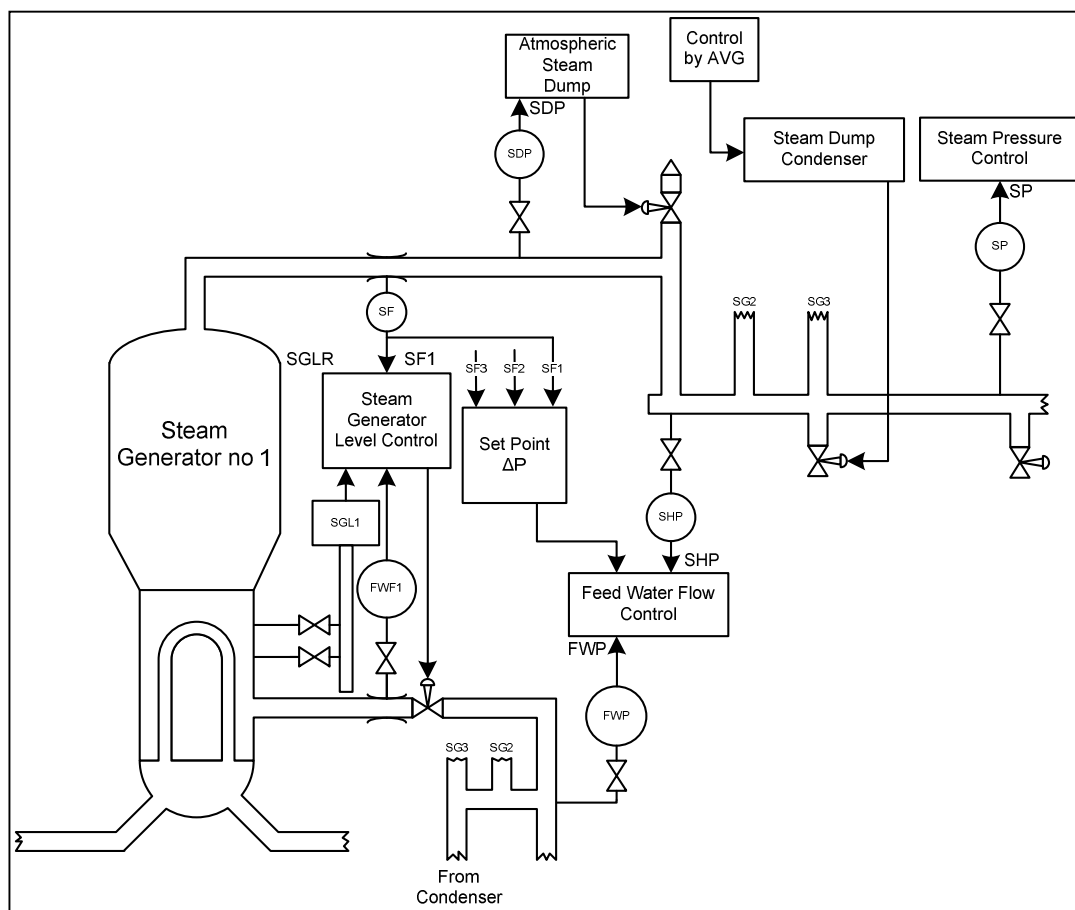


Fig.A-9. Steam generator with related controls

Atmospheric steam dump control

When the condenser steam dump or condenser is unavailable, the atmospheric steam dump channels are used to:

- Permit control of steam generator pressure at loads smaller than 10% Pn, and
- permit cooling down or controlled heating up of the reactor coolant system.

The atmospheric steam dump system is equipped with three identical independent channels with independent control systems. The steam pressure at the steam generator outlet is measured and passed on to the PI controller, where it is compared to an internal set point value.

$$K_{12} \left(1 + \frac{1}{T_{15}s} \right) \quad (A-4)$$

The controller dictates the opening of the steam dump valves.

A.9. Steam generator level control

The steam generator level is controlled by feed water flow and steam flow. Steam flow is determined by the turbine load, and so the feed water flow needs to be adjusted accordingly to maintain acceptable steam generator levels. The feed water flow is regulated by feed regulating valves and turbine-driven feed water pumps with motor-driven feed water pumps as back-up.

The feed water flow set point is dynamic and obtained by maintaining the water head pressure and steam head pressure ratio constant at loads between 0 and 20% with the level increasing linearly as a function of turbine load to offset the differential change between the inlet and outlet pressures of the steam generators. The level error signal is passed on to a PI controller that controls the speed of the turbine- and motor-driven feed water pumps (Koeberg, 1997).

$$K_2 \left(1 + \frac{1}{T_2s} \right) \quad (A-5)$$

A.10. Condenser level control

The condenser level has a dynamic set point that varies as a function of load to prevent unnecessary water make-up and discharge due to temperature variations. Water make-up is supplied via a nozzle in the pressure header from the demineralised water storage tank. Larger make-up is achieved by a motor-operated valve in parallel with the normal make-up valve.

Turbine speed and load control

The turbine speed and power are controlled by operation of the high-pressure (HP) and low-pressure (LP) valves. The valve openings are determined from the sum of the speed and load measurements.

A.11. Generator voltage control

The generator voltage is controlled through changing the excitation current. The set point is determined by the operator through a control rheostat.

A.12. Safety Functions

The primary objective in the control of faulty plant behaviour and accidents is to prevent the release of radioactivity into the environment. This activity retention objective is supported by the safety I&C and the corresponding safety systems, with the safety I&C designed to match the set of safety functions based on the defence-in-depth concept for the following activity barriers:

- Fuel rod cladding,
- reactor coolant pressure boundary, and
- containment and safeguard buildings.

The integrity of these barriers is to be ensured by the associated safety functions. When faulty conditions are detected in more than one plant sub-system, the combination provides an indication to the nature of the fault. This provides a certain level of characterisation of the plant faulty behaviour. A number of postulated faults are combined into accident groups to assist with the characterisation process:

- Reactivity abnormalities:
 - Uncontrolled Rod Cluster Control Assembly (RCCA) bank withdrawal during subcritical state,
 - uncontrolled RCCA bank withdrawal at power,
 - rod drop and single RCCA withdrawal at power,
 - rod ejection,
 - Uncontrolled boron dilution.
- Loss of reactor coolant flow:
 - Forced decrease in reactor coolant flow,
 - partial loss of reactor coolant flow,
 - reactor coolant pump shaft break or locked rotor.
- Loss of primary coolant:
 - Small break LOCA,
 - intermediate and large break LOCA.
- Steam generator tube failure:
 - Rupture of up to 2 steam generator tubes.
- Loss of main heat sink:
 - Loss of condenser,
 - inadvertent closure of Main Steam (MS) isolation valves,
 - loss of off-site power.
- Loss of secondary fluid and overcooling events:
 - Spurious opening of MS bypass, SG relief train or SG safety valve,
 - failure of MS relief or safety valve to close after challenge,
 - steam system piping failure,

- o feedwater system piping failure.
- Other accidents during shutdown:
- Uncontrolled level drop during mid-loop operation,
- Loss of a Low Head Safety Injection/Residual Heat Removal (LHSI/RHR) cooling train.

If the second approach is followed, the adapted measurement data is not compared to the fixed operating envelope boundaries, but rather with the expected operating point of the dynamic reference. In this way, the maximum and minimum limits from Tab. A.2 are changes to dynamic expected values from the dynamic reference. Once the adapted measurement moves outside the reference and instrumentation tolerance boundary for all affected systems, a fault is detected and diagnosed.

Tab A.2 correlates these accident groups with the actuation criteria that are to be expected in each case and lead to reactor trip. The table shows that an adequate number of independent and diverse initiation criteria are provided in all cases for initiating reactor trip and/or turbine trip.

The combinations of fault indications in the different sub-systems are derived from simulating the various postulated faults and analysing its effect on the different subsystems. The information from the table is used in the reactor protection system to determine which safety actuation functions should be initiated to prevent structural damage to the reactor.

Tab.A.2. Fault groups with initiating measurements

Measurement indications	Uncontrolled control assembly withdrawal in subcritical cold condition	Uncontrolled control assembly withdrawal in subcritical cold condition	Inadvertent reduction in RCS boron concentration	Loss of reactor coolant pumps	Primary loss of coolant	SG tube rupture	Leaks and breaks in the MS system	Leaks and breaks in the Feed Water system	Loss of off-site power	Loss of main heat sink	Inadvertent closure of secondary loop isolation valve
Intermediate range neutron flux > max	x										
Intermediate range neutron flux doubling time > max	x										
Power range neutron flux rate of change > max		x	x								
Reactor thermal power > max		x	x								
RCP speed < min for > 1 loop				x					x		
PRZ level > max	x	x	x	x				x	x	x	x
PRZ pressure > max	x	x	x	x				x	x	x	x

PRZ pressure < min					x	x					
SG pressure > max				x					x	x	x
SG pressure drop > max							x				
SG pressure < min							x		x		
SG level A < min							x	x	x		
SG level A > max						x					
Containment pressure > max					x		x	x			

A.13. Instrumentation and transmission accuracies

To ensure effective fault detection and characterisation it is required to determine the instrumentation equipment and information channel accuracies. The accuracy figures was made available by the Koeberg power station as obtained from instrument specifications for sensors and from manufacturer's data for electronic modules (Eskom, 1997).

Accuracies are calculated:

- at the transmitter level (measurement accuracy)
- at the threshold detector level (trip accuracy during routine testing) under normal operating conditions with instruments calibrated at set point value.

Combined errors are calculated by taking the square root of the sum of the squares of component errors (Eskom, 1997):

$$\varepsilon = \sqrt{\sum_{n=1}^{\infty} (e_n)^2} \quad (\text{A-6})$$

In Tab.A.3 below, the combined accuracies of the various measurement instrumentations are listed.

Tab.A.3 Instrumentation accuracies

Channel	Maximum error
Reactor coolant pressure	2.72%
Reactor coolant flow	3.12%
Pressuriser pressure	2.67%
Pressuriser level	3.11%
Hot leg and cold leg temperature	0.49%
Delta temperature	3.15%
Average temperature	1.08%
Steam generator level:	3.11%
Feedwater flow rate:	2.90%
Steam pressure:	1.40%
Steam flow:	3.07%
Turbine first stage pressure:	1.40%
Volume control tank level	3.06%
Accumulator pressure	2.72%
Accumulator level	3.35%

Containment pressure	2.72%
Refuelling water storage tank level	2.80%
Containment spray	2.35%

With a maximum error of 3.35% for the accumulator level, indicates that the indicated fault will be increased or decreased by values in the order of between a 1000th and 10000th of the reference value and expected disturbance signals. If we assume that the simulator would be able to maintain similar accuracy levels to result in a 6.7% maximum error, the error factor increases very slightly but remains below the 1000th error factor level.

