Feasibility of Risk-Informed Regulation for Generation-IV Reactors

By

Craig H. Matos

B.S., Nuclear Engineering (2003)
The Pennsylvania State University

Submitted to the Department of Nuclear Science and Engineering
In Partial Fulfillment of the Requirements for the Degree of

Master of Science in Nuclear Engineering

At the

MASSACHUSETTS INSTITUTE OF TECHNOLOGY
June 2005

Signature of Author ______________________________
Department of Nuclear Science and Engineering
May 20, 2005

Certified by ______________________________
Professor George E. Apostolakis
Department of Nuclear Science and Engineering
Thesis Supervisor

Certified by ______________________________
Professor Emeritus Michael J. Driscoll
Department of Nuclear Science and Engineering
Thesis Reader

Accepted by ______________________________
Associate Professor Jeffery A. Coderre
Chairman, Department Committee on Graduate Studies

(This page intentionally left blank)

Feasibility of Risk-Informed Regulation for Generation-IV Reactors

By

Craig H. Matos

Submitted to the Department of Nuclear Science and Engineering
On May 20, 2005 in Partial Fulfillment of the Requirements for the
Degree of Master of Science in Nuclear Engineering

ABSTRACT

With the advent of new and innovative Generation-IV reactor designs, new regulations must be developed to assure the safety of these plants. In the past a purely deterministic way of developing design basis accidents was prevalent, however this is felt to not be satisfactory, since this leaves insufficient safety restrictions in certain areas, while being overly restrictive in others, not being able to optimize where the safety constraints are truly needed. Currently the USNRC is investigating how one might go about this approach, but no method is finalized. In this paper, a methodology for creating risk-informed design basis accidents is developed. This not only incorporates the Surrogate Risk Guidelines developed by the USNRC for each overall accident initiator the plant may experience, but helps to select which sequences are the most important to that initiator, and from that develop a set of risk-informed assumptions that form the basis of the design basis accident. This method was applied to the test case of the Massachusetts Institute of Technology's Gas-Fast Reactor (GFR) design, as considerable risk-informed design work has been carried out on various initiators for this design (including Turbine Trip, Loss-of-Coolant Accident, and Loss-of-Offsite Power). The turbine trip was chosen for extensive investigation. It was found that the CDF of this event for the GFR (7.098E-6 / RY) did not pass the overall NRC Surrogate Risk Guideline (1E-6 / RY). The method identified the dominating sequence, which was dominated itself by the failure of the passive shutdown cooling system for the GFR design. It was determined that the designers could in fact develop a risk-informed DBA by developing a set of assumptions to ensure success in the Passive SCS. This process showed how risk-informed DBAs could be developed for various new reactor designs.

Thesis Supervisor: George E. Apostolakis
Title: Professor of Nuclear Engineering

(This page intentionally left blank)

Acknowledgments

I would like to thank my advisor, Professor George Apostolakis, for all that he has taught me for the years I have been here. I want to thank him for his patience and time in teaching me to be a better student, engineer, and person. I would also like to thank my thesis reader, Professor Michael Driscoll, for the guidance he has given me on the GFR project and all the insights he has shown me through my years of research. I would like to thank Michael Delaney for helping me to begin my research and showing me what it was like to be an excellent student and research assistant.

This work was supported by the US Nuclear Regulatory Commission under a cooperative agreement with the MIT Department of Nuclear Science and Engineering and by the US Department of Energy (DOE) under a Nuclear Energy Research Initiative. I would like to thank the USNRC, USDOE, and the MIT Department of Nuclear Science and Engineering for all their support. The views presented here are those of the author and do not necessarily represent the views of the USNRC or USDOE.

I wish to thank my parents for being my biggest fans and for their love and support. I would also like to thank my sister and my brother who have been there for me when I needed them the most. Lastly, to my friends , who have shown me how to have fun and helped me realized how to keep a balanced life. I wish I could list you all, but that would take up a lot of space, so I just want to thank everyone important in my life for putting up with me through not only my time doing research, but all the other times as well.

(This page intentionally left blank)

Table of Contents

LIST OF FIGURES

(This page intentionally left blank)

LIST OF TABLES

(This page intentionally left blank)

Nomenclature

10CFR50	Code of Federal Regulations, Title 10, Part 50
AC	Alternating Current
ACRS	Advisory Committee on Reactor Safeguards
ATWS	Anticipated Transient without Scram
CCF	Common Cause Failure
CCDP	Conditional Core Damage Probability
CDF	Core Damage Frequency
CV	Check-Valve
CP	Check-Valve (when the coolant is flowing under passive, i.e., natural convection, flow)
DC	Direct Current
DOE	Department of Energy
ECCS	Emergency Core Cooling System
GDC	General Design Criteria
GFR	Gas-Cooled Fast Reactor (GCFR in older literature)
LERF	Large Early Release Frequency
LOCA	Loss of Coolant Accident
LOOP	Loss of Offsite Power
LOSP	Loss of Station Power
LWR	Light Water Reactor
NEI	Nuclear Energy Institute
NRC	Nuclear Regulatory Commission

PRA	Probabilistic Risk Assessment
RAW	Risk Achievement Worth
RIR	Risk Increase Ratio
RY	Reactor Year
RSS	Reactor Shutdown System
SCS	Shutdown Cooling System
SFC	Single Failure Criterion
SRP	Standard Review Plan for the Review of Safety Analysis Reports for Nuclear Power Plants
USNRC	United States Nuclear Regulatory Commission

(This page intentionally left blank)

I Introduction

In recent years, the nuclear industry has moved forward with new reactor designs. This has a been an effort seen throughout the world, and more recently the United States Department of Energy (US DOE) has taken it upon itself to push for these innovative designs, in what are called Generation-IV reactors. According to the DOE: “concerns over energy resource availability, climate change, air quality, and energy security suggest an important role for nuclear power in future energy supplies”. The DOE suggests that “while the current Generation II and III nuclear power plant designs provide an economically, technically, and publicly acceptable electricity supply in many markets, further advances in nuclear energy system design can broaden the opportunities for the use of nuclear energy” (US Department of Energy, 2002b).

Much of the industry has begun focusing on risk-informed design processes. This is a process that allows the designer to evaluate the design as it is being built. This usually occurs through the use of surrogate risk guidelines (such as core damage frequency (CDF) and large release frequency (LRF)) for safety criteria, as well as consideration for other concerns, such as sustainability and economics. Through probabilistic risk assessment (PRA), the designer can assure higher levels of safety for the plant, while still making the plant cost effective. One no longer needs to wait for a design’s completion to find out that it is not an acceptable one and must be modified.

With a move of the designers to a risk-guided system of design, the regulators have also taken the same approach. This is expressed by the NRC when they say: “a risk-informed regulatory structure that can be applied to license and regulate advanced (future) reactors, regardless of their technology, could enhance the effectiveness, efficiency, and predictability (i.e., stability) of new plant licensing" (USNRC, 2004). The need for the new form of regulation also deals with the lack of knowledge about these new designs. In the past, design-basis accidents were developed deterministically. At the time, there was no experience with light-water reactors to draw insights from. Over the last 30 years, due to experience gained from dealing with light water reactors and insights gained from risk-assessments done on the reactors, the set of DBAs has been modified. However, due to the limited applicability of historic light-water DBAs to future reactors, new methodologies must be used to form DBAs. As we have seen with light-water reactors, risk-analysis of reactors has shown us insights into where safety constraints are needed. This would help better determine where regulations should be placed and why as suggested here, a risk-informed method for developing DBAs for Generation-IV reactors would be beneficial to the industry.

Probabilistic risk analyses done on current LWR regulations have given the industry insights into how safety constraints should be reorganized. Certain areas were too conservative and rules needed to be relaxed (as currently evident in changes in the ECCS rule 50.46), while for other aspects certain needed safety constraints were missing (as shown in the development of the interfacing system LOCA, anticipated transient without SCRAM, and station blackout rules). This is why it has been felt that a risk-informed approach will be the key to having an acceptable level of safety for all Generation-IV reactors.

It is suggested that if a "technology-neutral framework" is developed for all generation-IV reactors it would lead to a more straight-forward way to develop a complete set of regulations for each reactor design, ensuring safety of the plant, workers and the public. It is recommended that a method for the development of a set of risk-informed regulations would help both the designers in knowing what expectations are required and not placing undue burden on them, the regulators in giving them an easy and straight-forward framework to deal with, and the public, by ensuring an envelope of safety that will account for all possible damaging accidents that could affect their health.

(This page intentionally left blank)

II Current Methodologies

II A Methods for DBAs

The foundation of current regulations is a set of Design Basis Accidents. A Design Basis Accident is a postulated accident that a nuclear facility "must withstand without loss of components, systems, and structures" (U.S. Code of Federal Regulations, 2004). They are a set of stylized accidents that are used as a bounding envelope for all other plant accidents. The boundary is set by the consequences of these accidents (i.e., the damage that they can do to the plant). They are more formally explained as "the postulated failure of one or more important systems and an analysis based on conservative assumptions" (Okrent, 1981). They are based on the General Design Criteria (GDC) as described in Appendix A of 10 CFR 50. The GDCs are defined by the NRC to "establish minimum requirements for the principal design criteria for water-cooled nuclear power plants similar in design and location to plants for which construction permits have been issued by the Commission" (U.S. Code of Federal Regulations, 2004).

The design basis accidents are all consistent with the structuralist defense-in-depth approach, which "asserts that defense in depth is embodied in the structure of the regulations and in the design of the facilities built to comply with those regulations" (Sorensen et al, 1999). The structuralist approach is a deterministic method of looking to see how one can place precautions into a system, just in case a current barrier or safety feature fails. In current DBA regulation (from Title 10 of the federal code of regulations), these precautions are in the form of conditions that meet the high level goals of "preventing accident initiators, terminating accident sequences quickly, and mitigating accidents that are not successfully terminated" (Sorenson et al, 1999). Certain requirements must be in place for the safety of all reactors, such as "reactor containment and emergency planning". This structuralist model is how current nuclear plants are regulated (Sorensen et al, 1999).

The DBAs only deal with "credible" accidents and do not deal with more severe accidents that are considered "beyond-design-basis" (U.S. Code of Federal Regulations, 2004). The accidents were originally determined by a panel of knowledgeable experts, who used ASME codes along with their own knowledge in the field (Okrent, 1981).

Currently, DBAs are separated into 9 categories: overcooling, undercooling, overfilling, loss of flow, loss of coolant, reactivity, anticipated transient without scram (ATWS), spent-fuel and waste system, and all remaining external events (ones which do not fall into any of the first 8 categories) fall into the final category (Okrent, 1981). For each DBA, given a set of assumptions, the plant must be able to stop/mitigate these accidents (i.e., bring the plant to cold shutdown). This is the deterministic basis upon which regulations for all nuclear reactors in the United States are currently determined by the NRC.

Design Basis Accidents provide a confidence level to the user, because they use a structuralist form of defense-in-depth (placing barriers to provide extra protection for the plant) to account for areas with non-quantified uncertainties in the plant's safety. This is an easy way for the regulatory staff to determine if a plant has met the regulatory requirements, because it is a list of requirements that one can check off if they have been met or not. However, problems may occur because, at times, DBAs can be overly conservative in some areas, and yet do not have enough safety constraints in other areas. Since there is a large amount of non-quantified uncertainty, the DBAs may overlook some needed safety requirement and overcompensate by adding unnecessary ones.

As stressed early, using a purely structuralist methodology, where safety barriers are added to account for a lack of confidence, does not seem to be a rational way to approach devising regulations for nuclear plants. It may not only introduce over-conservatism in areas where certain rules may not apply (such as the single-failure criterion not being needed for all accidents), but may also fall short when safety constraints are missed. The shortcomings of a purely deterministic methodology were shown in "Reactor Safety Study: An Assessment of Accident Risks in U.S. Commercial Nuclear Power Plants" (WASH-1400). This report showed that small LOCAs and transients were dominant risk contributors to plant systems, as opposed to previous deterministic thought of only looking at very large pipe breaks in the reactor coolant system. The importance of support systems and the significance of operator errors were also shown in WASH-1400 (Beckjord et al, 1993). The findings of the study and subsequent risk-analysis have helped the industry to change its view on the dominant accidents in a plant and allowed the industry to see what may have been missed in a purely deterministic setting. These were DBAs that were added due to findings in probabilistic risk assessment (PRA) research that showed these were areas where more safety constraints were required. By looking at the regulations from a purely structuralist point of view, one may not be able to encapsulate the real reason that the DBAs were originally created. By examining the similarities and differences between a purely deterministic methodology and a risk-informed regulations discussed in the next section, the advantages and disadvantages of the two can be clarified and proposals made on how to construct a more effective set of regulations.

II B Risk-Informed Regulations

PRA is used to identify the various accidents that may occur in a system, their consequences, and their likelihood of occurring. Uncertainty is quantified and placed into the overall scheme of the design project. Risk-informed regulation attempts to encompass the original intentions of the DBAs, to create a standard set of guidelines that will shows a reactor system can be safely built and operated. By using risk-information, the methodology creates a set of regulations that are used as an envelope to account for the worst possible, "reasonable" accidents. Through various tools, one tries to model a system to find what safety constraints are needed so that the system falls under the acceptable level of risk as defined by the stakeholders. PRA is one of these tools that will be used in the end by the stakeholders. The Stakeholders are those who have an interest in a particular decision, either as individuals or representatives of a group. This includes people who influence a decision, or *can* influence it, as well as those affected by it. A final deliberative process (which is a "back and forth" discussion between all stakeholders to help the decision maker determine the best course of action to take), is used to help the NRC staff decide what regulations are truly needed. The stakeholders will prioritize the risk factors to their own needs (where in regulation this usually involves putting safety of the workers and public as the number one priority).

The risk information taken from probabilistic risk assessment is able to provide a way of seeing, in a rationalist light (applying safety constraints where needed based on probabilistic data), where design basis accidents may need to have safety constraints focused (i.e., where these constraints need to be applied or lifted). A rationalist model for risk assessment is one where "defense in depth is the aggregate of provisions made to compensate for uncertainty and incompleteness in our knowledge of accident initiation and progression" (Sorensen et al, 1999).

The quantification of risk and the estimation of uncertainty through PRA is how this rationalist methodology has been developed. The rationalist method establish acceptance criteria (quantitatively), analyzes the plant using PRA to make sure the acceptance criteria are met, looks at the uncertainties in the analysis (including those dealing with model (incompleteness), and finally decides how to balance the uncertainties (Sorensen et al, 1999). The rationalist defense-in-depth model seeks to enhance the confidence one has in their risk-assessment model and other analysis. This model tries to decrease the probability of plant accidents and the provisions to do such become the rationalist methods defense-in-depth (Sorensen et al, 1999). This defense-in-depth can be found in the acceptance criteria. The quantification of acceptance criteria and formal analysis of the system (including uncertainty analysis) is where the rationalist model differs from the structuralist model. Unlike the structuralist method, the rationalist way of thinking only uses engineering judgment after all other "capabilities of the analyses have been exhausted" (Sorensen et al, 1999).

As discussed earlier, through the use of risk-assessment, one can see where safety constraints should be added. Historically, we have seen this applied with the creation of the station blackout and ATWS rules which were made to ensure plant safety (Apostolakis et al, 2001). Currently, the focus seems to be on lifting unnecessary constraints in areas where certain requirements are overly conservative or unneeded. Opponents of risk-informed regulations focus primarily on the removal of requirements. These opponents think that risk-informed regulations are only a way for the industry to ease the burden of regulations. This viewpoint is due in part because of the large gap in time between the point at which extra constraints were added (i.e., the examples of the ATWS and station blackout rules) and the current focus on removing unnecessary constraints. Both initiatives are used to focus the regulations around the safety significant areas of the plant, yet one may not see the big picture if they do not step back and look at the whole history of risk-informed regulations and PRA.

However, due to the lack of defined terminology, along with other mechanistic (deterministic) requirements such as clad temperature, oxidation, etc..., it is not possible to have a fully risk-based regulatory system. It also seems that the regulators, at this point in time and with the current mindset, may be scared to have a fully risk-based system. This is due to the fact that they do not know how to operate confidently in risk-space (which may again come from the fact that there are poorly defined standards and definitions). It may take some time, but hopefully if the need for a risk-informed system grows, we may, as an industry, be comfortable enough with risk-information to develop a set of fully risk-based regulations.