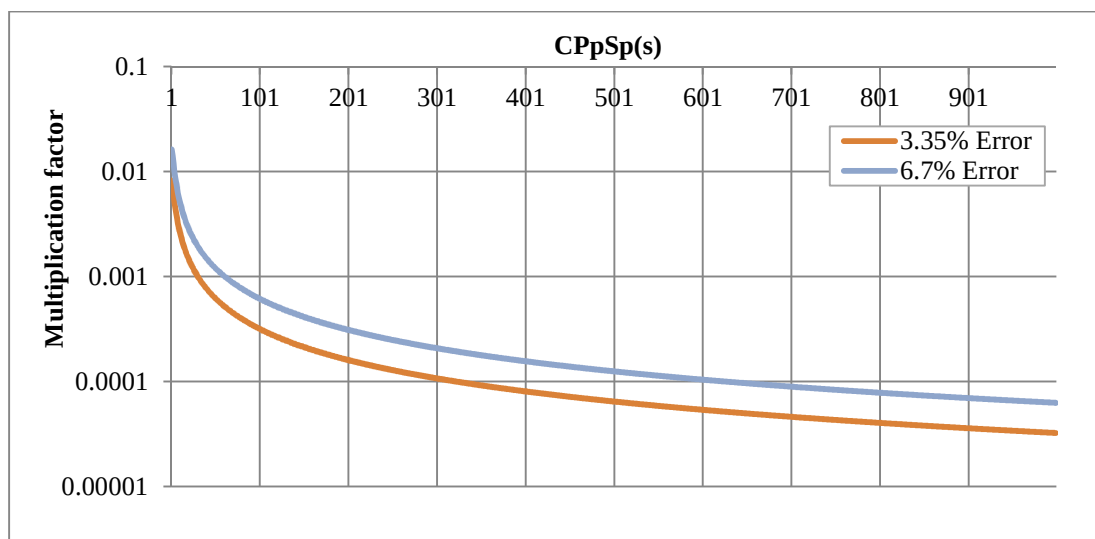


Fig.A-10. Multiplication factor for maximum instrumentation errors

A.14. Summary and conclusions

The trip conditions examined in this chapter form part of the safety systems of the plant together with the actuated safety systems that shut down the plant safely during accident conditions. The described protection and control systems are licenced and implemented with only slight variations in all nuclear plants around the world.

B. Appendix

B.1. Implementation

This section discusses the implementation of the PDS in an existing PWR. It provides schematics of the entire system with all data required from the PWR I&C systems. The implementation is done as a diagnostic system that does not interfere with the existing operation of the plant.

To implement the proposed fault identification system, an interface between the real time simulator and the actual plant is required. The interface in Fig.B-1 compares the measured parameters of the plant with the simulated parameters from the simulator as well as the control system actions of the plant with the simulated control system actions of the simulator. In Fig.B-1, the complete PDS interface is depicted, with all primary control systems feeding measured information to the control system as well as the PDS. The plant control system also feeds its control parameters to the PDS. On the other side of the PDS, the simulator is running in real time with the very same conditions as the plant. Any known external controls such as load change and manual controls that initiate transients in the plant are also fed to the simulator.

Once the PDS starts detecting differences in instrumentation or control variables between the plant and the simulator, the diagnostic sequence is initiated. In all cases, the first difference that the PDS would register is a difference in instrumentation measurements compared to the simulated measurements. This would immediately be followed by the control system reacting to compensate for the fault. If the control system does not react to compensate for the measurement variance, the measured parameter is still within its allowed tolerance. This prevents the PDS from identifying false faults.

Once the control system of the plant and that of the simulator have started varying, the PDS uses the variance to calculate what the plant measurements would have been without the control system attempting to counter the effects of the fault. The PDS also uses the variance in the control parameters to build a transfer function of the fault, using the transfer functions of the specific control system. Once the transfer function has been acquired, the system response to the fault is transformed by the transfer function to the original input produced by the fault disturbance into the system. This may happen in more than one control system at once, with the produced fault disturbance having the same cause for all control system variances. Combining the fault disturbance from all the systems characterises the fault completely.

The following sections in this chapter discuss the various subcomponents of the PDS in more detail.

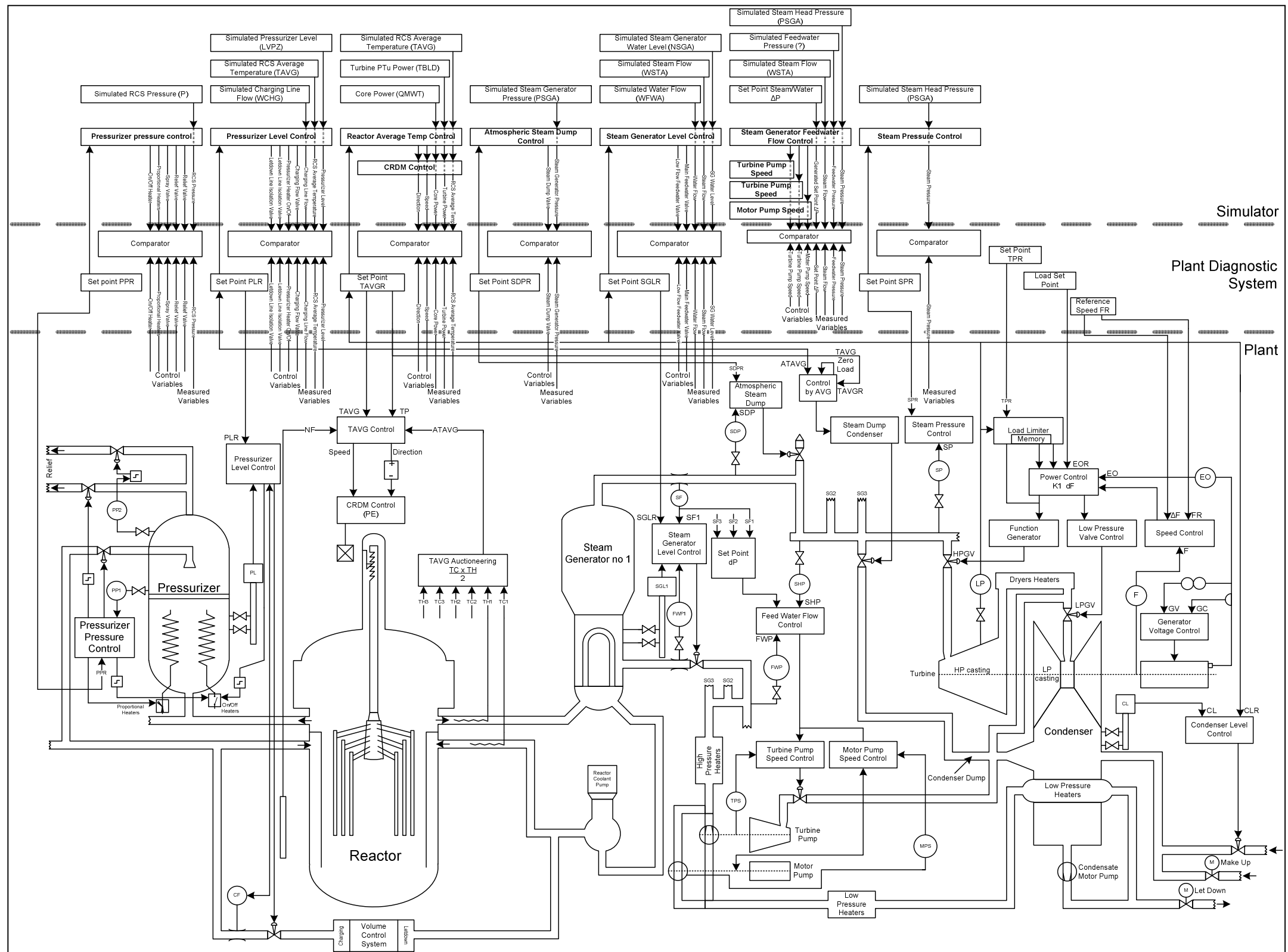


Fig.B-1. Full PDS implementation

B.2. Power control PDS

Power is controlled by changing the reactor average temperature. The temperature is controlled by moving control rods in and out of the reactor core. The PDS requires both real and simulated control and instrument parameters. The system is depicted in Fig.B-2.

From the measurement instrumentation, the PDS requires:

- RCS average temperature,
- turbine power, and
- core power.

From the control system, the PDS receives:

- control rod direction, and
- control rod speed.

In the case of a fault causing over or under temperature, the system will recognise the fluctuation in temperature, followed by the reaction of the control rods moving in or out of the core. In many instances, the control system (movement of control rods) will be able to return the temperature – and, thus, the power – to the design temperature for the required power. Since the temperature and power will soon return to normal, the existing protection systems would be unable to detect a fault condition, especially during expected transients such as load following where the control rods are expected to move to adapt to the power level. The simulator, running in real time with the plant, would be following the same expected transient. It would not be aware of the fault conditions and, so, would not have the control rods react to the change in temperature owing to the fault. The difference between the expected control rod and actual control rod operation results in providing much more information about the plant health than the plant measurements alone.

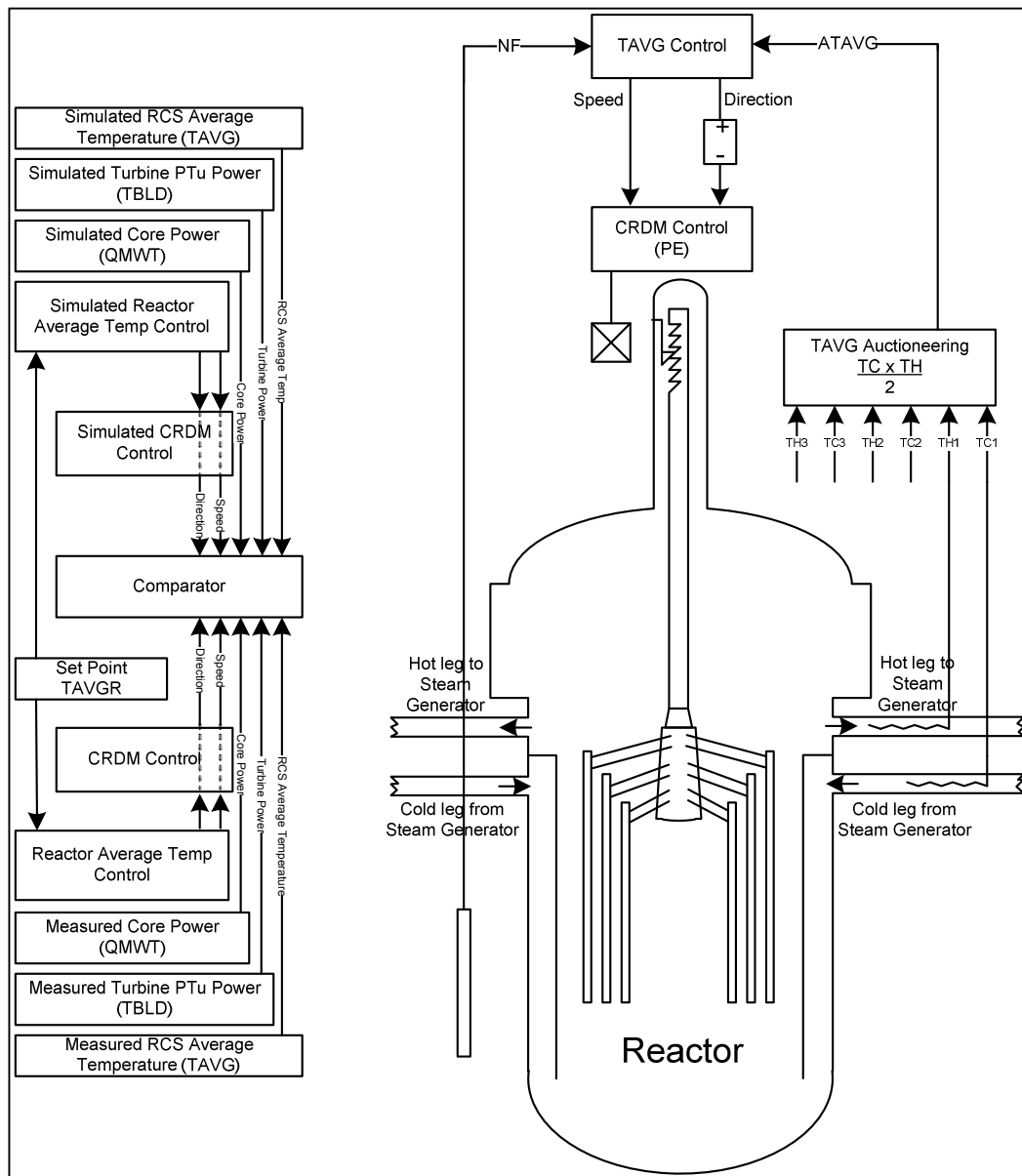


Fig.B-2. Reactor temperature control with PDS

To model this, we introduce an unknown fault disturbance into the real plant. The fault disturbance should be zero during normal plant operation with the plant and the simulator in synchronisation. When a fault occurs, the fault disturbance would change, but remain unknown, and since the expected operation of the control rods is known thanks to the online simulator, the fault disturbance remains the only unknown in the plant.

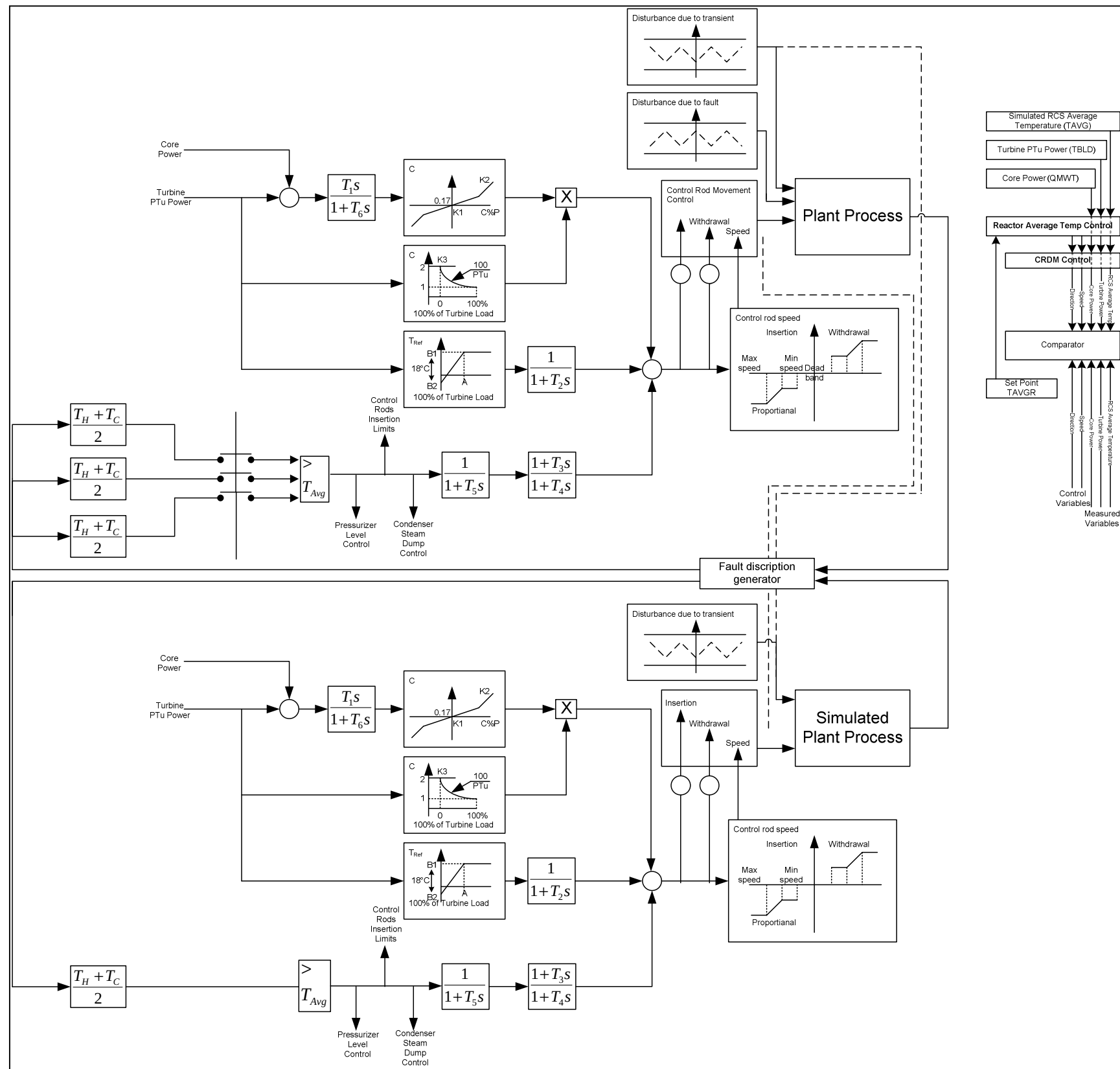


Fig.B-3. Power control schematic with PDS

Fig.B-3 depicts the full power control schematic with both the control and instrumentation parameters from the plant and the simulator. The plant and the simulator also both include input disturbances from expected transients. These disturbances would activate the control system to return the measurement parameters to the design value. The schematic of the plant also includes a fault disturbance that is not included in the simulator, since an unknown fault disturbance could be non-zero in the plant, but not in the simulator.

B.3. Pressuriser level control PDS

The pressuriser level control logic controls the timing and size of the letdown and charging flow valves. The PDS requires control and instrument parameters from both the plant and the simulator for comparison. The system is depicted in Fig.B-4.

From the measurement instrumentation, the PDS requires:

- RCS average temperature,
- pressuriser level,
- charging line flow, and
- letdown line flow.

From the control system, the PDS receives:

- Charging valve opening,
- letdown valve opening, and
- pressuriser heater on/off status.

In the case of a fault causing the pressuriser level to move outside the expected range for normal temperature fluctuations, the system will recognise the change in pressuriser level, followed by the reaction of the charging or letdown valves operating to increase or decrease the pressuriser level. In many instances, the control system (charging and letdown flow) will be able to return the pressuriser level to the designated pressuriser level. Since the pressuriser level will soon return to normal, the existing protection systems would be unable to detect a fault condition, especially during expected transients such as load following where the charging and letdown valves are constantly moving to adapt the pressuriser level. The simulator, running in real time with the plant, would be following the same expected transient, would not be aware of the fault conditions and, so, would not have the charging and letdown valves react to compensate for the change in pressuriser level due to the fault, only for the expected transient. The difference between the expected residual flow and actual residual flow provides much more information about the plant health than the plant measurements alone.

To model this, we introduce an unknown fault disturbance into the real plant. The fault disturbance should be zero during normal plant operation with the plant and the simulator operating in synchronisation. When a fault occurs, the fault disturbance would change, but remains unknown, and since the expected operation of the charging and letdown valves is known thanks to the online simulator, the fault disturbance remains the only unknown in the plant.

Fig.B-5 depicts the full pressure and level control schematic with both the control and instrumentation parameters from the plant and the simulator. The plant and the simulator both include the input disturbances from expected transients. These disturbances would activate the control system to return the measurement parameters to the design value. The plant, however, also includes a fault disturbance that is not included in the simulator.