II C Insights from Current Methods

The difference between the two methodologies seems to be the inclusion of uncertainty measures (PRA methodology) versus a structuralist defense in depth methodology of adding margins/barriers to account for the lack of quantified uncertainty (DBA methodology). In a purely structuralist design basis accident approach, when one perceives a lack of safety, one is tempted to use a structuralist methodology to introduce multiple barriers and constraints "just in case". Ideally, one should instead, logically find where safety is needed and apply extra precautions to only those safety significant areas. Using the DBA methodology solely in a structuralist light, one can become overly conservative and apply extra, unneeded constraints, which can hinder the project both by adding barriers where they are not needed and also not addressing areas which may require more safety constraints. This has been shown, as discussed earlier, throughout the history of PRA.

From what has been discussed, along with current risk-informed activities on both the regulatory and industry sides, risk-informed regulations will be shown not only to be needed, and also how they can be feasibly developed. Probabilistic risk assessment, in the right hands can be a very powerful tool. If this tool is used to re-sculpt the design basis accidents into a more effective form, yet still keep the overall foundations that were their original basis, the industry will be able to move forward with greater confidence. PRA methods are a way to determine if a failure (and its subsequent failures) is a "reasonable" occurrence. Using this tool, we can build the envelope envisioned in the original intent of the DBAs. These accidents still remain the bounding cases, yet now the reason they were chosen is more justifiable and the uncertainty for these scenarios can now be quantified and measured against. However, structuralist Defense-in-Depth concepts can also be integrated into a risk-informed structure. This acts as conservatism built directly into the DBA to protect against unknowns (that may not even be accounted for when analyzing uncertainty). This level of structuralist conservatism that is applied accounts for the unknowns not covered in the purely risk-based methodology. Thus, by using a risk-informed methodology that combines a purely risk-based and a purely structuralist approach, would give the industry a more complete amalgam to use in regulations. This added level of completeness in the industry's main concern in creating a regulatory structure. Using risk-information in the regulatory process, one would be able to focus the regulations more effectively on the areas where safety constraints are truly needed.

(This page intentionally left blank)

III Current Activities

III A NRC Work

The NRC is developing a technology neutral framework for new plant licensing. The NRC plans to first propose a set of guidelines and criteria for all reactors. The framework will be technology-neutral with the hope of then creating and implementing technology specific guidelines for new reactors. Thus a set of regulatory requirements will be developed from these first two tasks. The NRC is combining protective strategies developed from safety fundamentals to produce regulations that provide more confidence in a plant's safe operation. This new framework will employ defense-in-depth principles to develop the new regulatory requirements. Once technology neutral regulations have been finalized, the NRC will propose a technology-specific framework to use along with the technology-neutral regulations, to form these technology-specific regulations, as shown in figure III-1 (USNRC, 2004).

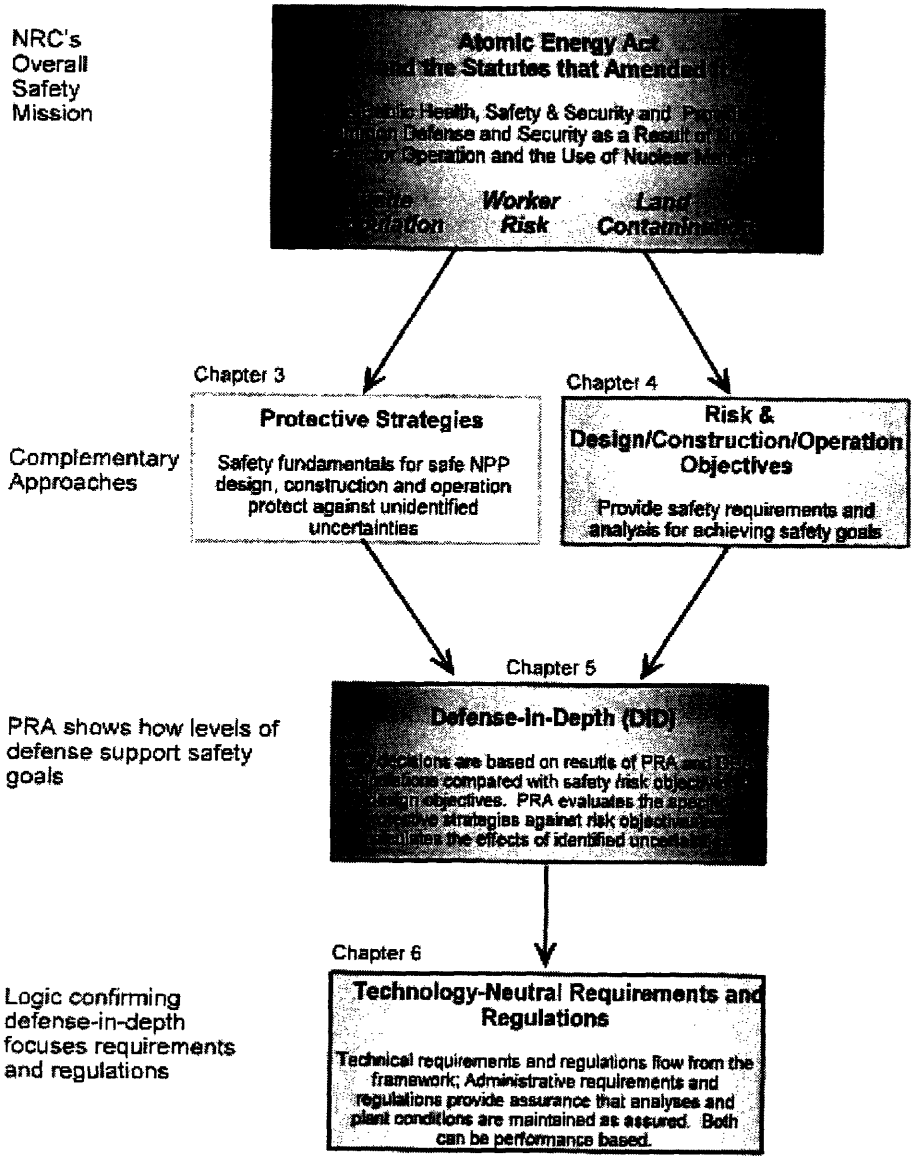

NRC's Overall Safety Mission
Atomic Energy Act
and the Statutes that Amended It
Public Health, Safety & Security and Protection
Common Defense and Security as a Result of
Reactor Operation and the Use of Nuclear Material
Site Radiation
Worker Risk
Land Contamination
Chapter 3
Protective Strategies
Safety fundamentals for safe NPP design, construction and operation protect against unidentified uncertainties
Chapter 4
Risk & Design/Construction/Operation Objectives
Provide safety requirements and analysis for achieving safety goals
Complementary Approaches
Chapter 5
Defense-in-Depth (DID)
Decisions are based on results of PRA and DID
evaluations compared with safety risk objectives and
design objectives. PRA evaluates the specific
protective strategies against risk objectives and
calculates the effects of identified uncertainties
PRA shows how levels of defense support safety goals
Chapter 6
Technology-Neutral Requirements and Regulations
Technical requirements and regulations flow from the framework; Administrative requirements and regulations provide assurance that analyses and plant conditions are maintained as assured. Both can be performance based.
Logic confirming defense-in-depth focuses requirements and regulations

Figure III-2 NRC Technology-Neutral Framework (USNRC, 2004)

The overall protection requirements, intended to protect the public/worker health and safety are in the form of dose limits. From ALARA, the public's dose limit is proposed to be 100 mrem/year. Risk limits for accidental exposure are also given and ranges of dose are based on the frequency of occurrence. Based on these ranges, the NRC has created a "Frequency-Consequence Curve" (in rem per reactor-year as shown in figure III-3).

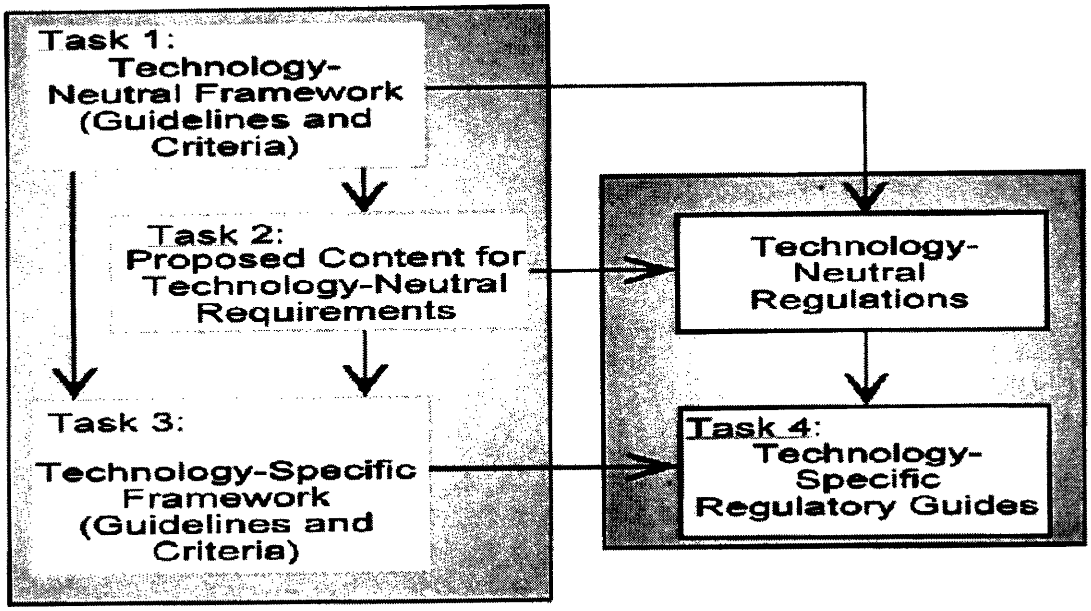

Task 1:
Technology-Neutral Framework (Guidelines and Criteria)
Task 2:
Proposed Content for Technology-Neutral Requirements
Task 3:
Technology-Specific Framework (Guidelines and Criteria)
Technology-Neutral Regulations
Task 4:
Technology-Specific Regulatory Guides

Figure III-1 Framework for a Regulatory Structure for New Plant Licensing (USNRC, 2004)

The NRC thinks that the current regulatory methods can be improved and ones that employed both engineering judgment and Probabilistic Risk Assessment (PRA) would give the regulators more confidence in a reactors safety. As a safety net to what might still be unknown after PRA would be accounted for in the defense-in-depth (DID) approach (using deterministic analysis). They intend to use four protective strategies: barrier integrity, limiting the frequency of initiating event, employing safety systems for accident prevention and mitigation, and accident management programs. These all contribute to defense-in-depth. After employing these strategies, a top-down methodology would be used to develop the requirements for new reactor design, construction and operation (USNRC, 2004). This framework structure is shown in figure III-2.

sum of all sequences which have the same initiator) for the large early release frequency. For both given SROs, mean values are used (USNRC, 2004). Table III-1 lists these SROs.

Table III-1 Surrogate Risk Objectives (USNRC, 2004)

	(1) Prevention-Mitigation Assessment: Consider the Strategies in Pairs			
	Prevent		**Mitigate**	
	Core Damage Frequency $\le 10^{-4}$/year		Conditional Probability of Early Containment Failure** $\le 10^{-1}$	
	(2) Initiator-Defense Assessment: Consider the Strategies Individually (Preferred)			
	Limit the Frequency of Accident Initiating Events (Initiators)	Limit the Probability of Core Damage Given Accident Initiation	Limit Radionuclide Release During Core Damage Accidents	Limit Public Health Effects Due to Core Damage Accidents
	Initiator Frequency	Conditional Core Damage Probability	Conditional Early Containment Failure Probability**	Conditional Individual Fatality Probability
Anticipated Initiators	≤ 1/year	$\le 10^{-4}$	$\le 10^{-1}$	*
Infrequent Initiators	$\le 10^{-2}$/year	$\le 10^{-2}$	$\le 10^{-1}$	*
Rare Initiators	$\le 10^{-6}$/year	≤ 1	≤ 1	*

Notes:

The product across each row gives LERF < 10^{-5}/year. Responding systems and procedures are not designed for rare events. When applying the quantitative guidelines in this figure, in general, no individual sequence should contribute more than 10% of the value listed.

* No quantitative guideline propose, using LERF as a surrogate.

** This strategy does not imply that risks associated with late containment failure can or will be ignored. Potential causes of late containment failure and associated mechanisms for radionuclide removal prior to containment failure will be considered. A quantitative guideline of ≤ 0.1 is proposed for the probability of a late large release given a core damage accident

Design objectives were investigated by looking at event selection. To have an adequate safety envelope for accidents, initiating events were broken into 3 categories: Anticipated initiators (< 1/ry), Infrequent initiators (< 10^{-2}/ry but >10^{-6}/ry), and Rare initiators (< 10^{-6}/ry). These are all mean values. Any events occurring less frequently than 10^{-6}/ry are not considered. These categories are used to ensure that for frequent events, criteria for lower consequences are

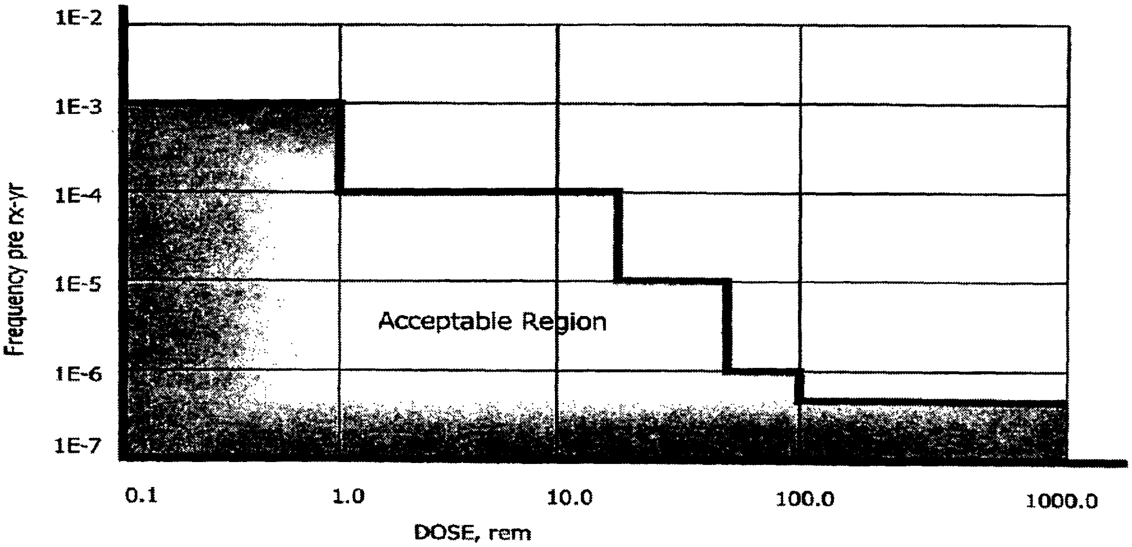


Figure III-3 Frequency Consequence Curve (USNRC, 2004)

The frequency-consequence space is divided into an acceptable and unacceptable region. This allows the regulators to apply comparable dose limits to accidents based on the frequency of an accident or initiator of that type occurring (USNRC, 2004).

To implement the frequency-consequence curve, surrogate risk objectives (SRO) are being created. These SROs are based on the previously developed Quantitative Health Objectives (QHOs), which were used as a basis for risk-informed accident criteria. These are used as both accident protection and accident mitigation criteria. The latent fatality QHO had been 2E-6 per year, which led to a proposed SRO of 1E-5 per reactor year for the sum of all sequences which have the same initiator (which is 10% of the total CDF value for the entire plant, which is 1E-4, as shown in table III-1). Even though these are what the NRC is proposing, they claim that the applicant can propose an alternate criterion, if they can take advantage of other plant specific characteristics. The mitigation criterion is based on the early fatality QHO of 5E-7 per reactor year. The NRC used this to propose a SRO of 1E-5 per reactor year (for the

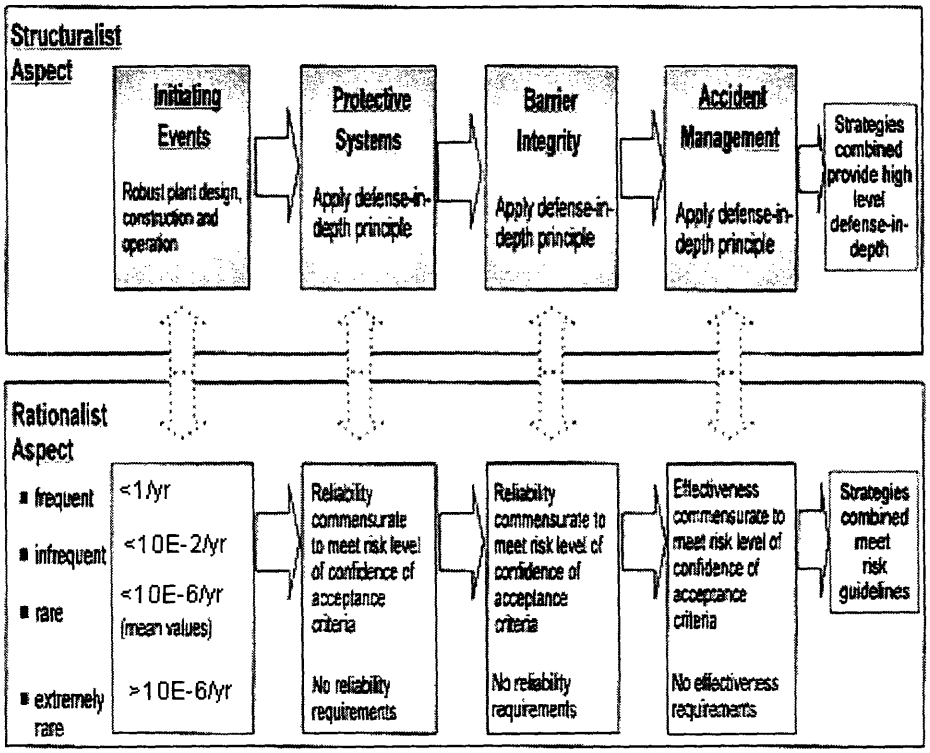

Structuralist Aspect
Initiating Events
Robust plant design, construction and operation
Protective Systems
Apply defense-in-depth principle
Barrier Integrity
Apply defense-in-depth principle
Accident Management
Apply defense-in-depth principle
Strategies combined provide high level defense-in-depth
Rationalist Aspect
frequent
infrequent
rare
extremely rare
<1/yr
<1 0E-2/yr
<1 0E-6/yr (mean values)
>1 0E-6/yr
Reliability commensurate to meet risk level of confidence of acceptance criteria
No reliability requirements
Reliability commensurate to meet risk level of confidence of acceptance criteria
No reliability requirements
Effectiveness commensurate to meet risk level of confidence of acceptance criteria
No effectiveness requirements
Strategies combined meet risk guidelines

Figure III-4 Defense-in-Depth Model (USNRC, 2004)

NRC's proposed framework gives a way for criteria and objectives to be established for the set of new reactors, by using a risk-informed methodology. The NRC is now working on how it can define the scope and develop the actual technology-neutral requirements for new reactors. The framework will be used as a guide to find out what needs to be done for a plant to meet the four protective strategies and adhere to the defense-in-depth criteria.

III B NEI Work

The Nuclear Energy Institute (NEI), is also currently developing a "Risk-informed, performance-based regulatory framework for power reactors". This framework was developed for both design and operational requirements of power reactors. This includes how these new requirements can fit into current regulatory channels including all current documentation methods. This is all detailed in the White Paper that was put out by NEI in 2002. This White established. Various criteria and dose levels will be established for each class of events. A proposed 95% confidence level would be used along with best estimate analysis being employed for treatment of uncertainties (USNRC, 2004).

The NRC tries to use the defense-in-depth approach in the treatment of uncertainties. It takes principles from Regulatory Guide 1.174 along with various ACRS papers on defense-in-depth. The NRC team dealt with the various types of uncertainties (including random, state of knowledge and completeness uncertainties). Human errors are also included. Defense in depth will be used in a structuralist way on the high level, where deterministic requirements will be put in place to address completeness uncertainties, while at the lower levels, the rationalist defense-in-depth method will be employed, using probabilistic methods to assure that certain protective goals are met. The model the NRC uses tries to integrate both approaches into a coherent model for new reactor licensing (USNRC, 2004). This integrated model is shown in figure III-4.

Paper set out to make “NRC activities and decisions more effective, efficient and realistic”. Resources of the power reactor would now be used for systems which would be more safety significant according to the risk-based performance measures used. The White paper intends to establish an alternative to the current regulatory guide 10CFR50 (Nuclear Energy Institute, 2002). This optional part would be called 10CFR53. Part 53 would now implement risk-informed methods. NEI thinks that with this new set of requirements they can not only keep the protection that the industry benefited from with 10CFR50, but will now also be able to draw more out of their available resources while making their system more safety oriented (Nuclear Energy Institute, 2002).

Like the NRC, NEI’s main focus was a defense-in-depth approach based on their cornerstones. Defense-in-depth becomes a main part of their discussions and is used in their iterative process to increase plant safety. Figure III-5, shows how the NEI defense-in-depth process would be implemented (Nuclear Energy Institute, 2002).

Defense-in-Depth Process

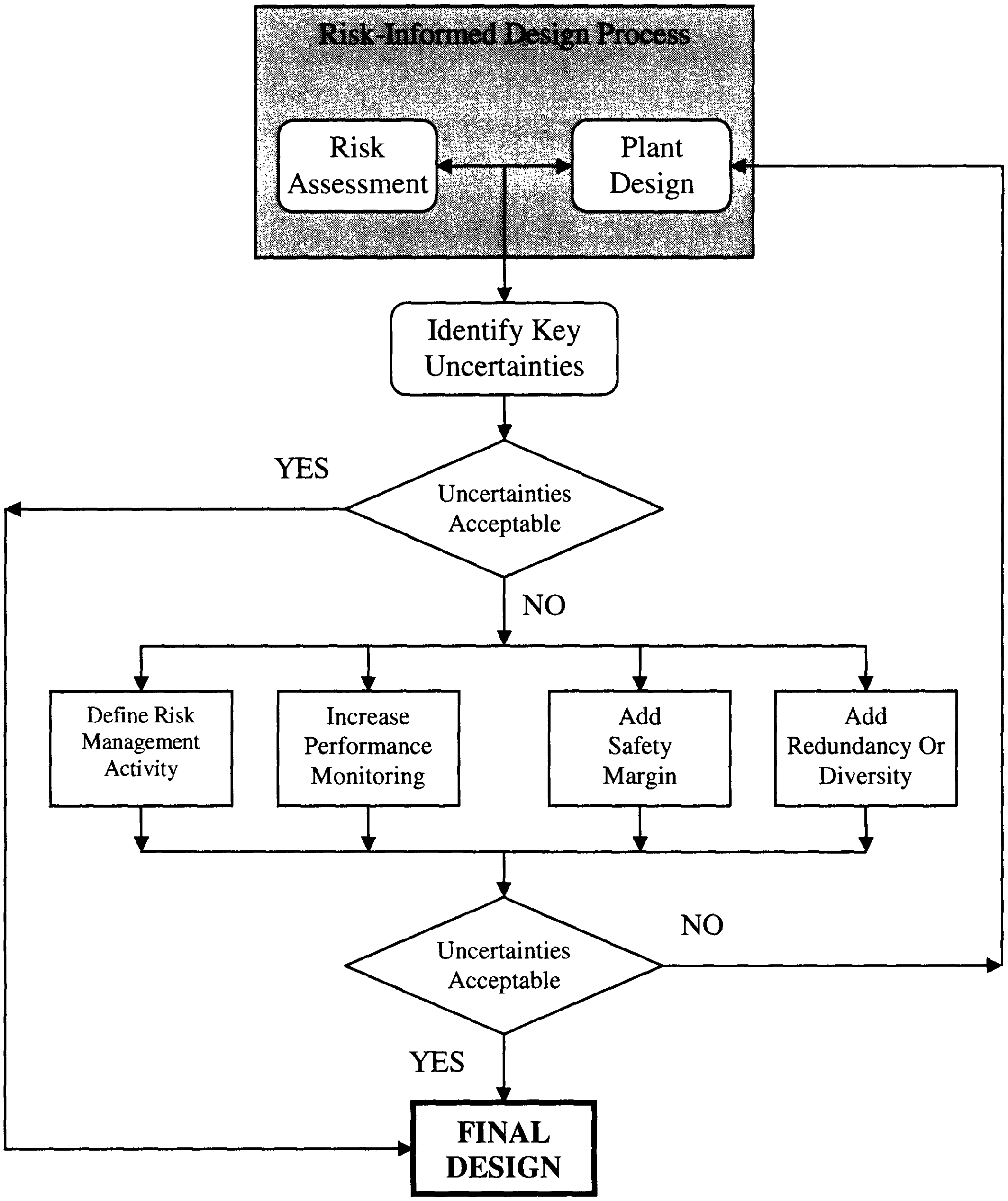

Risk-Informed Design Process
Risk Assessment
Plant Design
Identify Key Uncertainties
YES
Uncertainties Acceptable
NO
Define Risk Management Activity
Increase Performance Monitoring
Add Safety Margin
Add Redundancy Or Diversity
NO
Uncertainties Acceptable
YES
FINAL DESIGN

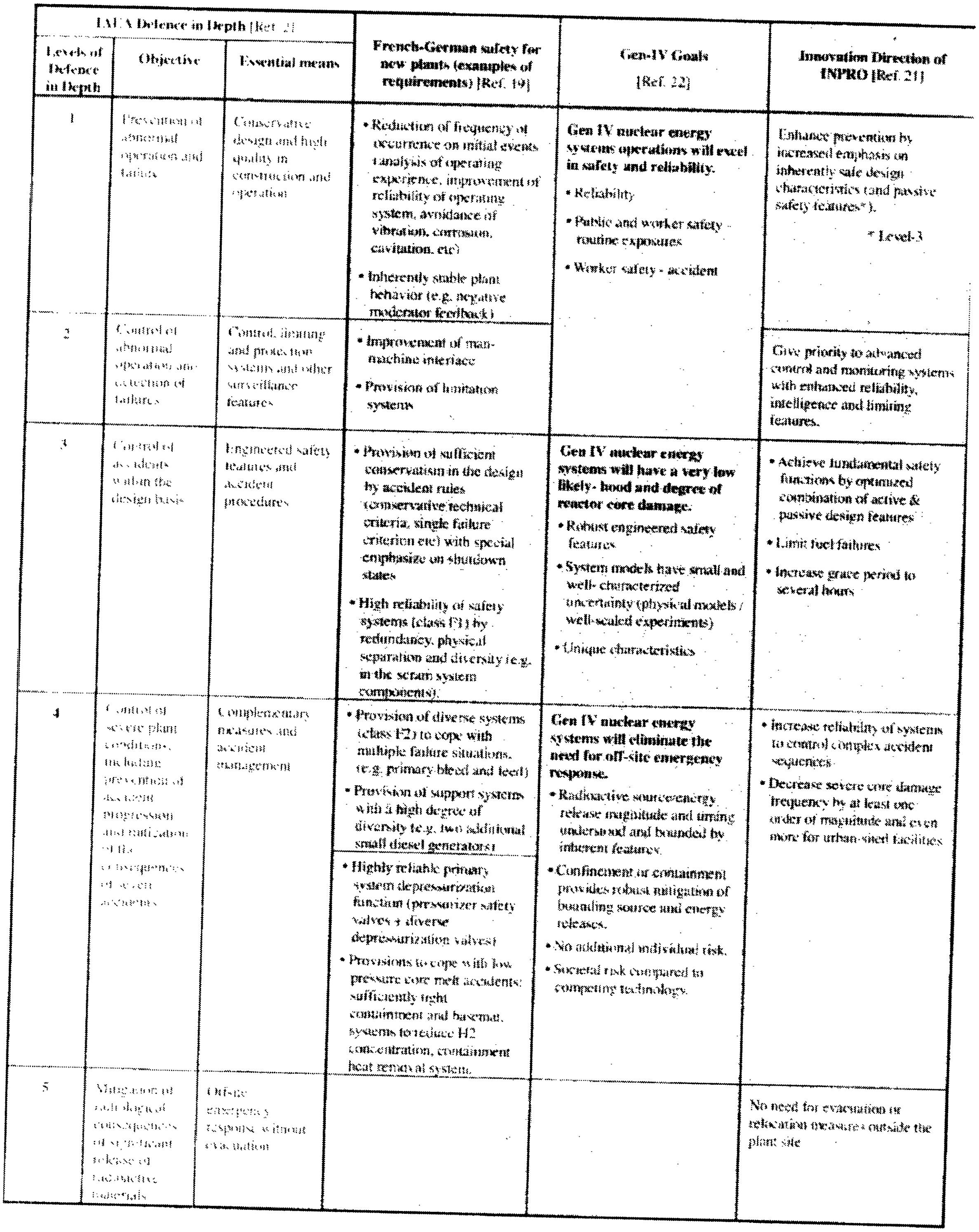
Figure III-5 NEI Defense-in-Depth Process (Nuclear Energy Institute, 2002)

The designer and the PRA team would work together to develop a risk-informed design during which one would identify any of the "key uncertainties" in the design. During this time, the design team would also work to meet the acceptance criteria defined in NEI's proposed 10CFR53 (these criteria have yet to be quantified or developed). Then any unacceptable uncertainties found would be dealt with by any combination of the four defense-in-depth strategies. These are: defining risk management activities, increasing performance monitoring, adding safety margin, and/or add redundancy or diversity. This would be an iterative process between the PRA/Design teams and the regulators, until satisfactory levels of acceptable uncertainties were reached and a final acceptable design is developed (Nuclear Energy Institute, 2002).

III C IAEA Work

The International Atomic Energy Agency (IAEA) is currently developing safety standards for "evolutionary and innovative reactors". These standards will also be based on the Defense-in-Depth approach. Based on knowledge gained from current reactors in operation and the current safety standards, the IAEA will develop standards which encapsulate current approaches yet are also improved through the use of "probabilistic insights". The IAEA would create a set of global requirements that are consistent for reactors in all countries. These would include: "large LWRs, innovative LWRs, MHTGRs and small liquid metal cooled LMRs". As an international organization, the IAEA would create a set of requirements that would satisfy not only the safety needs of the various reactors, but also the current standards of the various countries these reactors are located in (Saito et al, 2004).

The IAEA breaks up their safety goals (based on defense-in-depth) into five levels. These are: prevention of abnormal operation and failure, control of abnormal operation and detection of failures, control of accidents within the design basis, control of severe plant conditions, and mitigation of radiological consequences (Saito et al, 2004). This is shown in figure III-6.



IAEA Defence in Depth [Ref. 2]			French-German safety for new plants (examples of requirements) [Ref. 19]	Gen-IV Goals [Ref. 22]	Innovation Direction of INPRO [Ref. 21]
Levels of Defence in Depth	Objective	Essential means			
1	Prevention of abnormal operation and failures	Conservative design and high quality in construction and operation	• Reduction of frequency of occurrence on initial events (analysis of operating experience, improvement of reliability of operating system, avoidance of vibration, corrosion, cavitation, etc) • Inherently stable plant behavior (e.g. negative moderator feedback)	**Gen IV nuclear energy systems operations will excel in safety and reliability.** • Reliabilty • Public and worker safety - routine exposures • Worker safety - accident	Enhance prevention by increased emphasis on inherently safe design characteristics (and passive safety features*). * Level-3
2	Control of abnormal operation and detection of failures	Control, limiting and protection systems and other surveillance features	• Improvement of man-machine interface • Provision of limitation systems		Give priority to advanced control and monitoring systems with enhanced reliability, intelligence and limiting features.
3	Control of accidents within the design basis	Engineered safety features and accident procedures	• Provision of sufficient conservatism in the design by accident rules (conservative technical criteria, single failure criterion etc) with special emphasize on shutdown states • High reliability of safety systems (class F1) by redundancy, physical separation and diversity (e.g. in the scram system components).	**Gen IV nuclear energy systems will have a very low likely- hood and degree of reactor core damage.** • Robust engineered safety features • System models have small and well- characterized uncertainty (physical models / well-scaled experiments) • Unique characteristics	• Achieve fundamental safety functions by optimized combination of active & passive design features • Limit fuel failures • Increase grace period to several hours
4	Control of severe plant conditions, including prevention of accident progression and mitigation of the consequences of severe accidents	Complementary measures and accident management	• Provision of diverse systems (class F2) to cope with multiple failure situations. (e.g. primary bleed and feed) • Provision of support systems with a high degree of diversity (e.g. two additional small diesel generators) • Highly reliable primary system depressurization function (pressurizer safety valves + diverse depressurization valves) • Provisions to cope with low pressure core melt accidents: sufficiently tight containment and basemat, systems to reduce H2 concentration, containment heat removal system.	**Gen IV nuclear energy systems will eliminate the need for off-site emergency response.** • Radioactive source/energy release magnitude and timing understood and bounded by inherent features. • Confinement or containment provides robust mitigation of bounding source and energy releases. • No additional individual risk. • Societal risk compared to competing technology.	• Increase reliability of systems to control complex accident sequences • Decrease severe core damage frequency by at least one order of magnitude and even more for urban-sited facilities
5	Mitigation of radiological consequences of significant release of radioactive materials	Off-site emergency response without evacuation			No need for evacuation or relocation measures outside the plant site

Figure III-6 Process Examples of Safety Goals for Future Reactors Base on Defense in Depth (Saito et al, 2004)

If defense-in-depth for this methodology is implemented correctly, a failure at one level of defense will not endanger the defense of other levels. The different levels of defense are thusly independent. The IAEA hopes to uses these defense-in-depth levels, along with French-German safety standards, Gen-IV goals, and the direction of the International Project on Innovative Nuclear Reactors and Fuel Cycles (INPRO), to develop their safety standards (Saito et al, 2004). The overall safety standards will be placed into three levels: safety fundamentals (objectives), safety requirements, and safety guides (recommendations and guidance) (Saito et al, 2004).