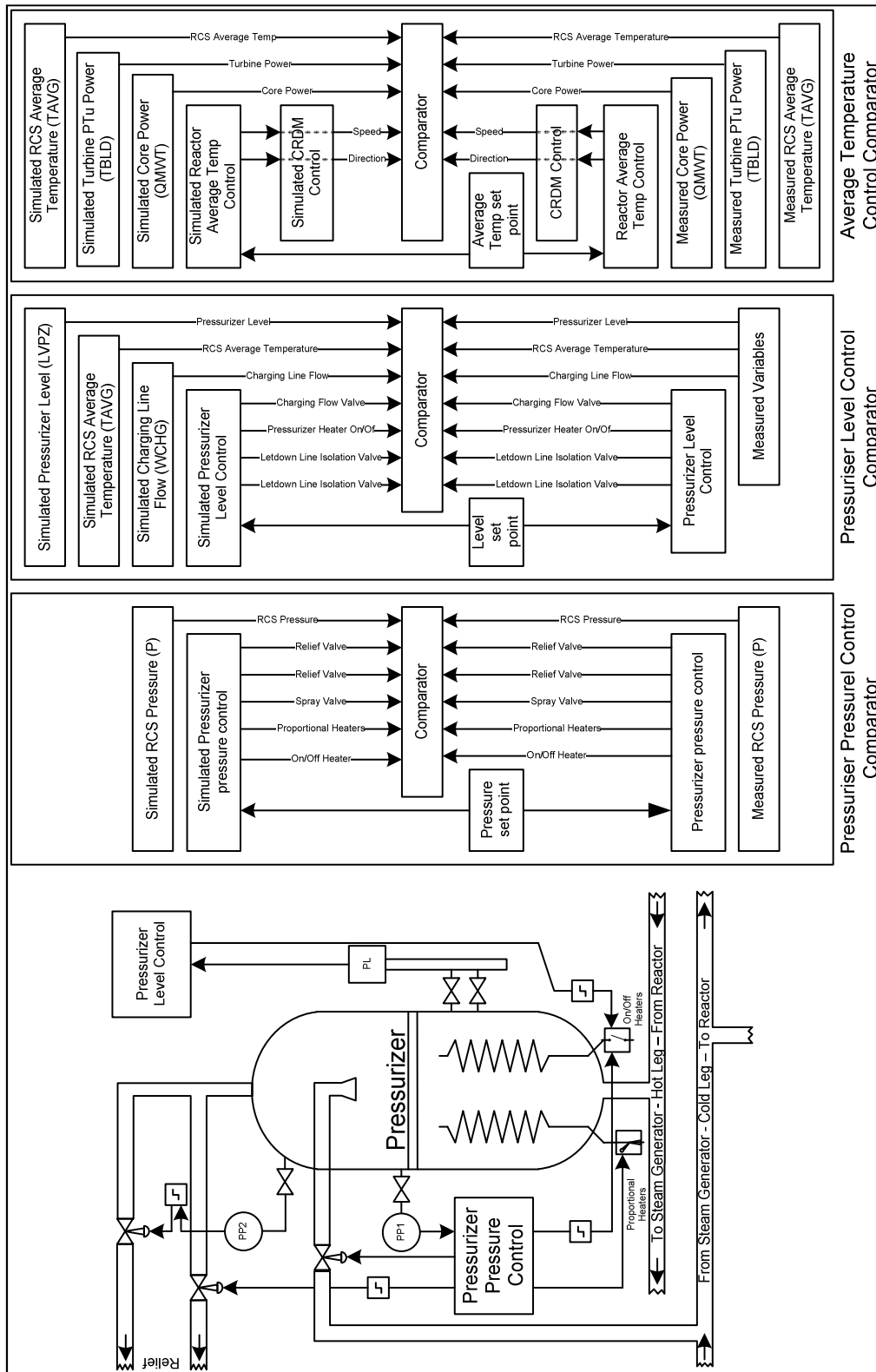


Fig.B-4. Pressure and level control with PDS

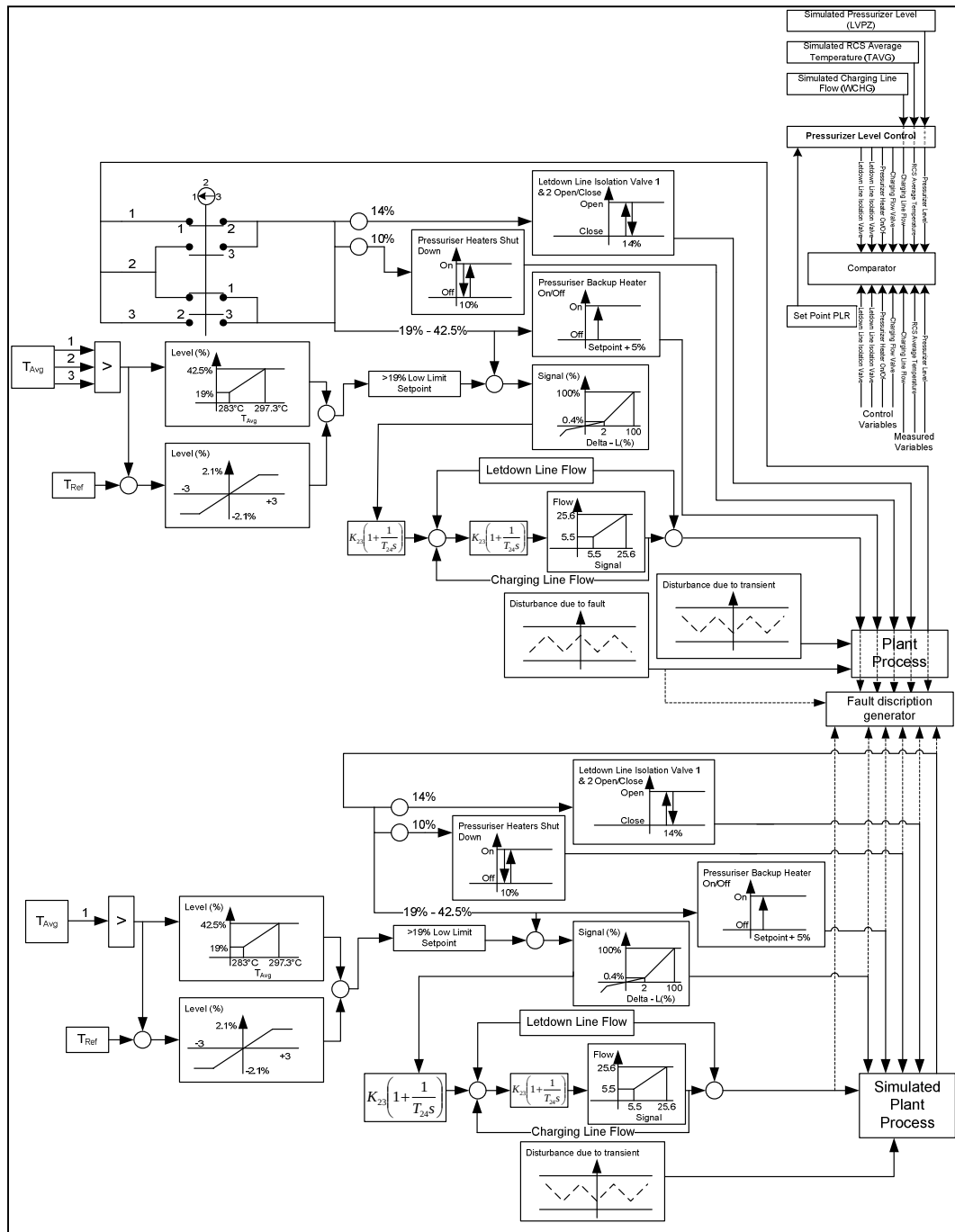


Fig.B-5. Pressuriser level control schematic with PDS

B.4. Pressuriser pressure control PDS

Pressure control measurements of the pressuriser are used, while the pressure is controlled by a proportional heater and back-up heater for low pressure. For high pressure, the pressuriser spray and relief valves are used.

The PDS requires compared control and instrument parameters. The system is depicted in Fig.B-6.

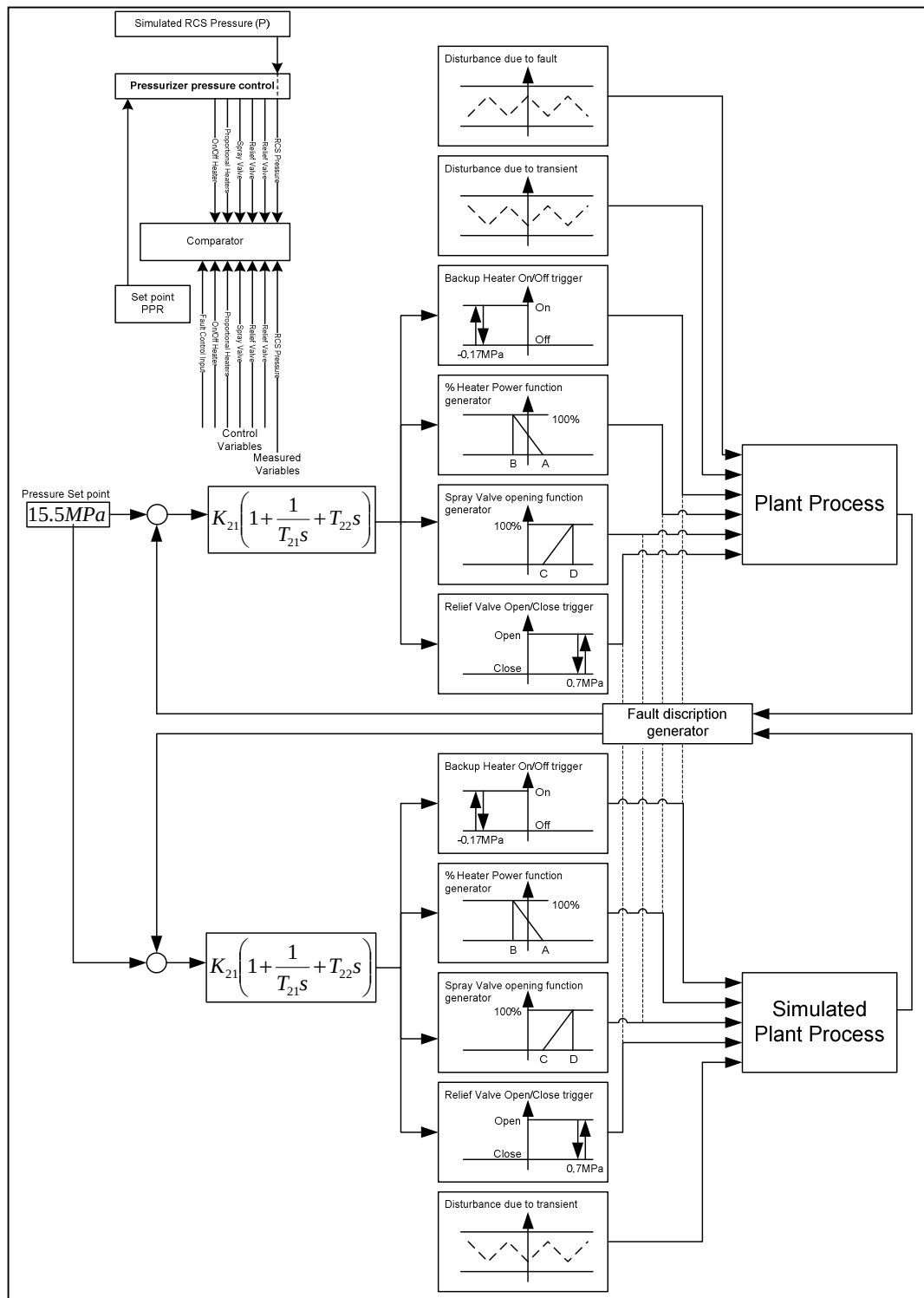


Fig.B-6. Pressure control schematic with PDS

From the measurement instrumentation, the PDS requires:

- RCS average temperature.