The current IAEA push is for technology neutral requirements and a top-down approach. There is also a push to help place less constraints on designers, by using a risk-informed approach. Using these technology neutral requirements (also with a top-down approach) IAEA will develop requirements for technology specific designs (based on control of reactivity, removal of heat from the core, and confinement of radioactive materials) (Saito et al, 2004). These are all examined by looking first at the level of defense (starting with an objective), then using what "basic safety system" can protect the public, finding "challenges to the function", "mechanisms to posing the challenges" and finally "provisions" to guard against those mechanisms causing the challenges (Saito et al, 2004). This is the basic plan in which IAEA hopes to use both its defense-in-depth knowledge, along with risk-assessment insights, to develop their safety standards. An example of this is shown in figure III-7.

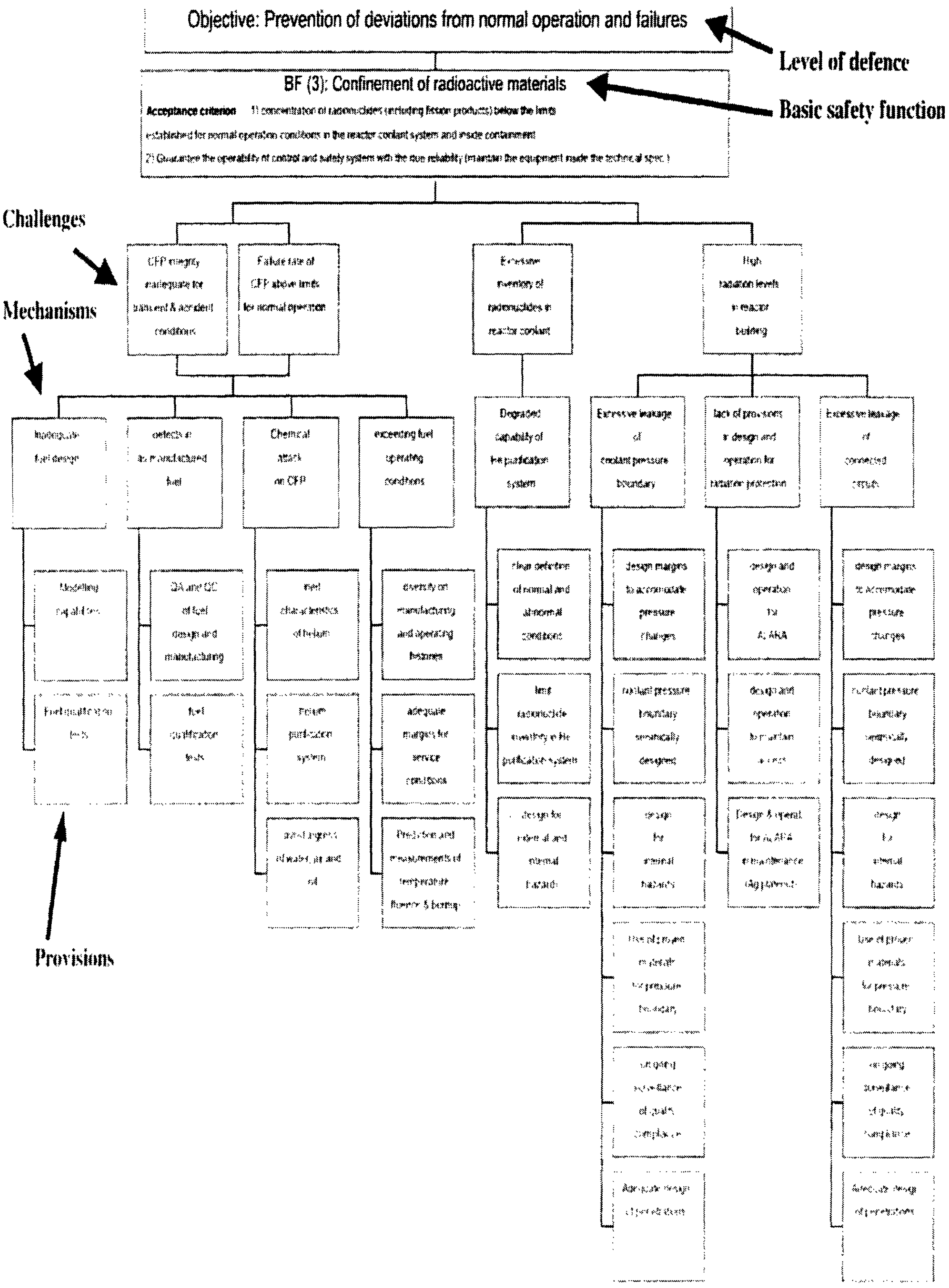

Objective: Prevention of deviations from normal operation and failures
Level of defence
BF (3): Confinement of radioactive materials
Basic safety function
Acceptance criterion 1) concentration of radionuclides (including fission products) below the limits established for normal operation conditions in the reactor coolant system and inside containment
2) Guarantee the operability of control and safety system with the due reliability (maintain the equipment inside the technical spec.)
Challenges
Mechanisms
Provisions
CFP integrity inadequate for transient & accident conditions
Failure rate of CFP above limits for normal operation
Excessive inventory of radionuclides in reactor coolant
High radiation levels in reactor building
Inadequate fuel design
defects in as manufactured fuel
Chemical attack on CFP
exceeding fuel operating conditions
Degraded capability of the purification system
Excessive leakage of coolant pressure boundary
lack of provisions in design and operation for radiation protection
Excessive leakage of connected circuits
Modelling capabilities
Fuel qualification tests
QA and QC of fuel design and manufacturing
fuel qualification tests
inert characteristics of helium
helium purification system
avoid ingress of water, air and oil
diversity on manufacturing and operating histories
adequate margins for service conditions
Prediction and measurements of temperature fluence & burnup
clear definition of normal and abnormal conditions
limit radionuclide inventory in the purification system
design for internal and external hazards
design margins to accommodate pressure changes
coolant pressure boundary seismically designed
design for internal hazards
Use of proven materials for pressure boundary
on going surveillance of quality compliance
Adequate design of penetrations
design and operation for ALARA
design and operation to maintain access
Design & operat. for ALARA in maintenance equipment
design margins to accommodate pressure changes
coolant pressure boundary seismically designed
design for internal hazards
use of proven materials for pressure boundary
on-going surveillance of quality compliance
Adequate design of penetrations

Figure III-7 Example of IAEA Defense-in-Depth Approach (for MHTGR) (Saito et al, 2004)

III D NERAC Work

The Nuclear Energy Research Advisory Committee (NERAC) has developed a "Technology Roadmap for Generation IV Nuclear Energy Systems". This project is trying to define the steps needed to be taken to support innovative Generation IV plant designs. The NERAC goals, which are dissimilar to those of the NRC, which only focus on safety, are shown in figure III-8.

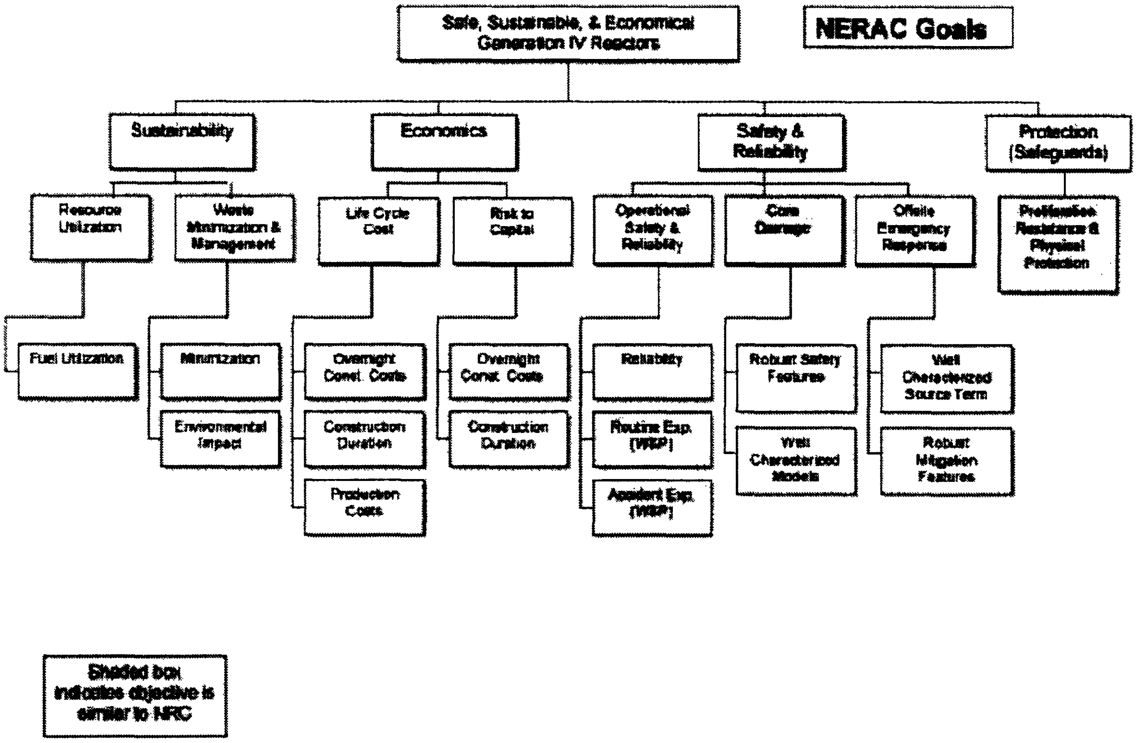


Figure III-8 NERAC Goals (U.S. Department of Energy, 2002a)

NERAC focuses on four factors: sustainable nuclear energy, competitive nuclear energy (Economics), safe and reliable systems, and proliferation resistance and physical protection (U.S. Department of Energy, 2002a). Many experts in the nuclear field have come together to develop this roadmap, so that the industry as a whole, along with the public, and all other stakeholders will benefit from the research being done.

NERAC will use the four goal areas (split up into 8 goals), along with 15 criteria for those goals, to develop metrics for which for which a design can be judged for each of these criteria, and thus for each equally important goal areas. This process is shown in Figure III-9.

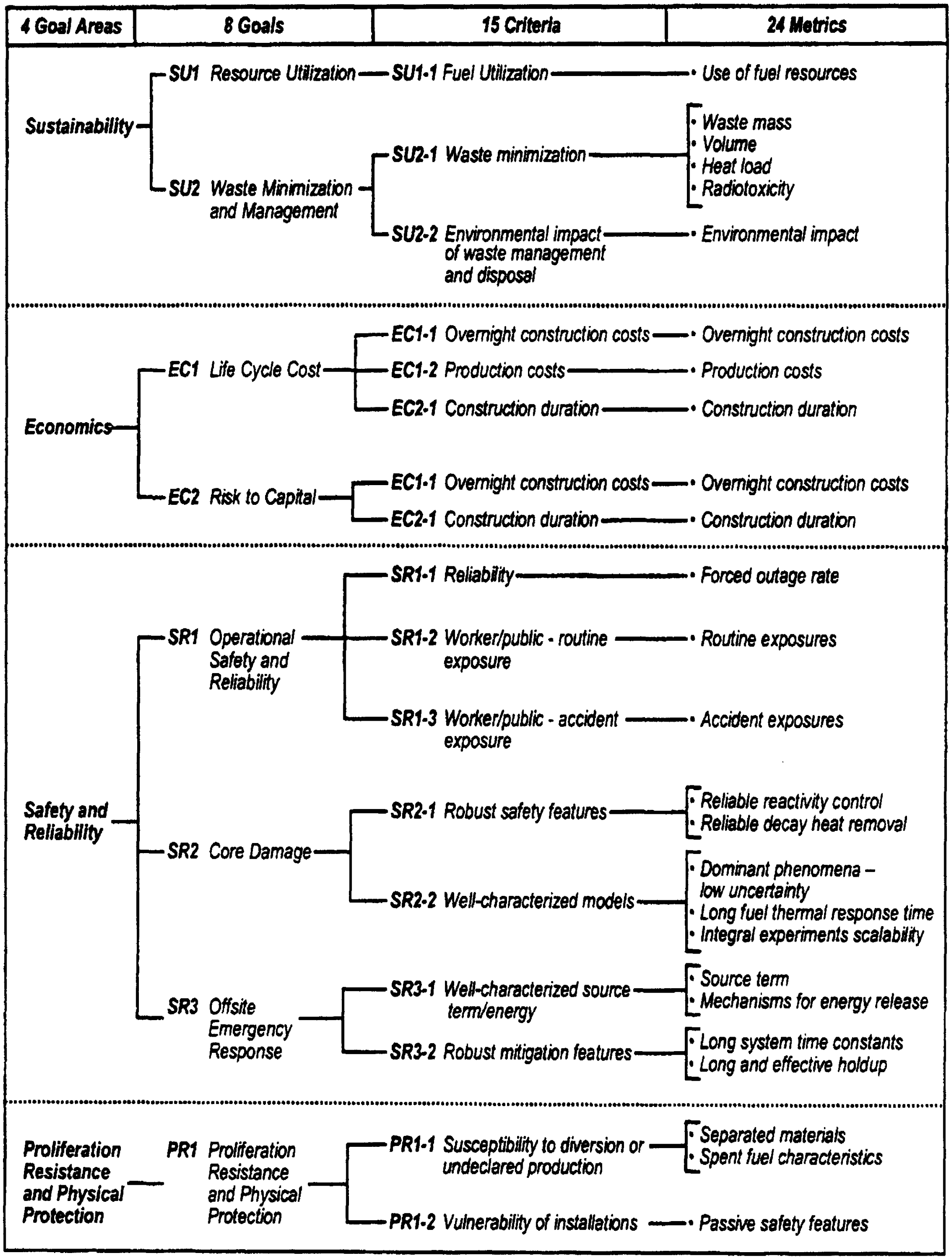

4 Goal Areas
8 Goals
15 Criteria
24 Metrics
Sustainability
SU1 Resource Utilization
SU1-1 Fuel Utilization
• Use of fuel resources
SU2 Waste Minimization and Management
SU2-1 Waste minimization
• Waste mass
• Volume
• Heat load
• Radiotoxicity
SU2-2 Environmental impact of waste management and disposal
• Environmental impact
Economics
EC1 Life Cycle Cost
EC1-1 Overnight construction costs
• Overnight construction costs
EC1-2 Production costs
• Production costs
EC2-1 Construction duration
• Construction duration
EC2 Risk to Capital
EC1-1 Overnight construction costs
• Overnight construction costs
EC2-1 Construction duration
• Construction duration
Safety and Reliability
SR1 Operational Safety and Reliability
SR1-1 Reliability
• Forced outage rate
SR1-2 Worker/public - routine exposure
• Routine exposures
SR1-3 Worker/public - accident exposure
• Accident exposures
SR2 Core Damage
SR2-1 Robust safety features
• Reliable reactivity control
• Reliable decay heat removal
SR2-2 Well-characterized models
• Dominant phenomena – low uncertainty
• Long fuel thermal response time
• Integral experiments scalability
SR3 Offsite Emergency Response
SR3-1 Well-characterized source term/energy
• Source term
• Mechanisms for energy release
SR3-2 Robust mitigation features
• Long system time constants
• Long and effective holdup
Proliferation Resistance and Physical Protection
PR1 Proliferation Resistance and Physical Protection
PR1-1 Susceptibility to diversion or undeclared production
• Separated materials
• Spent fuel characteristics
PR1-2 Vulnerability of installations
• Passive safety features

Figure III-9 NERAC Goal Areas, Goals, Criteria and Metrics (U.S. Department of Energy, 2002a)

III E ACRS Work

III E i New Reactor Certification Impediments

In the paper "Impediments to the Certification of New Technology Reactor Designs" (Kress, 2002), Kress discusses the challenges he felt would arise as new reactor designs began to become certified under the proposed new requirements of the USNRC. These included not only the current design basis accidents (DBA) but also applying the concepts of defense-in-depth and risk-informed acceptance criteria. Kress suggests that these three areas will be where the new reactor designers run into trouble with certification (Kress, 2002).

Current standards and DBAs were made for light water reactors (LWR). So, for new concepts, such as the GFR, a new set of requirements must be constructed or current requirements amended. This is more important for designs which are greatly dissimilar from current reactors (and thus cannot be certified using current regulations) (Kress, 2002). Kress gives two options for regulating these new designs, which are either using current DBA methodology along with "exemptions and design-specific requirements" or using the newly proposed risk-informed technology-neutral methodology for regulation (Kress, 2002).

In discussing risk-informed criteria, Kress thinks there is a lack of risk-acceptance criteria, only quoting Regulatory Guide 1.174 as having metrics of CDF and LERF for proposed changes to plant licensing. He suggests these have a limited use and a more defined, "full range" (including uncertainties) set of risk-acceptance criteria need to be developed. The author stresses that a more fully developed metric should be used (using a frequency/consequence (cost) methodology) (Kress, 2002).

Kress proposes that the current DBA methodology also impedes new reactor designs from certification. The proposed DBAs are ones which have frequencies consistent with that of frequency values for LWRs. He worries, though, about the overall frequency cutoff (including previously excluded events) for the reactor design and suggests that the value may vary with design. The question is how to set this value. Kress advises that instead of the current way of doing things, there should be an iterative process between a design team and its PRA team. A cut-off frequency value would be proposed and a process would occur between both teams until both the cut-off frequency requirement and the DBA requirements were met. It is believed this process could set the overall value for a new design (Kress, 2002). This is similar to how the PRA group for the MIT-GFR has been operating. The PRA group uses the MIT Framework which has used a similar way of developing criteria and using a deliberative design process between the PRA and design teams till those criteria are met for the best design (Apostolakis et al, 2004).

Lastly, Kress discusses how the concept of defense-in-depth poses impediments to the process. Defense-in-depth seems to be most prevalent when applied to the containment. Many of these regulations, however do not seem to apply to gas-cooled reactors as they did to LWRs (such as large break LOCA specifications, pressure specifications, and source term specifications). Kress thinks there needs to be a way to identify what is a safe containment based on DID principles. Currently, the ACRS uses the "structuralist" and "rationalist" principles explained earlier. He advises that the structuralist view meeting the DBAs is not fully related to the overall risk of the design (Kress, 2002). There needs to be a quantifiable metric to find if defense-in-depth features are acceptable. He suggests that the rationalist approach puts too much "faith" in PRA technologies (Kress, 2002). Since there is not a lot of experience with these new designs, this faith may be unwarranted (Kress, 2002). Overall, the three impediments listed all center around developing a risk-informed regulatory framework. They show that there is a need for risk-informing design basis accidents, leading to a smoother certification process for new technology reactor designs.

III E ii Risk-Informing Appendices A & B to 10 CFR Part 50

Sorensen's work for the ACRS is on risk-informing the general design criteria (GDC) for appendix A of 10 CFR 50. This involves changing the GDC from "important to safety" to "important to risk". It also involves making the individual criteria risk-informed. Lastly it involves replacing the current GDCs to offer instead, risk-informed goals and criteria (Sorensen, 2002). The key parts of Appendix A that were identified in Sorensen's work are: single failures of passive components, redundancy and diversity requirements, type, size and orientation of pipe breaks (this is our main concern when informing the 50-46 ECCS rule), and the possibility of "non-random, concurrent failures of redundant elements in control systems" (Sorensen, 2002).

The GDC are meant to reduce the overall consequences of an accident (i.e., the risk to the public). The GDCs require redundancy and diversity (including items such as the single failure criteria (SFC)), assuming the system will then be more reliable. It seems disconcerting that these would be required rather than the quantitative value for the overall system reliability as is now being proposed by the NRC's new framework (Sorensen, 2002).

In 1993, the Regulatory Review Group (RRG) found that Appendix A was "performance-based, contributed to safety and did not go beyond what was required for safety (Sorensen, 2002). They also found that the burden being faced by many plants was when the staff went beyond these safety requirements and also in the enforcing of these "over-commitments" (Sorensen, 2002). This is why it is felt that quantitative safety goals should be used to develop these GDCs and why many screening criteria (such as the SFC) are being replaced by risk-informed regulations.

What is being proposed by Sorensen are three possible methods. The first is changing the GDCs so they only apply to components which are "risk-significant". The second is to look at the individual criteria and change requirements to reflect the risk of each (as it compares with the overall safety of the system). Lastly, he proposes that the GDCs could be replaced with risk-acceptance criteria (Sorensen, 2002).

Sorensen gives various examples of ways in which the rules such as the SFC is not needed when parts of the GDC (or the whole GDC itself) is replaced with risk-based safety goals. He brings up the point, when dealing with criterion 33, that PRA could be used to find if safety significant features are truly risk-significant (Sorensen, 2002). However, the most significant portion of his work, as dealing with the current NRC work, is with criterion 35 (which deals with the ECCS). Here, as with discussions by the NRC and ACRS, Sorensen brings up the point of changing the rule that "treats the double-ended break of the largest pipe in the reactor coolant system in addition to offsite power being unavailable and a single failure in the most critical place as the DBA for the ECCS" (Sorensen, 2002). However, the largest pipe may not be "reasonable" as it may not be the most frequent pipe to have the highest consequences. PRA methodology could be used to determine which is the most risk significant pipe break size for LOCAs to use in criterion 35. This would likely be based on the frequency consequence curve discussed earlier, where this would be the pipe-break LOCA to cause a great amount of damage, and also the frequency of it occurring would still be "reasonable" under risk-standards.

Overall, the individual criteria's contribution to the systems risk would be used in determining a new risk-informed appendix A to 10CFR50 (Sorensen, 2002). It might be hard to test with current reactor facilities the proposed changes to see if they met the newly developed risk-informed GDC, yet it is felt that for new reactor designs this is something that can be tested.

By establishing quantitative reliability requirements, one could truly have a system with criteria that are not only safety-significant, but also risk-significant. For one to risk-inform the DBAs, one must first be able to find a quantitative basis for risk in the GDCs.

III F Current University Work

III F i Risk-Informed Regulation/Design Methodologies

At the current time, a methodology to develop risk-informed regulations is underway at MIT. This follows the four step-decision making methodology shown in figure III-10.

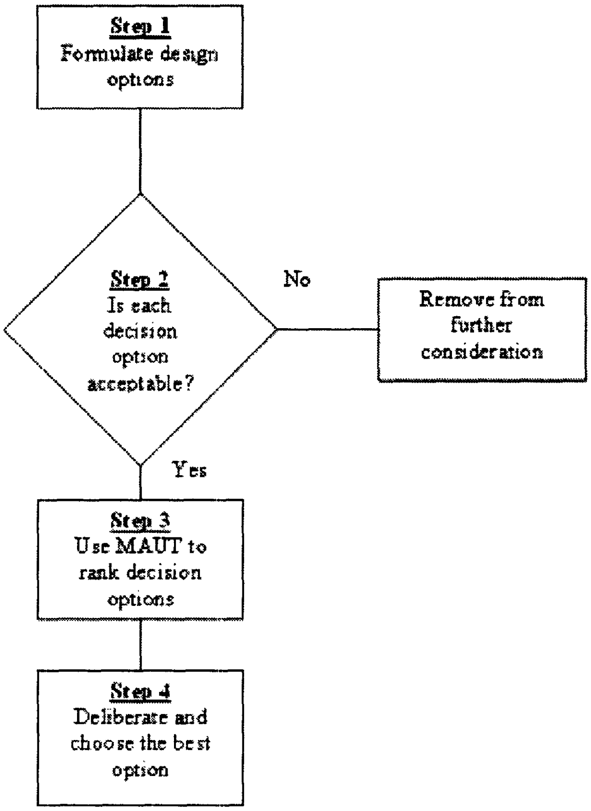

Step 1
Formulate design options
Step 2
Is each decision option acceptable?
No
Remove from further consideration
Yes
Step 3
Use MAUT to rank decision options
Step 4
Deliberate and choose the best option

Figure III-10 Four Step Methodology (Apostolakis et al, 2004)

Here, the regulator dealing with a new reactor design (or a designer) could examine decision options formulated by a designer for various aspects of their design. They would then go to step two, where they would check, using the MIT Framework developed by Apostolakis et al, if such an option would be acceptable (Apostolakis et al, 2004). The acceptable options would then be ranked using multi-attribute utility theory (or some other suitable metric). Finally, the stakeholders would deliberate over the results and choose the best option for their design. This would be an iterative process between the designer and the regulator, as will be discussed further (Apostolakis et al, 2004).

The MIT Framework used in step two is shown in figure III-11.

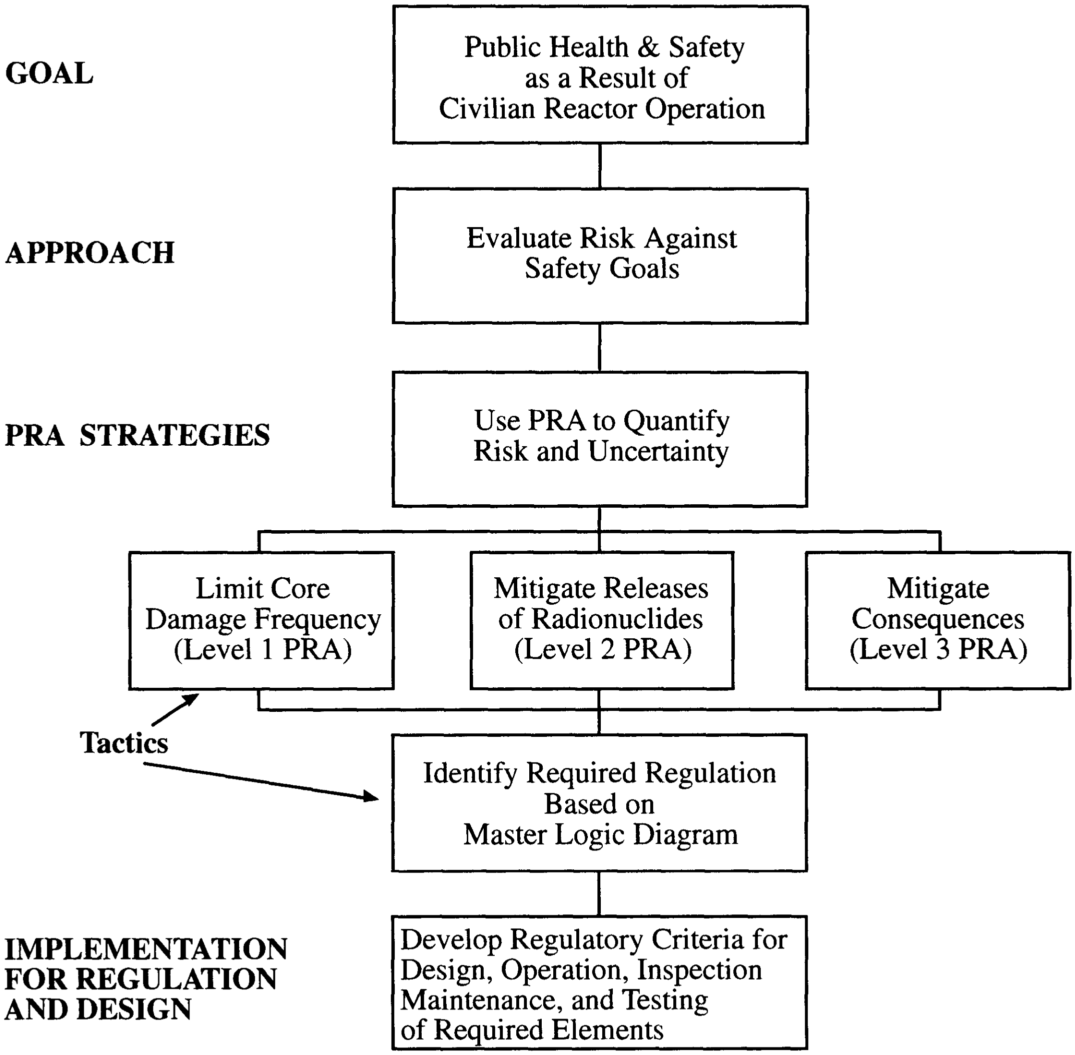

GOAL
Public Health & Safety as a Result of Civilian Reactor Operation
APPROACH
Evaluate Risk Against Safety Goals
PRA STRATEGIES
Use PRA to Quantify Risk and Uncertainty
Limit Core Damage Frequency (Level 1 PRA)
Mitigate Releases of Radionuclides (Level 2 PRA)
Mitigate Consequences (Level 3 PRA)
Tactics
Identify Required Regulation Based on Master Logic Diagram
IMPLEMENTATION FOR REGULATION AND DESIGN
Develop Regulatory Criteria for Design, Operation, Inspection Maintenance, and Testing of Required Elements

Figure III-11 MIT Framework (Apostolakis et al, 2001)

Like the methodology of the NRC, shown earlier, the MIT Framework also uses a top-down hierarchy to find if design options are acceptable. The top goal of overall safety and health of the public is also the same. An approach is given of how to reach those goals, along with PRA strategies of where to implement the approach and Tactics of how to implement this approach. Finally, through these steps, criteria are developed for risk-informed regulation and design. Uncertainties would be included and risk quantified to achieve proper regulations (Apostolakis et al, 2001).

The iterative design process, which will be useful to both designer and regulator, is currently being tested. This is the development of the implementation of PRA strategies talked of in the MIT Framework (along with an extra preliminary check of deterministic criteria to account for unknowns, and which also shows that this is a risk-informed rather than risk-based methodology). In figure III-12, this process, where a bare bones reactor is developed by a designer and a risk-informed methodology is used, is shown.

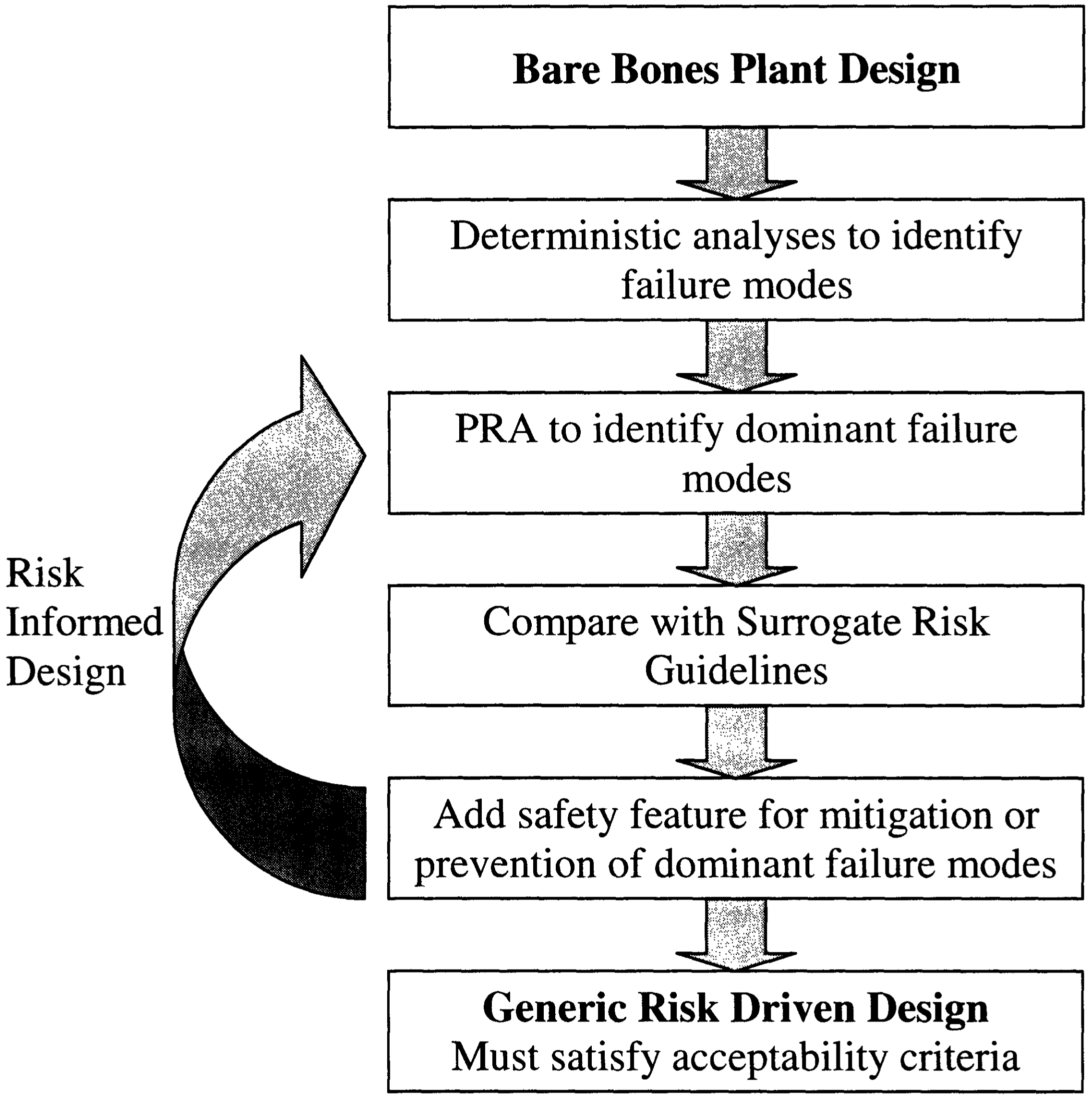

Bare Bones Plant Design
Deterministic analyses to identify failure modes
PRA to identify dominant failure modes
Compare with Surrogate Risk Guidelines
Add safety feature for mitigation or prevention of dominant failure modes
Generic Risk Driven Design
Must satisfy acceptability criteria
Risk Informed Design

Figure III-12 Bare-Bones Design Methodology (Apostolakis et al, 2001)

The designer begins with a bare-bones plant and first uses the current methodology of deterministic analysis to find any possible failure modes. Then the new PRA methodologies are used to find failure modes. These are checked against surrogate risk guidelines (as discussed earlier in the NRC's current work) and if the guidelines are not met, safety features are added in an iterative process until they do. Once this occurs, the result is an acceptable "generic risk-driven design" (Apostolakis et al, 2001).