From the control system, the PDS receives:

- Spray valve opening,

- relief valve opening,
- proportional heater power level, and
- back-up heater on/off status.

In the case of a fault causing the RCS pressure change to move beyond what is expected, the system will recognise the change in pressure, followed by the reaction of the proportional heater or spray valve operating to increase or decrease the pressure; for larger pressure changes, the back-up heater or pressure relief valves are employed. In many instances, the control system (heaters or valves) will be able to return the RCS pressure to the design pressure. Since the RCS pressure will soon return to normal, the existing protection systems would be unable to detect a fault condition, especially during expected transients such as load following where the pressure changes are expected owing to changing temperatures and coolant flow. The simulator, running in real time with the plant, would be following the same expected transient. It would not be aware of the fault conditions and, so, would not have the heaters or valves react to compensate for the change in pressure owing to the fault, only for the expected transient. The difference between the expected heater power and real heater power, as well as the difference between expected valve openings and real valve openings, result in providing much more information about the plant health than the plant measurements alone.

Fig.B-6 depicts the full control schematic with both the control and instrumentation parameters from the plant and the simulator. The plant and the simulator both include the input disturbances from expected transients. These disturbances would activate the control system to return the measurement parameters to the design value. The plant, however, also includes a fault disturbance that is not included in the simulator. The fault disturbance should be zero during normal plant operation with the plant and the simulator in synchronisation.

B.5. Steam generator control PDS

The steam generator level is controlled by feed water flow and steam flow. The turbine load determines steam flow, so the feed water flow is adjusted accordingly to maintain acceptable steam generator levels. The secondary circuit steam dump system is used to reduce steam pressure during certain transients by releasing steam from upstream of the turbine inlet valves to the condenser or the atmosphere when the condenser is unavailable.

From the measurement instrumentation, the PDS requires:

- SG water level,
- steam flow, and
- water flow.

From the control system, the PDS receives:

- Main feed water valve opening and
 - low flow feed water valve opening
- for level control.

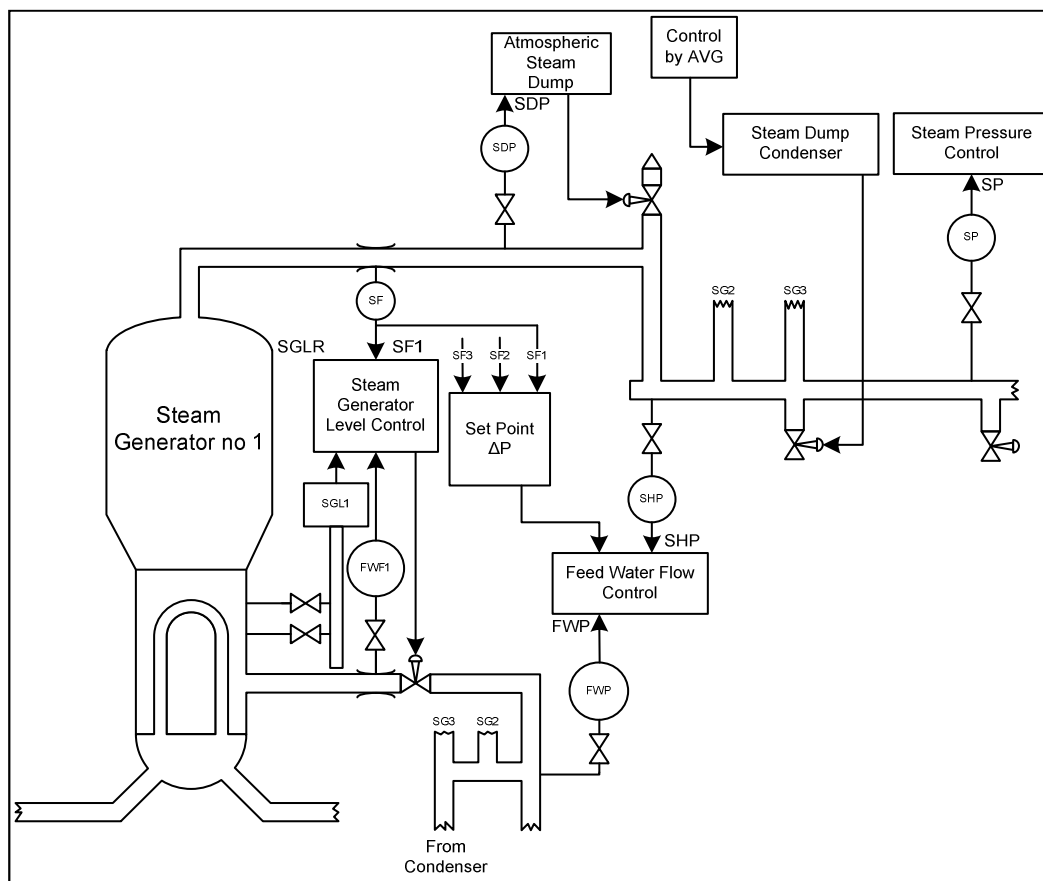


Fig.B-7. Steam generator control

For feed water flow control, the PDS requires:

- Steam pressure,
- feed water pressure, and
- steam flow rate.

From the measurement instrumentation the PDS requires:

- motor pump speed and
 - turbine pump speed
- from the control system.

For steam pressure control, the PDS requires:

- steam pressure

From the measurement instrumentation the PDS requires:

- atmospheric steam dump valve opening and
 - condenser steam dump valve opening
- from the control system.

In the case of a fault causing the SG secondary pressure or level to move beyond what is expected, the system will recognise the change in pressure or level, followed by the reaction of the condenser or atmospheric steam dump control valve to operate to reduce excess steam pressure, since the turbine power is directly controlled by the steam pressure. In the case of a large reduction of steam pressure, the turbine power will be reduced. The SG level is continually maintained by feed water inflow, which will increase as the level drops.

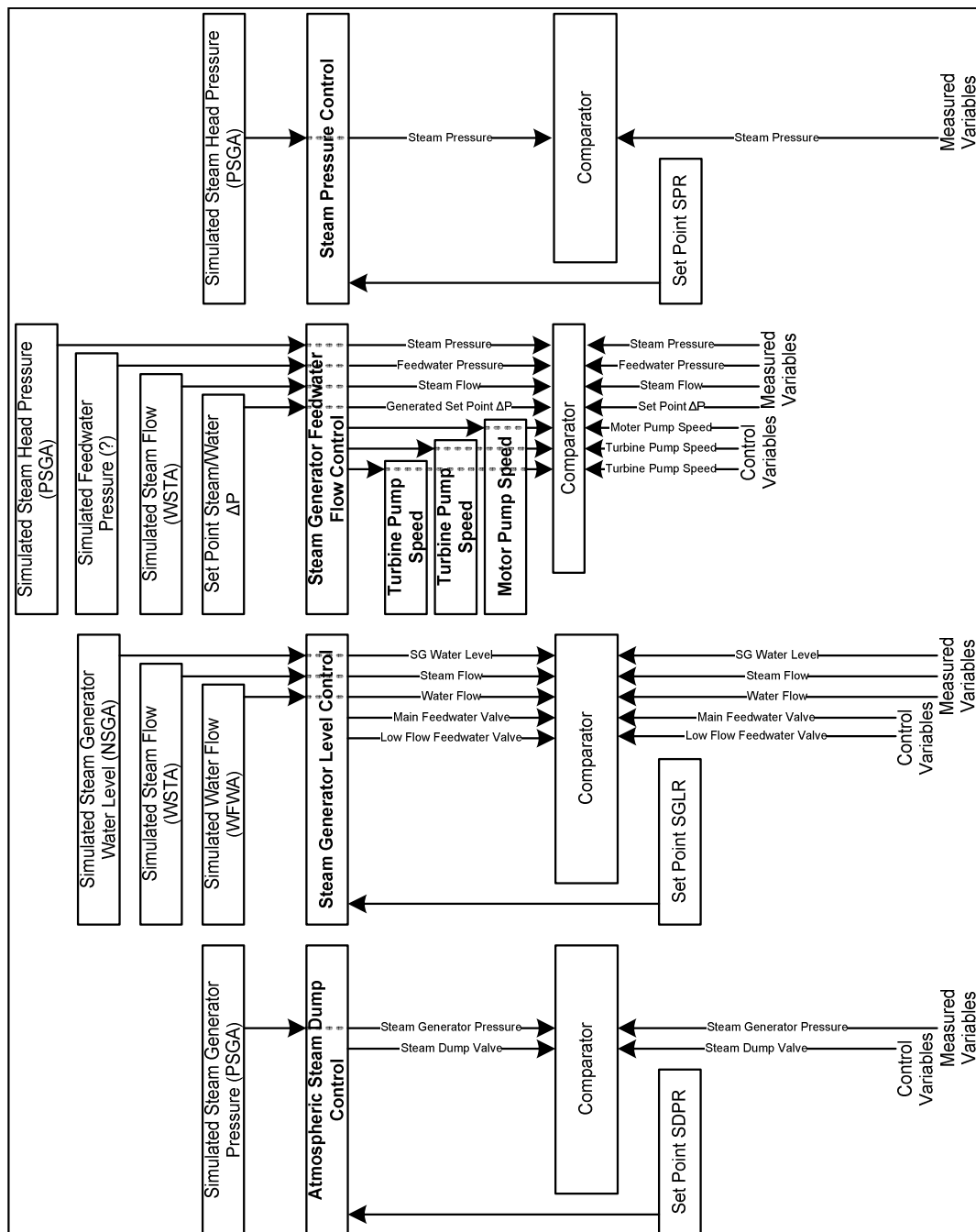


Fig.B-8. Steam generator controls with PDS

Since the SG level is maintained at an acceptable level, the existing protection systems would be unable to detect a fault condition, especially during expected transients such as load following where

the level changes are expected due to changing temperatures, coolant flow, and steam pressure changes. The simulator, running in real time with the plant, would be following the same expected transient, would not be aware of the fault conditions and, so, would not have the increased/decreased flow or valves react to compensate for the change in level or pressure due to the fault, only for the expected transient. The difference between the expected SG feed water inflow, as well as the difference between expected valve openings and real valve openings, results in providing much more information about the plant health than the plant measurements alone.