Due to the fact that the regulatory process for Generation IV reactors seems to be a constant negotiation between designer and regulator, deterministic analysis will not be able to develop a set of regulations that are complete and provide the regulatory agency with a level of confidence needed to assure safe plant operation. This is why a methodology as shown above, with an iterative risk-informed step, is needed to account for lapses in completeness in the deterministic methodology. The traditional deterministic approach uses only defense-in-depth to assure safety, however when developing new reactor designs this may not be enough (Apostolakis et al, 2001). The addition of safety margins is the key to determining what failure modes can occur in this new design that are unaccounted for previously, as well as using rational thought to not be overly conservative. This helps the industry to find out where safety could be better placed, rather than blindly placing more barriers to get protection.

III F ii MIT-GFR Work

The above methodologies are currently being applied to the test case of the MIT-Gas-Cooled Fast Reactor (GFR). The CO_2 cooling system for this bare-bones reactor design is currently being developed using risk-informed techniques, as this is one of the more safety-critical systems. The bare-bones cooling system is shown in figure III-13.

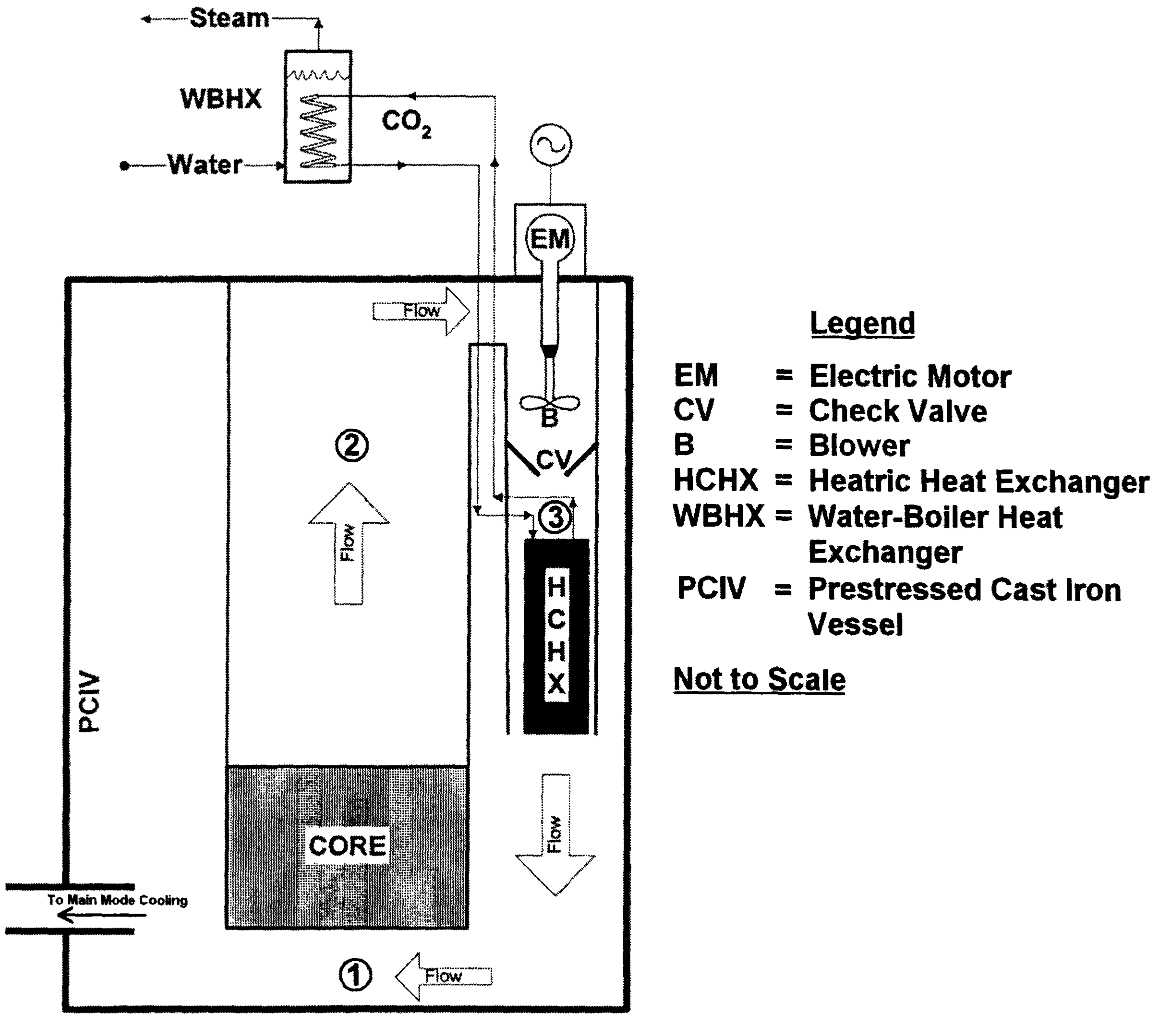


Figure III-13 Bare-Bones Design for GFR Cooling System

The negotiating process talked of earlier between the designer and regulator is currently being used, with a "mock-regulator" in place. This process will help drive the design team to a safer reactor design, more aligned with the concerns of the regulatory agency. The overall four-step methodology will be used, along with the MIT Framework to not only make sure the safety requirements are met (from a regulatory standpoint), but these methodologies will also help with the cost effectiveness and the efficiency of the overall design.

The PRA team currently employing these methodologies is working with the design team to try to form a set of risk-informed design basis accidents that can be used for Generation IV reactors. If this can be accomplished for this technology-specific test case, it is hoped that a similar technology-neutral methodology can be applied. This methodology could then create risk-informed DBAs for all next generation reactor designs. This is the basis for the current thesis work, and will be exemplified through work done on the GFR: specifically in the accident initiators of the Turbine Trip, Loss of Offsite Power (LOOP) and Loss-of-Coolant Accidents, discussed later in greater detail.

III G Current Activities Conclusions

It was seen that the NRC, IAEA, NEI, and NERAC had similar views that regulations for future reactors should move to a more risk-informed system to improve the safety of generation-IV reactors. Defense-in-depth was something that all groups currently working on regulations for generation-IV reactors determined was necessary. Both the NRC and the IAEA have said they would develop a technology-neutral framework for all reactor types. This it is thought would be an easier way to then develop more technology specific methods at a later time.

It was found that unlike the NRC and IAEA, NEI would like to develop a set of requirements that not only helped protect the plant, but also had some focus on benefiting the industry (by drawing more out of the available resources). NERAC's framework for risk-informed regulation also had differences from the NRC and IAEA methodologies. While the NRC and IAEA methodologies focused solely on safety, NERAC focused on 4 goals: Sustainability, Economics, Safety/Reliability, and Protection. This shift in focus, no matter how much weight is given to safety over the other three, seems to go against what is said in the four-step methodology (Apostolakis et al, 2004). I feel one should place focus solely on safety before dealing with any other aspect of the design. Once safety criteria are met, then and only then should one start to see how to better other aspects of the design.

The work done by the ACRS also brought insights. The impediments to new reactor certification given current regulations are discussed. Current LWR reactors were shown not to fully apply to new reactor concepts, thus limiting the innovativeness of these new designs (Kress 2002). It is also shown that the defense-in-depth currently used in the containment for LWRs may not apply to future gas-cooled reactor concepts. The ACRS work also expressed interest in a quantitative value for system reliability, being disconcerted by the lack thereof in current regulations.

Overall, most of the methodologies discussed were quite similar (with minor variations). The only methodologies which differed were ones from an industry standpoint, because they were also looking out for their best interests. In these cases, the groups proposing them do not view them from a safety-first standpoint. I feel that these are methods that should not be used because for innovative concepts which have never been tested, regulations need to prove the reactor designs are safe before any other goals should be taken into consideration, to provide adequate confidence to the plant, its workers, and the public.

(This page intentionally left blank)

IV Turbine Trip Initiator Work for GFR

While investigating the development of design-basis-accidents, the turbine trip initiating event was looked at for the GFR plant design. The DBA for this accident scenario is defined for a LWR plant in its UFSAR as "the reactor would be tripped directly from a signal derived from the turbine emergency trip fluid pressure and turbine stop valves. The turbine stop valves close rapidly (typically in 0.1 seconds) on loss of trip fluid pressure actuated by one of a number of possible turbine trip signals" (U.S. Code of Federal Regulations, 2004). The design basis accident assumes the turbine is tripped abruptly, reactor SCRAM, a loss of either onsite power (assuming offsite power is working) or offsite power (assuming onsite power is working), and finally the Single Failure Criteria (SFC) is applied. The SFC is defined as: "A single failure means an occurrence which results in the loss of capability of a component to perform its intended safety functions. Multiple failures resulting from a single occurrence are considered to be a single failure. Fluid and electric systems are considered to be designed against an assumed single failure if neither (1) a single failure of any active component (assuming passive components function properly) nor (2) a single failure of a passive component (assuming active components function properly), results in a loss of the capability of the system to perform its safety functions" (USNRC, 2003).

For the GFR, an event tree was developed. This is shown in figure IV-1. First the turbine is tripped. Then, it is checked whether or not the reactor can be SCRAMed. If the SCRAM fails, then the reactor would be attempted to be shutdown via the reactor feedback (which the design team postulates can be safely achieved). If the SCRAM does occur, then it is checked whether we have offsite and subsequently onsite (both AC and DC) power. If either the onsite or offsite systems give power to the plant, then the active shutdown cooling system (SCS) is checked to see whether it is available. In either case (plant having or not having power), there is always the ability of the passive SCS system to help cool the plant. Finally, it is checked to see if the ultimate heat sink is functional. This ultimate heat sink has yet to be determined (and will likely be modeled as the large cooling ponds of current LWR reactors for the time being).

For the GFR plant test cases that are being run, the design team has currently settled on a set-up to use for the bare-bones reactor. So, for these cases, the onsite AC Power has loops set-up in a 2x100% system. Also the offsite DC Power uses batteries in a 2x100% set-up. Both the active and passive SCS systems for these test cases have 3x50% loop set-ups. For each of these systems, fault trees were developed (as well as the overall event tree) in the Systems Analysis Program for Hands-on Integrated Reliability Evaluations (SAPHIRE), a computer code developed for the USNRC, by Idaho National Engineering and Environmental Laboratories (INEEL). These trees are shown graphically in figures IV-2 through IV-81, while the reactivity feedback system, offsite power, and ultimate heat sink were each taken as basic events (due to lack of knowledge on specific design at the present time). The component failure data for each of these fault trees are listed in Appendix A, Table A-1. The sources for the data are also included in this table.

The reason the GFR group investigated accidents such as this were two-fold. The first is the designer's standpoint. The investigation of various initiators and their impact on plant safety (in the form of CDF and LERF) helps the designer to know where safety constraints (such as adjusting systems and components to decrease risk factors). Knowledge of where to add redundancy and diversity to prevent the plant from exceeding surrogate risk guidelines will help the designer re-organize their design to meet the goals of the regulatory agency. They can see deficiencies in their design and make changes to fix them. The insights used from a risk analysis of the plant and its systems, based on current regulatory requirements (such as DBAs), will help the designer to make the design more effective and safer for all stakeholders. The designer will not have to do a large overhaul that may come from a completed design that had failed to meet regulatory requirements if they had been using risk-informed methodologies to verify the design during the various earlier stages of the design process.

The second part of the two-fold reason for looking at GFR accident initiators, and their impact on plant safety, was from a regulatory standpoint. To a regulator, the investigation of these initiators (and their impact on plant safety) is an effective way to evaluate a plant design. It shows to the regulator (as it did to the designer) weaknesses in the plant and leaves smaller room for argument than a purely deterministic system might. Regulators could more easily pinpoint what systems (or components) in the design were unsafe (based on surrogate risk guidelines) and could tell the designers what systems (or components) in the design would need to be modified or improved to comply with current regulatory guidelines. It allows regulators (who have knowledge of probabilistic risk assessment) to review the system and to judge how well it holds up to regulatory standards. Risk assessment can also show a regulator what could be missed by adapting a purely deterministic standpoint (which may leave a plant's safety lacking in certain areas and overly stringent in others).