Fig.B-7 depicts the full control schematic with both the control and instrumentation parameters from the plant and the simulator. The plant and the simulator both include the input disturbances from expected transients. These disturbances would activate the control system to return the measurement parameters to the design value. The plant, however, also includes a fault disturbance that is not included in the simulator. The fault disturbance should be zero during normal plant operation with the plant and the simulator in synchronisation.

B.6. Accounting for inaccuracies and time delays in the system implementation

As described in article 2, the system is robust against small inaccuracies and time delays. Inaccuracies would however reduce the speed at which the system is able to detect faults since the error region around the compared measurements and control operations becomes larger.

As false positives would result in producing doubt in the minds of plant controllers this should be avoided at all cost. For this reason, it is accepted that the PDS should always wait until measurement and simulated difference move beyond the measurement equipment tolerance and simulated measurement error before a certain fault is detected. Both the simulator error and the equipment tolerances should be available to the PDS at all times. During situations where large inaccuracies are present, the conventional plant protection system will detect the fault first and initiate the relevant safety actuation systems.

In order to prevent simulation and measurement noise from jeopardising the system, it is important that the information produced by the simulator should mimic the information received from the plant on all levels including the resolution and rate of quantization of signals.

B.7. Simulator and plant synchronisation

In order to prevent drift of plant measurements and control operations from the simulated equivalent values and since the simulator will always be running, the plant and simulator should be synchronised at certain points in the plant operation. For this reason the simulators' ability to solve a steady-state plant condition is very important. During steady state operation (such as operating at steady power) of the nuclear plant, the operators conduct a plant assessment from time to time to verify the health of the plant. At these points the simulator is set to solve the steady state condition with the plant

parameters and is synchronised with the plant. During steady state, all plant measurements are expected to be stable and so, no accumulation of time-delays can occur.

B.8. Summary and conclusions

This concludes the description of the implementation of the PDS in the primary control systems found in a PWR. With the system continually receiving data on plant measurements as well as control parameters, it becomes simple to calculate what the plant measurements would have been if the control system had not attempted to prevent the fault condition from moving the operating parameters outside the safe operating envelope. In the following chapter, a number of typical faults are simulated and analysed.

C. Appendix

C.1 Additional reference faults

C.1.1. Steam line break inside containment

Steam release due to a rupture of the main steam line could occur inside or outside the containment, since the main steam line passes through the containment. It is expected that an initial increase in steam flow will decrease as steam pressure drops. Since the containment is pressurised at atmospheric pressure, an increase in the containment pressure is expected if the fault occurs inside the containment. When simulating the accident, the size of the break is selected to be small enough for the control system to counter the changes due to the fault, so the fault would normally go undetected by the protection systems inside the reactor.

Tab.C.1. Steam line break configuration

Accident configuration	
Description	Steam line break inside containment
Delay time	100 s
Ramp time	0 s
Failure fraction	5 cm ²
Transient configuration	
Description	Load change
Transient size	100-80%
Transient rate	5% per minute
Event sequence	
Action	Time (s)
PZR proportional heater capacity change	0.0
PZR proportional heater capacity change	21.0
PZR proportional heater capacity change	192.5
PZR back-up heater capacity change	279.0
HPI pump 3 position change	331.0
PZR back-up heater capacity change	554.0
PZR proportional heater capacity change	667.5
PZR spray valve 1 position change	991.5
HPSI start high RB press 1.30 atmospheres	1 313.5
HPI pump 1 position change	1 313.5
HPI pump 2 position change	1 313.5

Letdown valve 1 position change	1 313.5
HPI pump 3 position change	1 313.5
Containment vent valve 1 position change	1 313.5
RBS pump 1 position change	1 313.5
Containment spray starts 1.3 atmospheres	1 313.5
Letdown valve 1 position change	1 314.0
Reactor SCRAM	1 314.5

In Tab.C.1, a trip is shown at time 1314.5s, 1014.5 seconds after the accident occurred. The trip is initiated due to the rise of pressure in the containment, with no indication as to the cause of the accident.

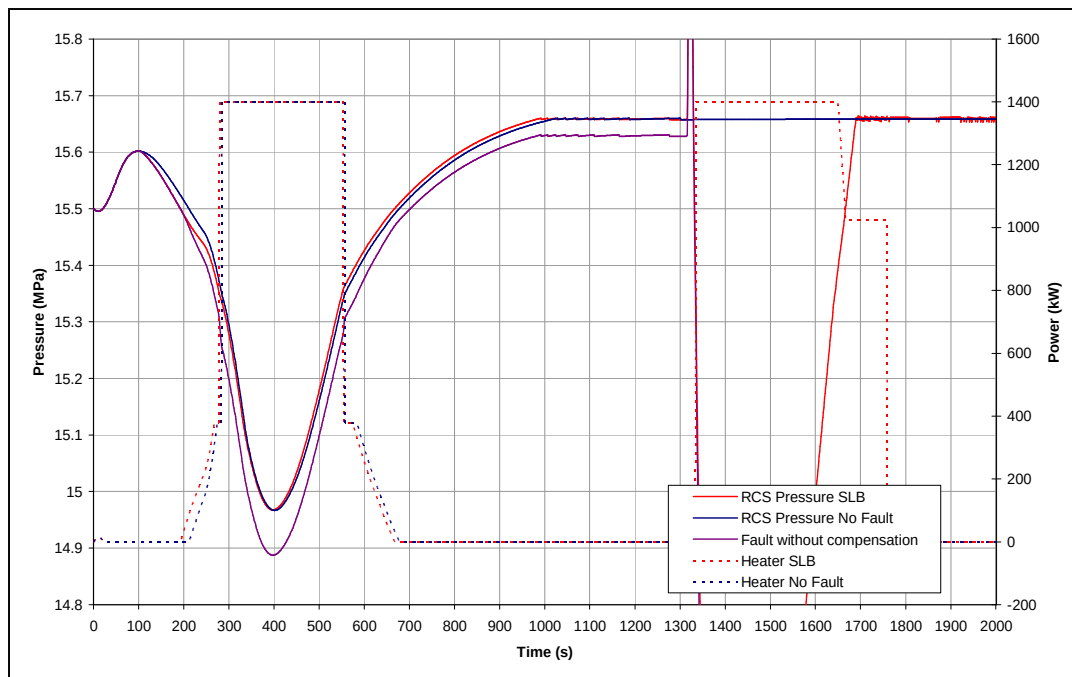


Fig. C-1. RCS pressure and heater operation

The first parameter to be analysed is that of the RCS pressure in Fig. C-1. In the case of a steam line break, the accident is isolated to the secondary coolant loop, and thus, the effect of this on the primary coolant loop is limited to a secondary effect caused by increased or decreased heat exchanger capacity. Nevertheless, a clear drop in pressure that would not occur without a fault present is seen, with the pressuriser heater operating to return the pressure to the expected value. With the compensating heater effect removed, a larger pressure drop is seen, with the pressuriser never returning the pressure to the operating point, with a pressure drop of 30 kPa due to the fault.

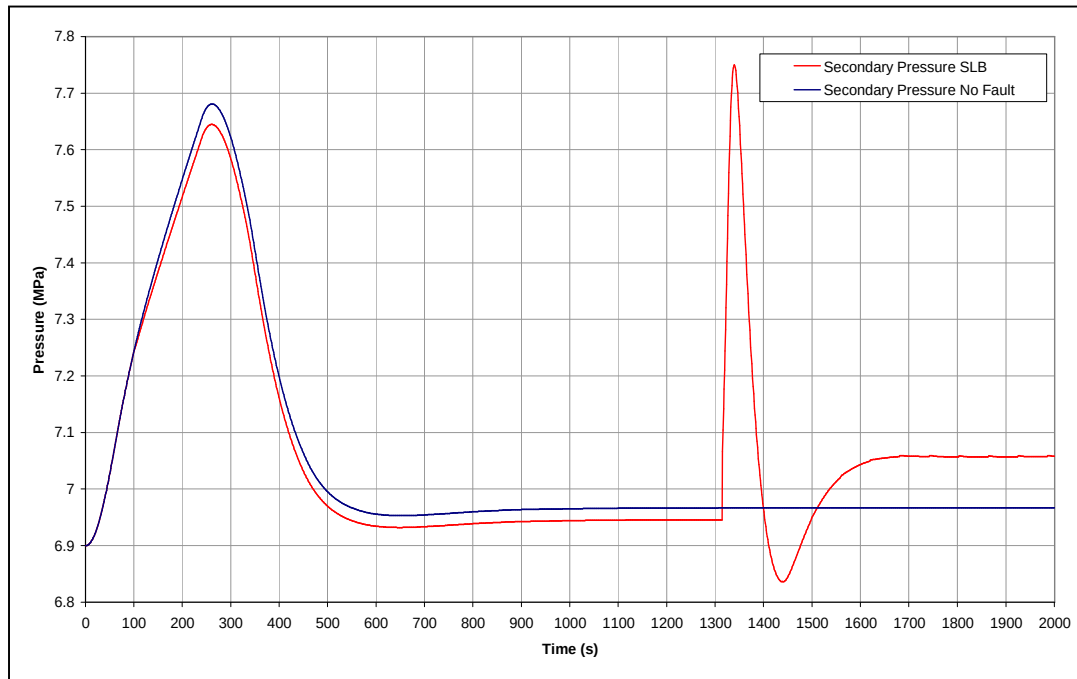


Fig.C-2. Secondary pressure

The pressure in the secondary coolant loop (Fig.C-2) where the fault is situated in this case is not specifically controlled, but usually maintained by the steam generator level with feed water inflow and steam outflow. The analysis still resembles that of other coolant loss accidents, so no indication as to the cause of the fault is evident yet.