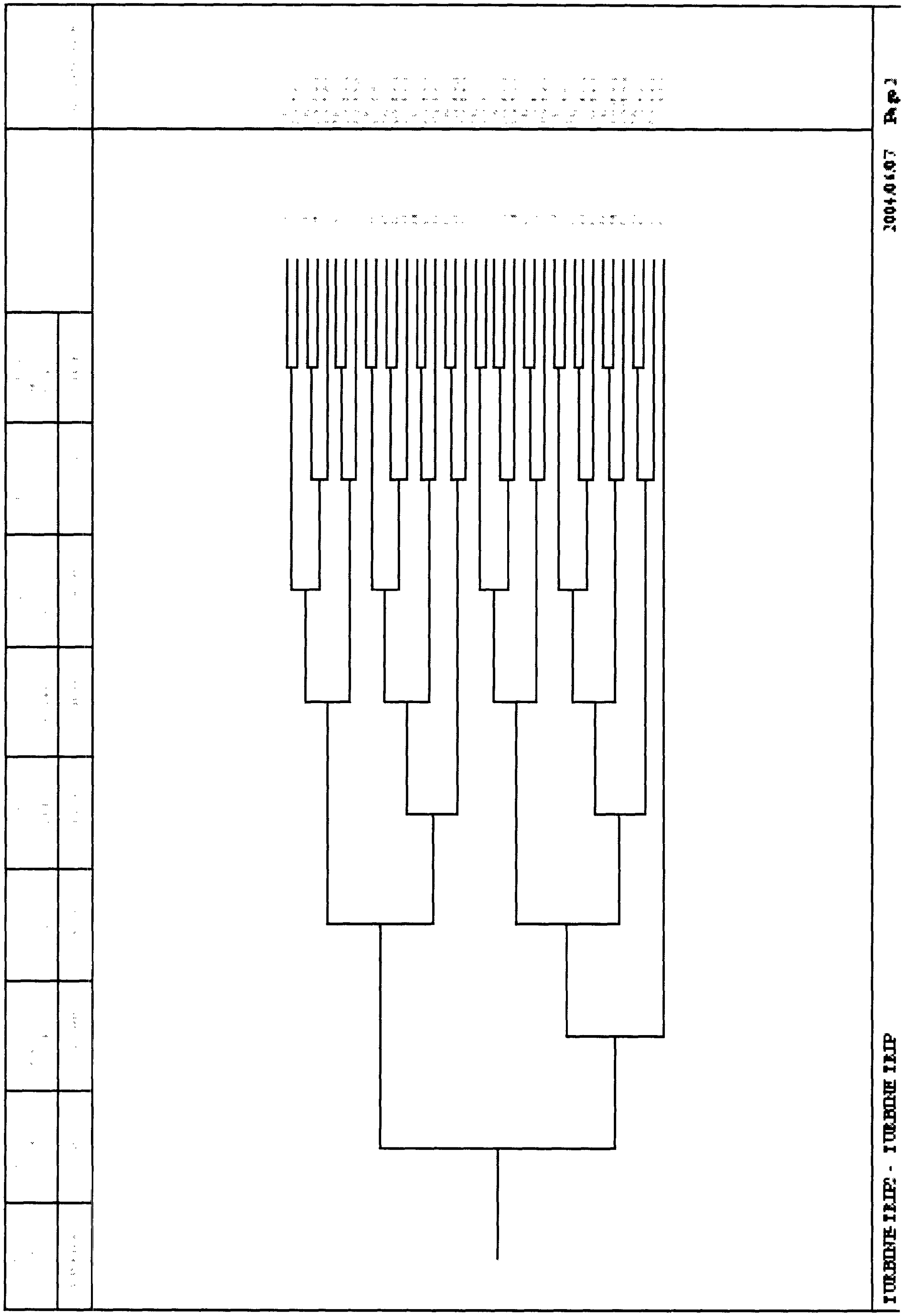


Figure IV-1 Event Tree for Turbine Trip Initiator in GFR

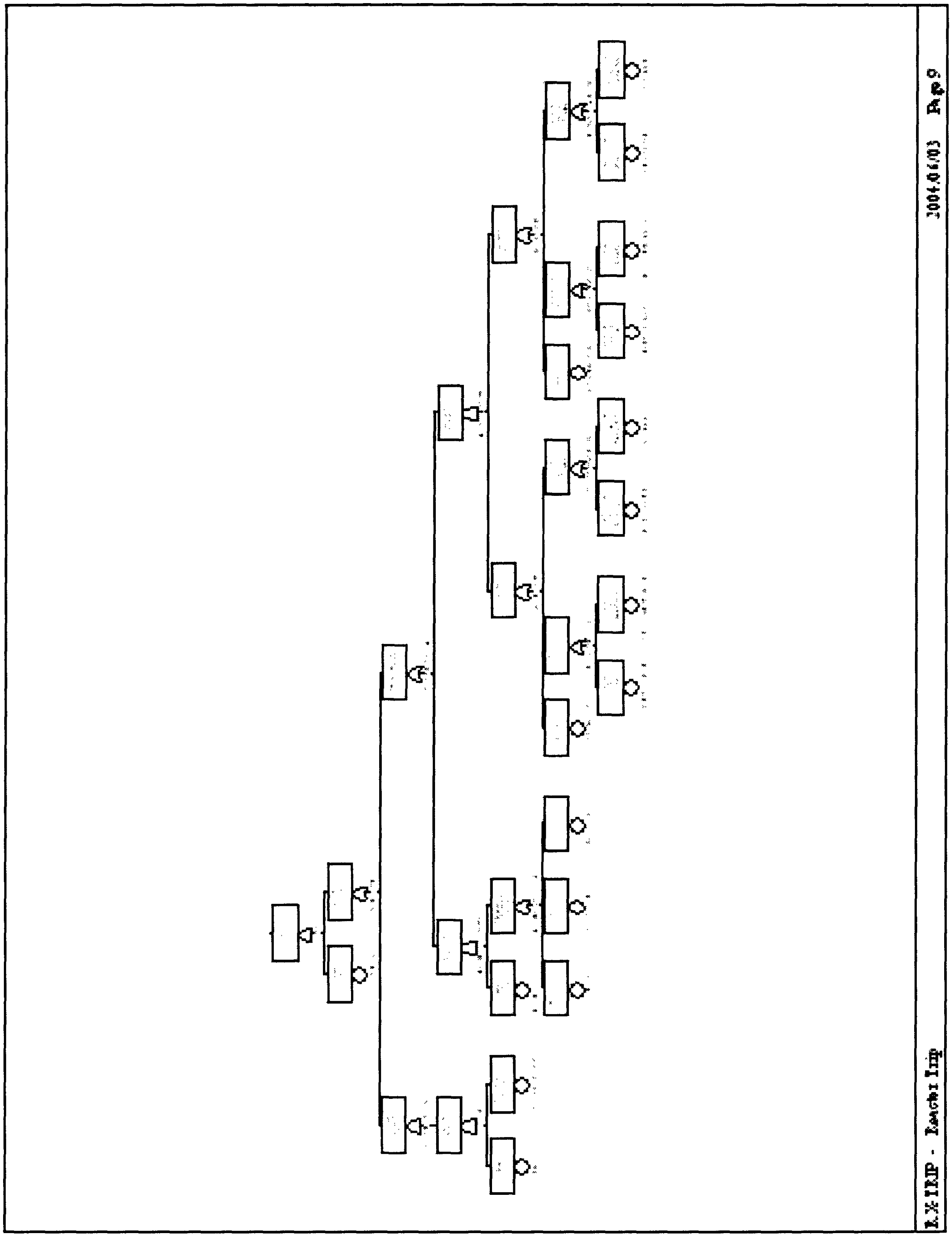


Figure IV-2 Fault Tree for Reactor Trip in GFR: Following "Zoomed In" Figures for enlarged, readable sections of the Fault Tree

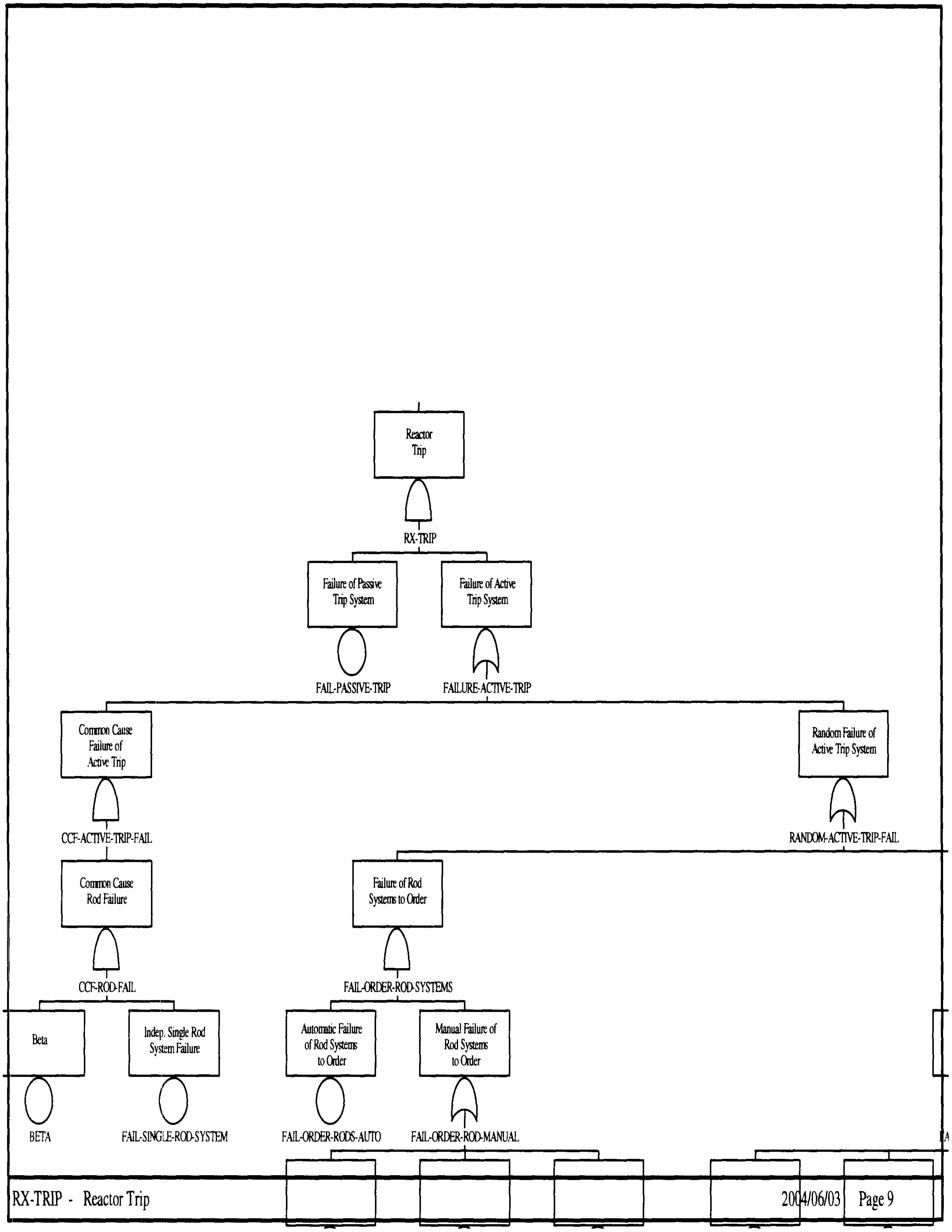

Reactor Trip
RX-TRIP
Failure of Passive Trip System
Failure of Active Trip System
FAIL-PASSIVE-TRIP
FAILURE-ACTIVE-TRIP
Common Cause Failure of Active Trip
Random Failure of Active Trip System
CCF-ACTIVE-TRIP-FAIL
RANDOM-ACTIVE-TRIP-FAIL
Common Cause Rod Failure
Failure of Rod Systems to Order
CCF-ROD-FAIL
FAIL-ORDER-ROD-SYSTEMS
Beta
Indep. Single Rod System Failure
Automatic Failure of Rod Systems to Order
Manual Failure of Rod Systems to Order
BETA
FAIL-SINGLE-ROD-SYSTEM
FAIL-ORDER-RODS-AUTO
FAIL-ORDER-ROD-MANUAL
RX-TRIP - Reactor Trip
2004/06/03
Page 9

Figure IV-3 Fault Tree for Reactor Trip in GFR: Zoom 1

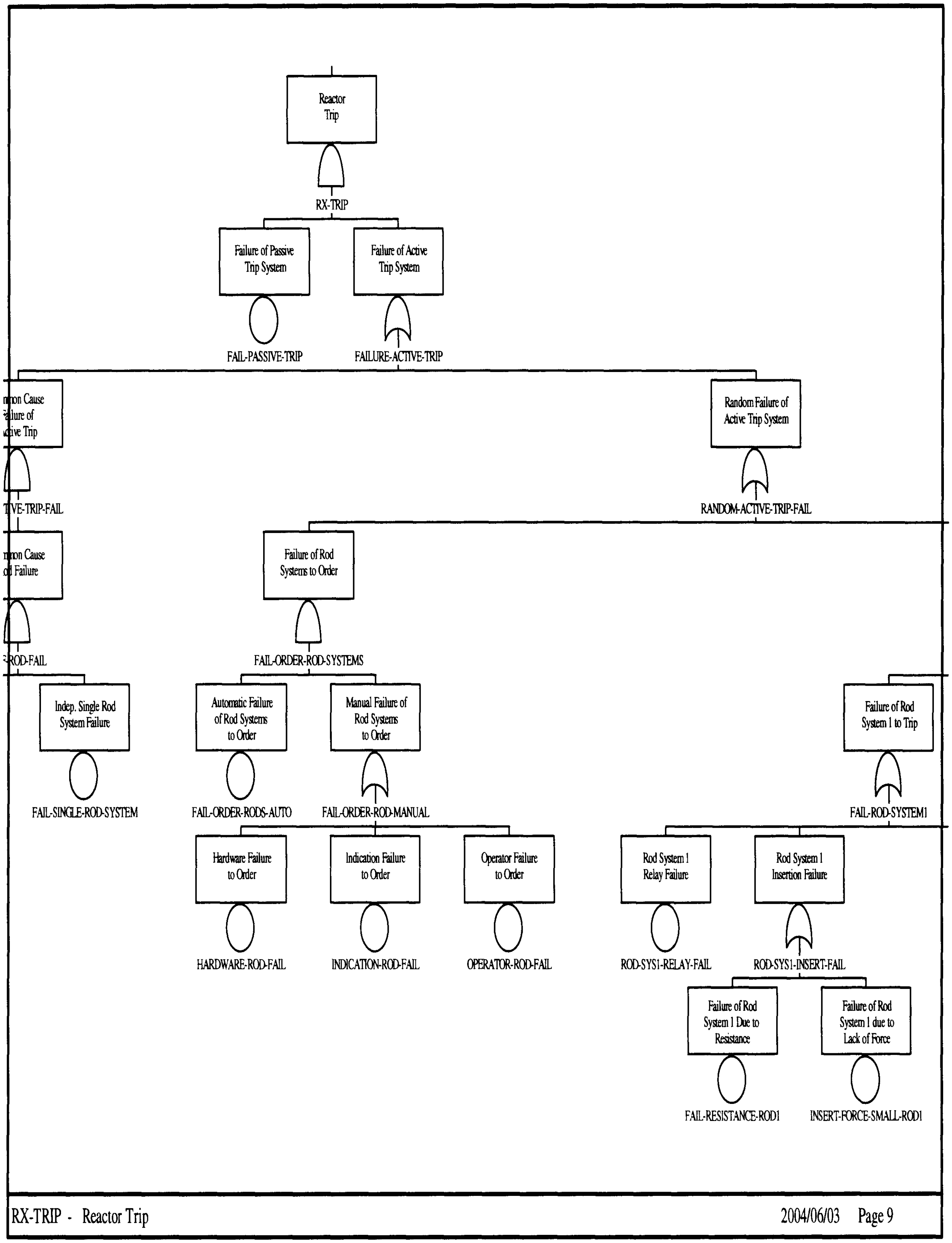


Figure IV-4 Fault Tree for Reactor Trip in GFR: Zoom 2

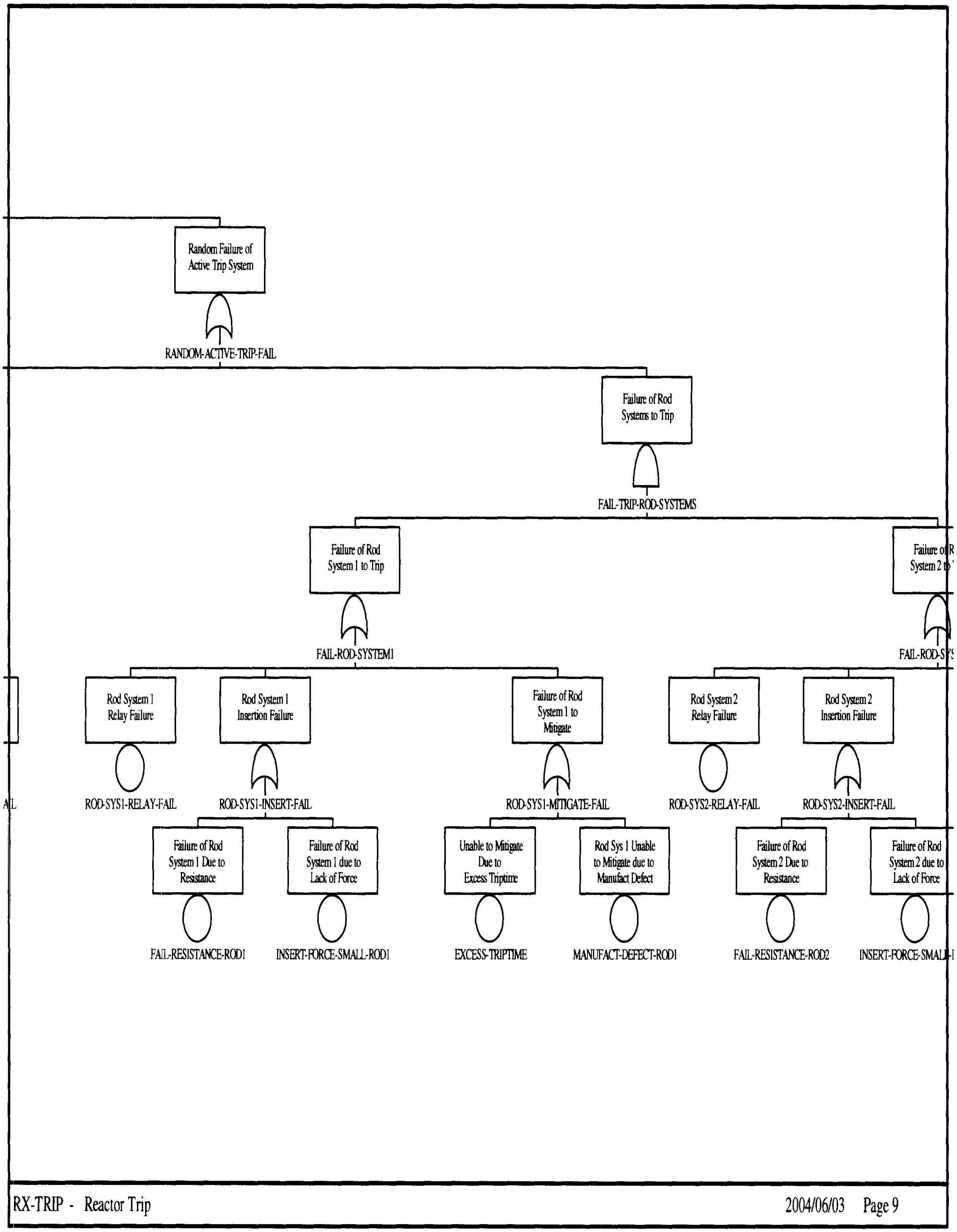

Random Failure of Active Trip System
RANDOM-ACTIVE-TRIP-FAIL
Failure of Rod Systems to Trip
FAIL-TRIP-ROD-SYSTEMS
Failure of Rod System 1 to Trip
FAIL-ROD-SYSTEM1
Failure of R System 2 to
FAIL-ROD-SYS
AL
Rod System 1 Relay Failure
ROD-SYS1-RELAY-FAIL
Rod System 1 Insertion Failure
ROD-SYS1-INSERT-FAIL
Failure of Rod System 1 to Mitigate
ROD-SYS1-MITIGATE-FAIL
Rod System 2 Relay Failure
ROD-SYS2-RELAY-FAIL
Rod System 2 Insertion Failure
ROD-SYS2-INSERT-FAIL
Failure of Rod System 1 Due to Resistance
FAIL-RESISTANCE-ROD1
Failure of Rod System 1 due to Lack of Force
INSERT-FORCE-SMALL-ROD1
Unable to Mitigate Due to Excess Triptime
EXCESS-TRIPTIME
Rod Sys 1 Unable to Mitigate due to Manufact Defect
MANUFACT-DEFECT-ROD1
Failure of Rod System 2 Due to Resistance
FAIL-RESISTANCE-ROD2
Failure of Rod System 2 due to Lack of Force
INSERT-FORCE-SMALL-
RX-TRIP - Reactor Trip
2004/06/03 Page 9