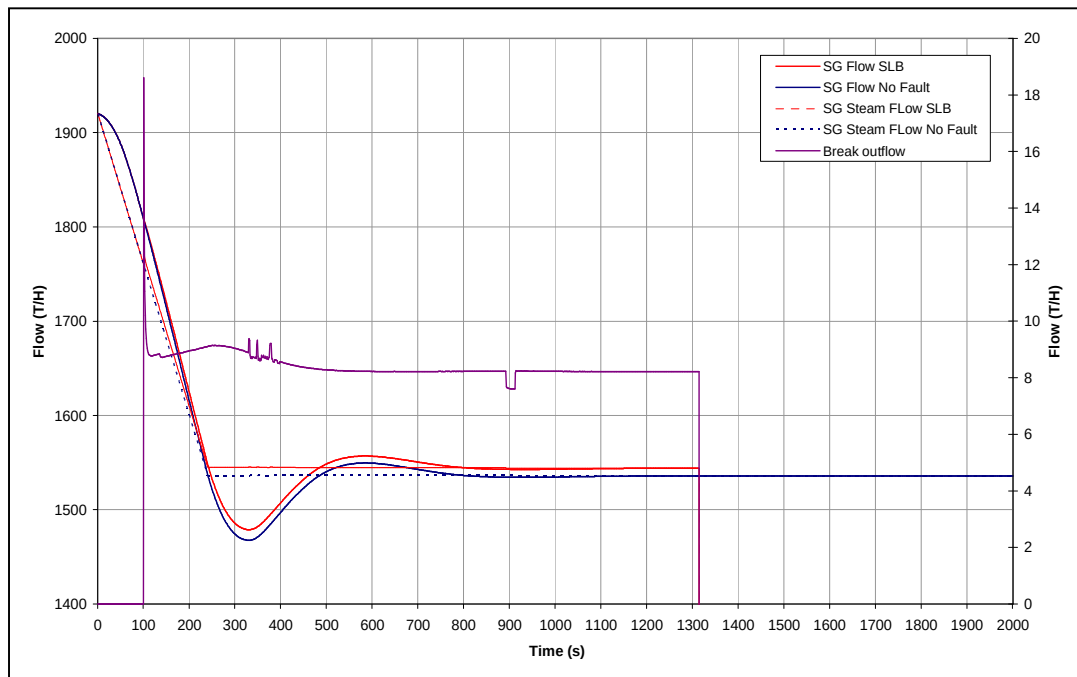


Fig.C-3. Steam generator flow

In the primary coolant system, no drop in coolant levels is evident, which indicates that the cause of drop in pressure should be located in the secondary coolant loop. This appears to be the case, as a drop in SG level is evident in Fig.C-3. An increase in feed water flow into the SG also indicates that the control system is attempting to reduce the effect of the fault. The steam flow exiting the break settles at 8.22 ton per hour.

The SG level drop is almost too small to notice, as the feed water flow makes up for the drop in the level. Using the formulated technique, the compensating effect of the control system can be removed to provide a new SG level, as if the control system only acted on expected transients such as the load change transient.

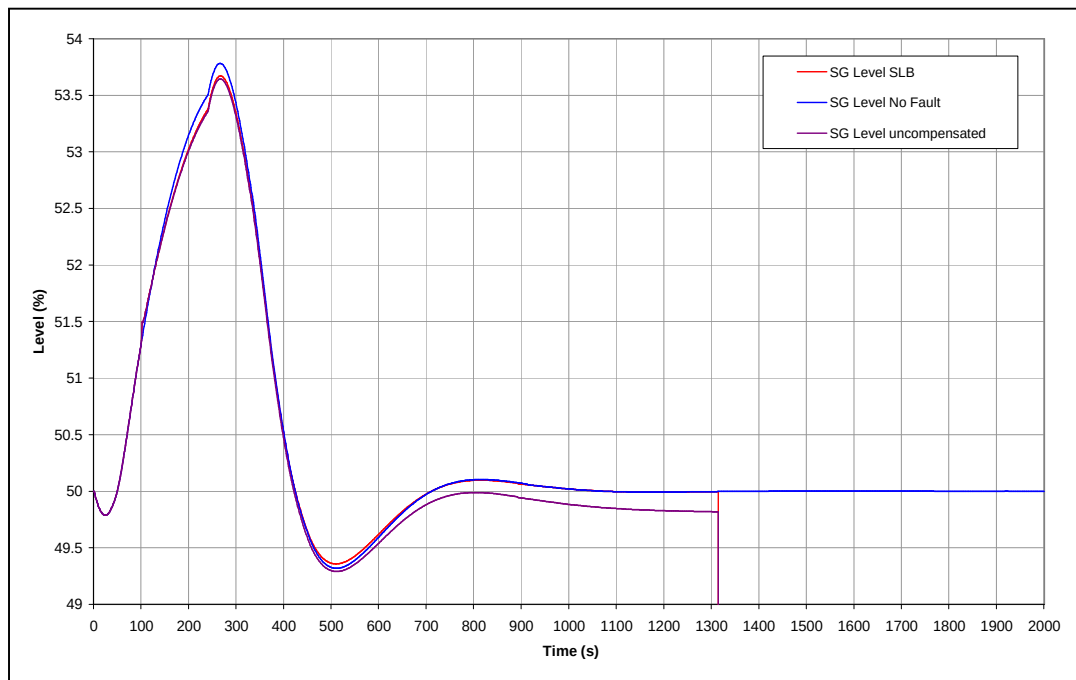


Fig.C-4. Steam generator level

As in previous examples, the flow through the break together with the pressure difference on the inside and the outside of the system allows the calculation of the break size, in this case, 5 cm². It is worth noting that the break is substantially larger for less coolant to leak per hour, since the secondary pressure is substantially lower.

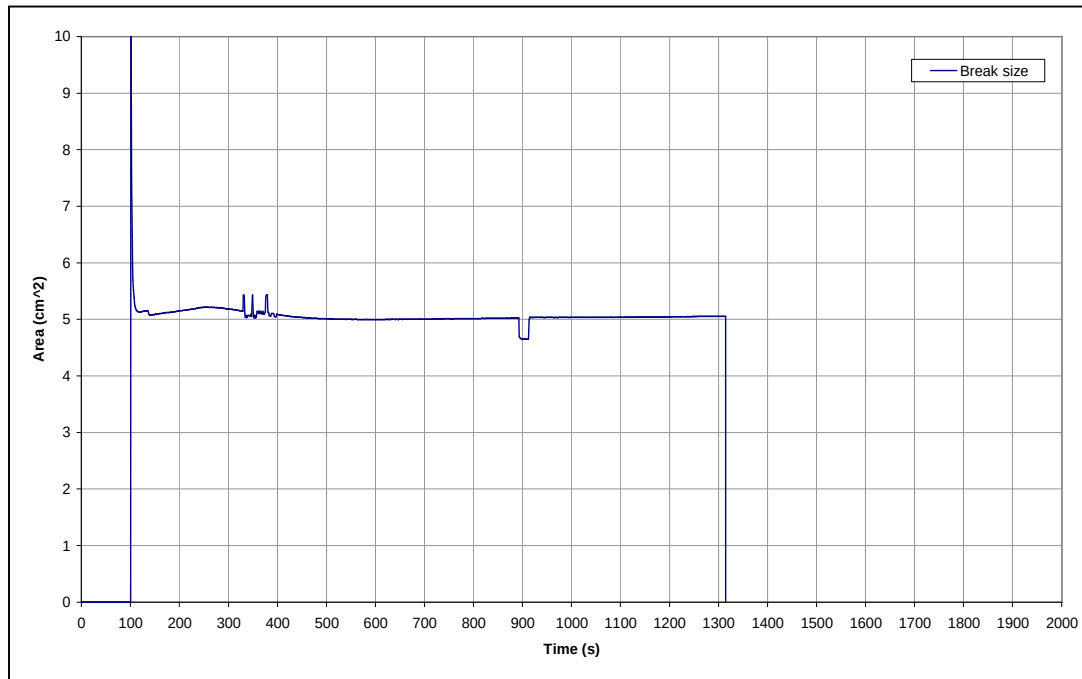


Fig.C-5. Steam line break size

As with the case of the LOCA, the break occurred inside the containment, resulting in a rise in containment pressure, which initiates the SCRAM sequence. This information remains useful, as the complete analysis indicates that a break of 5 cm² occurred on the secondary coolant system inside the containment.

By combining all of these effects, the fault can be derived as a leak and break in the secondary loop (inside containment) from Tab.A.2 as the fault was detected in the following control systems:

- SG Pressure control
 - Measurement: SG pressure drop larger than expected,
 - Measurement: SG pressure lower than expected.
- SG Level control
 - Control: SG makeup flow larger than expected,
 - Measurement: SG level lower than expected.
- Containment pressure monitoring
 - Measurement: Containment pressure larger than maximum allowed pressure.

In Tab.C.2, the PDS results are summarised.

Tab.C.2. Steam line break accident PDS results

Accident results		
	Proposed fault ID system	Existing Protection system
Categorised as	Loss of coolant from secondary coolant loop inside containment	Containment over pressure
Time faulty operation detected	1 015 seconds	1 315 seconds
Time fault categorised	1 015 seconds or earlier	1 315 seconds

Failure fraction 1	8.22 ton per hour	NA
Failure fraction 2	0.5 cm ²	NA

In the following case, the exact same break is simulated, with the break occurring outside the containment. The expected result is the same as this case, with the exception that the plant will receive no indication of the accident, and thus, no SCRAM will be initiated.

C.1.2. Steam line break outside containment

Steam release due to a rupture of the main steam line could occur inside or outside the containment, since the main steam line passes through the containment. An initial increase in steam flow is expected, which will decrease as steam pressure drops. No increase in the containment pressure would be seen if the break is outside the containment. When simulating the accident, the size of the break is selected to be small enough for the control system to counter the changes due to the fault, so the fault would normally go undetected.

Tab.C.3. Steam line break configuration

Accident configuration	
Description	Steam line break outside containment
Delay time	100 s
Ramp time	0 s
Failure fraction	5 cm ²
Transient configuration	
Description	Load change
Transient size	100-80%
Transient rate	5% per minute
Event sequence	
Action	Time (s)
PZR proportional heater capacity change	0.0
PZR proportional heater capacity change	21.0
PZR proportional heater capacity change	192.5
PZR back-up heater capacity change	279.0
HPI pump 3 position change	331.0
PZR back-up heater capacity change	554.0
PZR proportional heater capacity change	667.5
PZR spray valve 1 position change	992.0

In Tab.C.3, no trip takes place, as expected, since no fault can be detected, as the steam is released to the atmosphere.

The first parameter to be analysed is that of the RCS pressure in Fig.C-6. In the case of a steam line break, the accident is isolated to the secondary coolant loop, and so, the effect of this on the primary coolant loop is limited to a secondary effect caused by increased or decreased heat exchanger capacity. Nevertheless, a clear drop in pressure that should not exist without a fault present is seen, and the pressuriser heater is operating to return the pressure to the expected value.

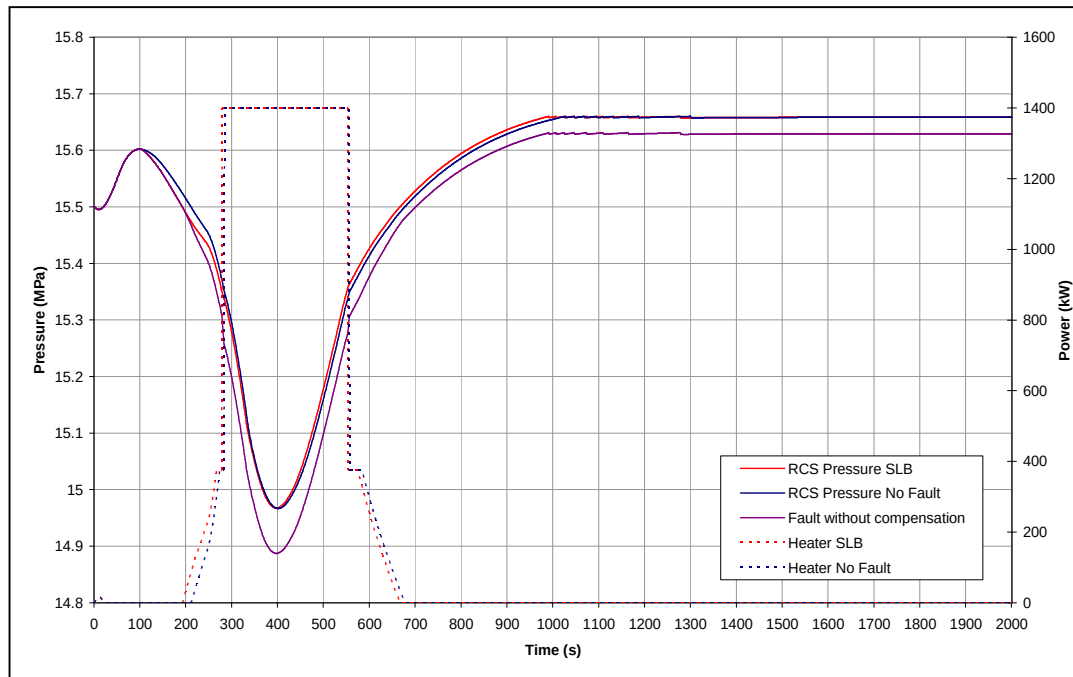


Fig.C-6. RCS pressure and heater operation

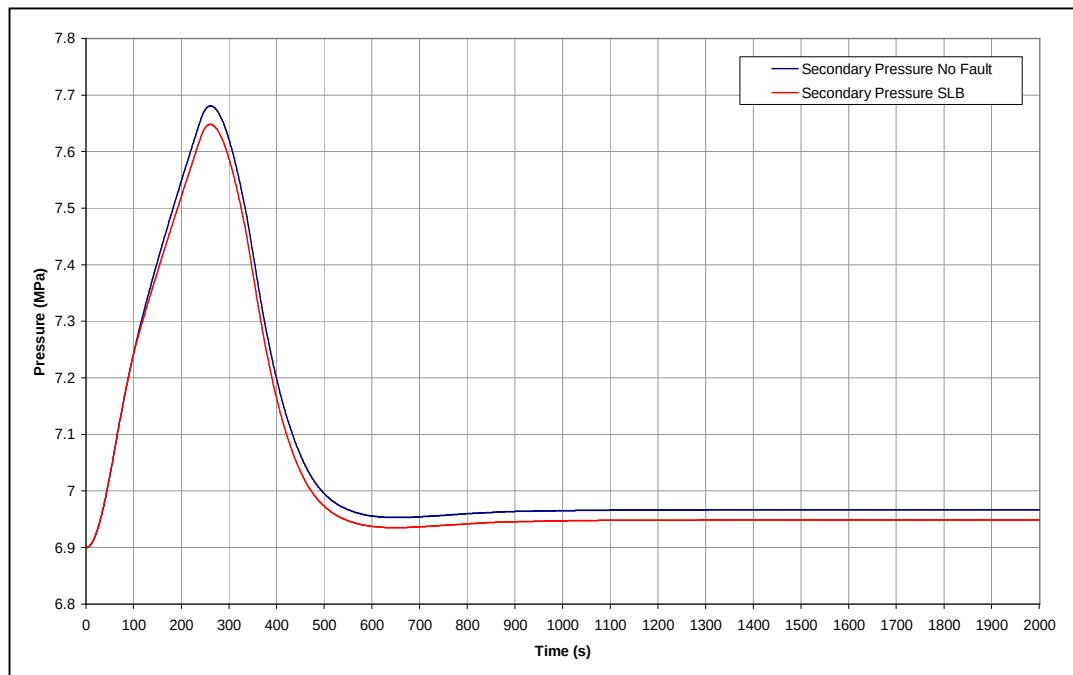


Fig. C-7. Secondary pressure

With the compensating heater effect removed, a larger pressure drop is seen, with the pressuriser never returning the pressure to the operating point, with a pressure drop of 30 kPa due to the fault.

The pressure in the secondary coolant loop where the fault is situated in this case is not specifically controlled, but usually maintained by maintaining the steam generator level with feed water inflow and steam outflow. The analysis still resembles that of other coolant loss accidents, so no indication as to the cause of the fault is evident yet.

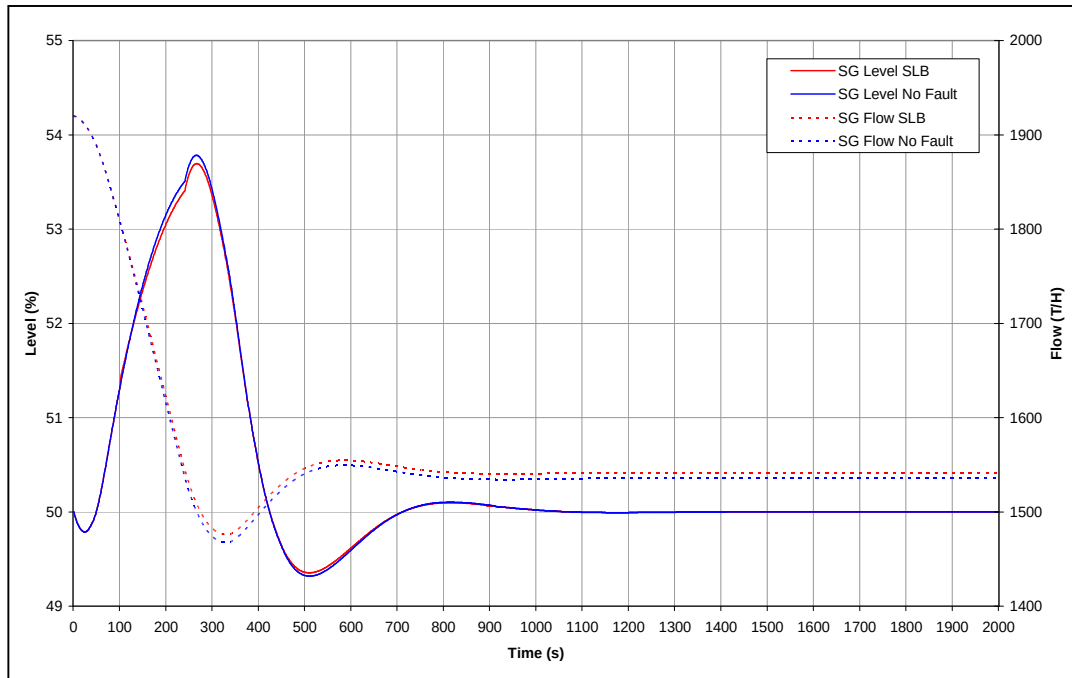


Fig.C-8. Steam generator level and inflow

In the primary coolant system, no drop in coolant levels is evident, which indicates that the cause of drop in pressure should be located in the secondary coolant loop. This appears to be the case, as a drop in SG level is evident from Fig.C-8. An increase in feed water flow into the SG also indicates that the control system is attempting to reduce the effect of the fault.

After analysing the case this far, it is clear that the results of the accident are exactly the same as those of the previous case, with the only exception that the reactor is never SCRAMed, since the containment pressure does not rise. The break size is calculated to be 5 cm² from the flow of 8.22 ton per hour.

By combining all of these effects, the fault can be derived as a leak and break in the secondary loop (outside containment) from Tab.A.2 as the fault was detected in the following control systems:

- SG Pressure control
 - Measurement: SG pressure drop larger than expected,
 - Measurement: SG pressure lower than expected.
- SG Level control
 - Control: SG makeup flow larger than expected,
 - Measurement: SG level lower than expected.

In Tab.C.4, the PDS results are summarised.

Tab.C.4. Steam line break accident PDS results

Accident results		
	Proposed fault ID system	Existing protection system
Categorised as	Loss of coolant from secondary coolant loop outside containment	Not categorised
Time faulty operation detected	1 015 seconds	Not detected
Time fault categorised	1 015 seconds or earlier	Not categorised
Failure fraction 1	8.22 ton per hour	NA
Failure fraction 2	0.5 cm ²	NA