Figure IV-5 Fault Tree for Reactor Trip in GFR: Zoom 3

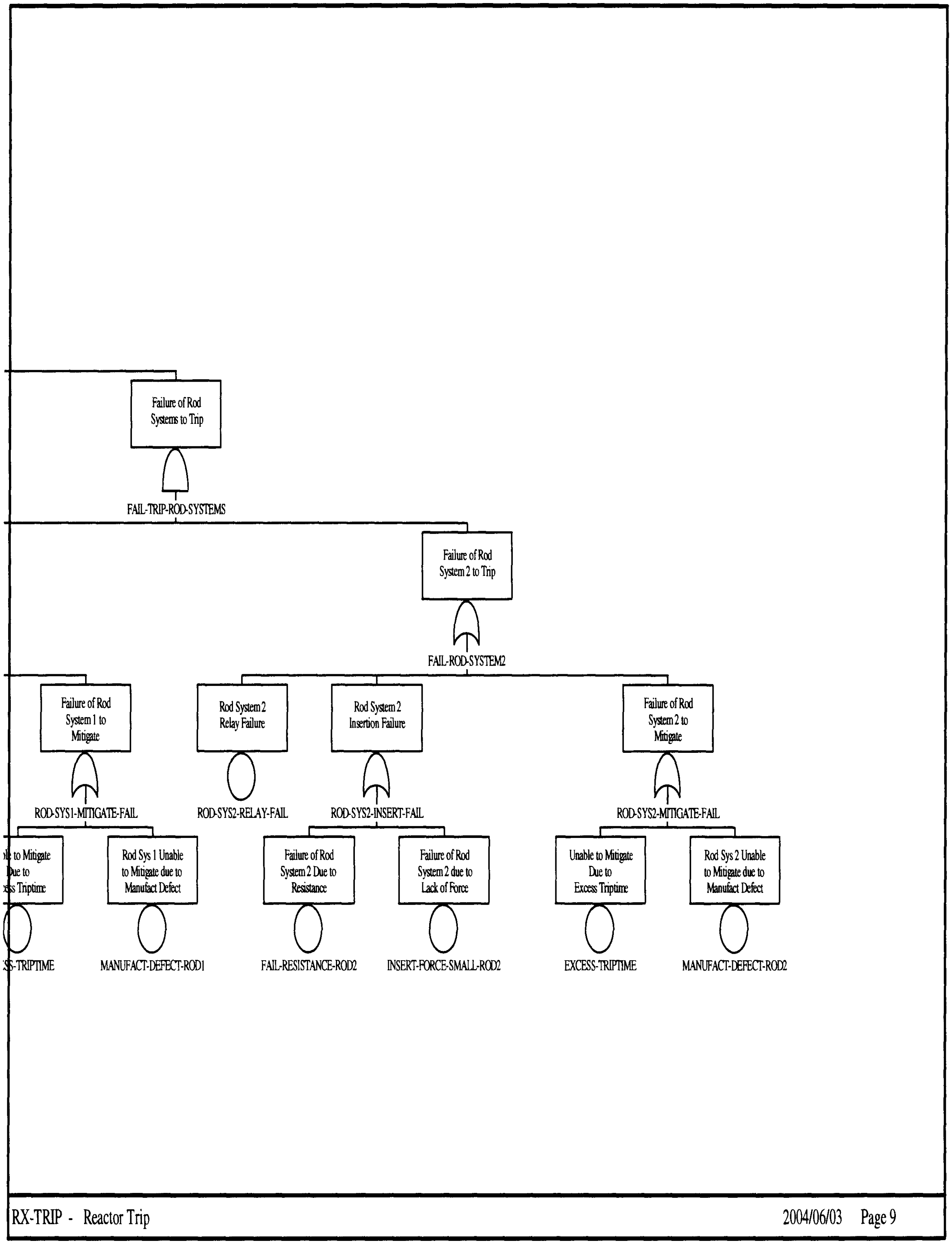

Failure of Rod Systems to Trip
FAIL-TRIP-ROD-SYSTEMS
Failure of Rod System 2 to Trip
FAIL-ROD-SYSTEM2
Failure of Rod System 1 to Mitigate
ROD-SYS1-MITIGATE-FAIL
Rod System 2 Relay Failure
ROD-SYS2-RELAY-FAIL
Rod System 2 Insertion Failure
ROD-SYS2-INSERT-FAIL
Failure of Rod System 2 to Mitigate
ROD-SYS2-MITIGATE-FAIL
le to Mitigate Due to ess Triptime
S-TRIPTIME
Rod Sys 1 Unable to Mitigate due to Manufact Defect
MANUFACT-DEFECT-ROD1
Failure of Rod System 2 Due to Resistance
FAIL-RESISTANCE-ROD2
Failure of Rod System 2 due to Lack of Force
INSERT-FORCE-SMALL-ROD2
Unable to Mitigate Due to Excess Triptime
EXCESS-TRIPTIME
Rod Sys 2 Unable to Mitigate due to Manufact Defect
MANUFACT-DEFECT-ROD2
RX-TRIP - Reactor Trip
2004/06/03 Page 9

Figure IV-6 Fault Tree for Reactor Trip in GFR: Zoom 4

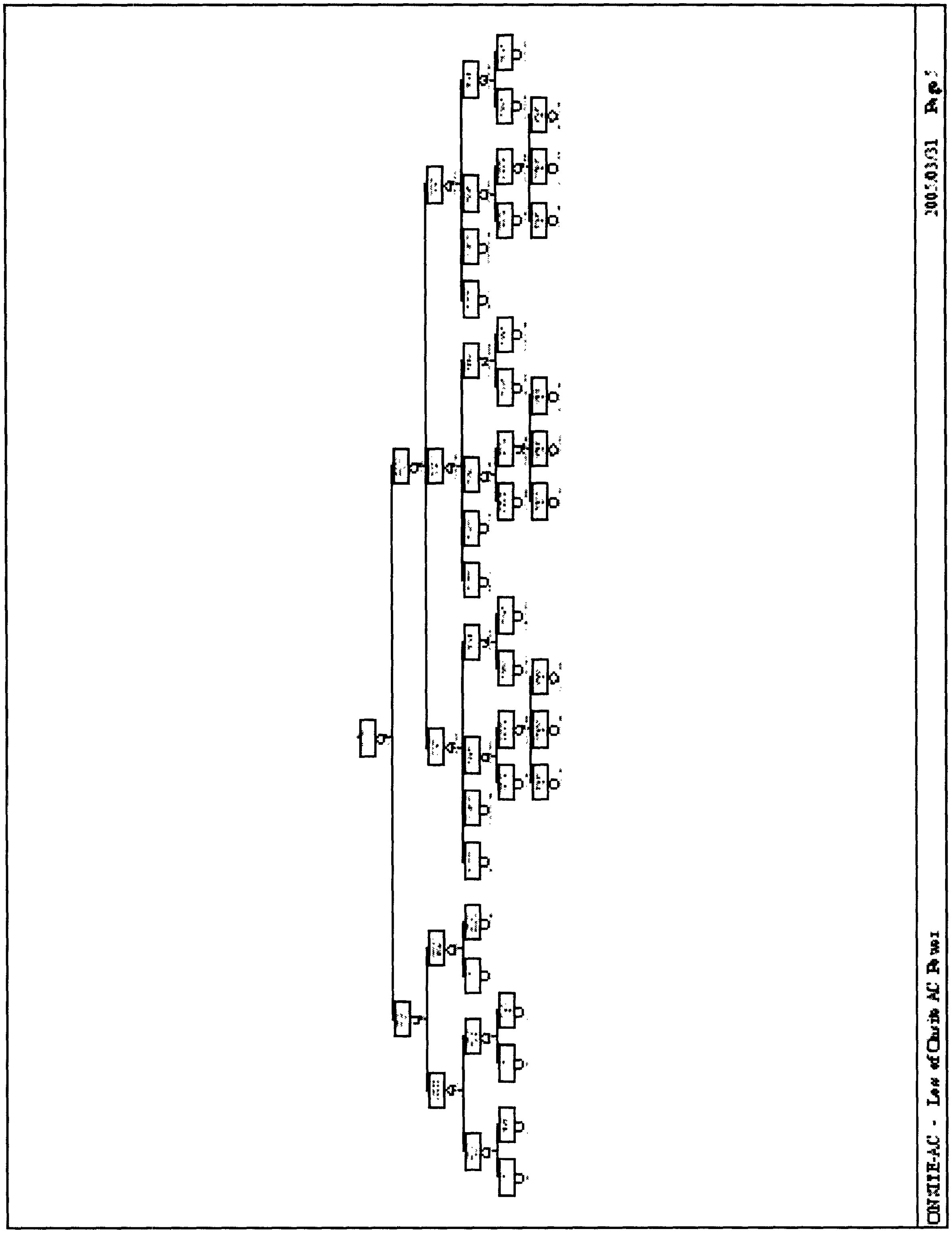


Figure IV-7 Fault Tree for Onsite AC Power in GFR: Following "Zoomed In" Figures for enlarged, readable sections of the Fault Tree

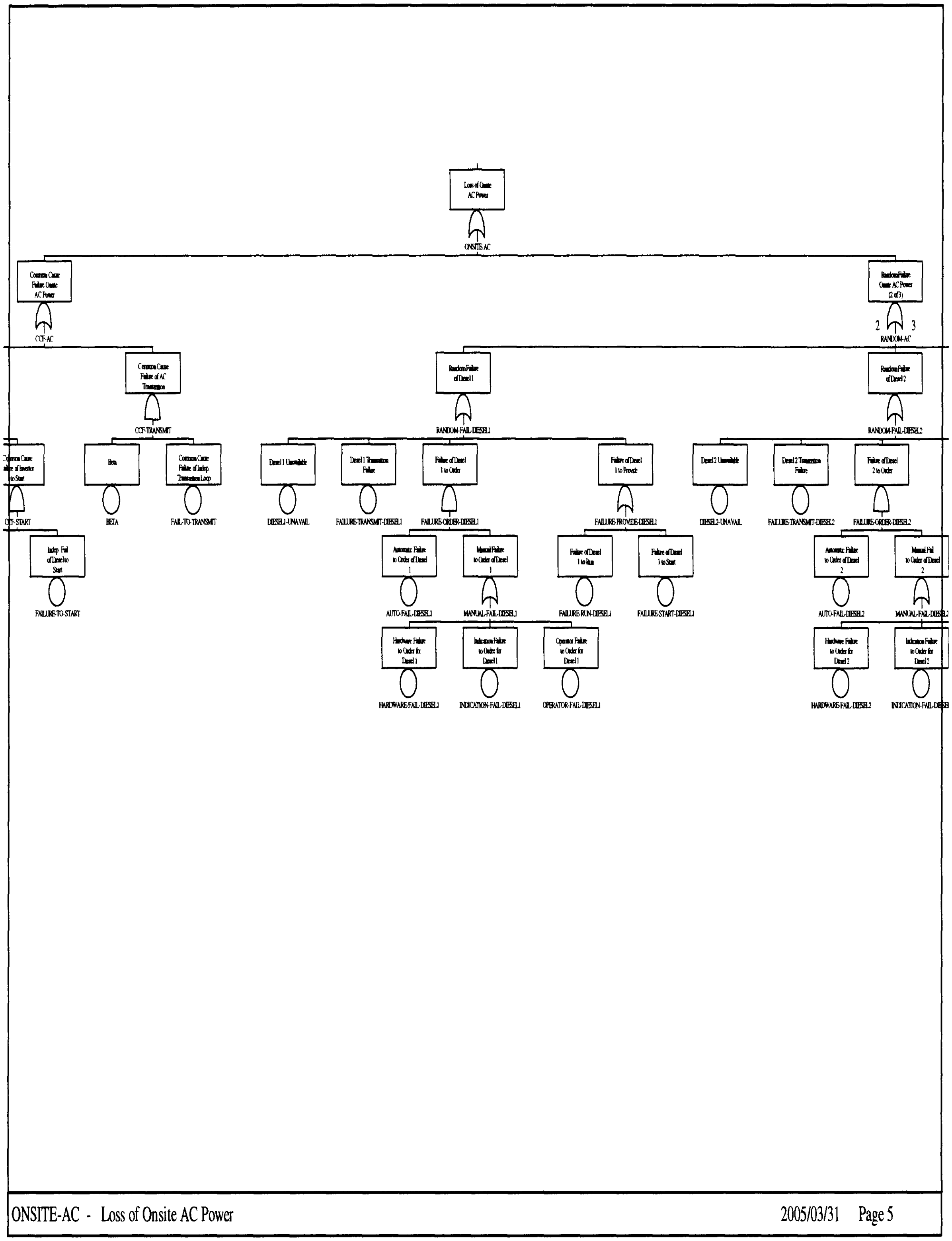

Loss of Onsite AC Power
ONSITE-AC
Common Cause Failure Onsite AC Power
CCF-AC
Random Failure Onsite AC Power (2 of 3)
2
3
RANDOM-AC
Common Cause Failure of AC Transmission
CCF-TRANSMIT
Random Failure of Diesel 1
RANDOM-FAIL-DIESEL1
Random Failure of Diesel 2
RANDOM-FAIL-DIESEL2
ommon Cause ailure of Inverter to Start
CCF-START
Beta
BETA
Common Cause Failure of Indep. Transmission Loop
FAIL-TO-TRANSMIT
Diesel 1 Unavailable
DIESEL1-UNAVAIL
Diesel 1 Transmission Failure
FAILURE-TRANSMIT-DIESEL1
Failure of Diesel 1 to Order
FAILURE-ORDER-DIESEL1
Failure of Diesel 1 to Provide
FAILURE-PROVIDE-DIESEL1
Diesel 2 Unavailable
DIESEL2-UNAVAIL
Diesel 2 Transmission Failure
FAILURE-TRANSMIT-DIESEL2
Failure of Diesel 2 to Order
FAILURE-ORDER-DIESEL2
Indep. Fail of Diesel to Start
FAILURE-TO-START
Automatic Failure to Order of Diesel 1
AUTO-FAIL-DIESEL1
Manual Failure to Order of Diesel 1
MANUAL-FAIL-DIESEL1
Failure of Diesel 1 to Run
FAILURE-RUN-DIESEL1
Failure of Diesel 1 to Start
FAILURE-START-DIESEL1
Automatic Failure to Order of Diesel 2
AUTO-FAIL-DIESEL2
Manual Fail to Order of Diesel 2
MANUAL-FAIL-DIESEL2
Hardware Failure to Order for Diesel 1
HARDWARE-FAIL-DIESEL1
Indication Failure to Order for Diesel 1
INDICATION-FAIL-DIESEL1
Operator Failure to Order for Diesel 1
OPERATOR-FAIL-DIESEL1
Hardware Failure to Order for Diesel 2
HARDWARE-FAIL-DIESEL2
Indication Failure to Order for Diesel 2
INDICATION-FAIL-DIESE
ONSITE-AC - Loss of Onsite AC Power
2005/03/31
Page 5

Figure IV-8 Fault Tree for Onsite AC Power in GFR: Zoom 1

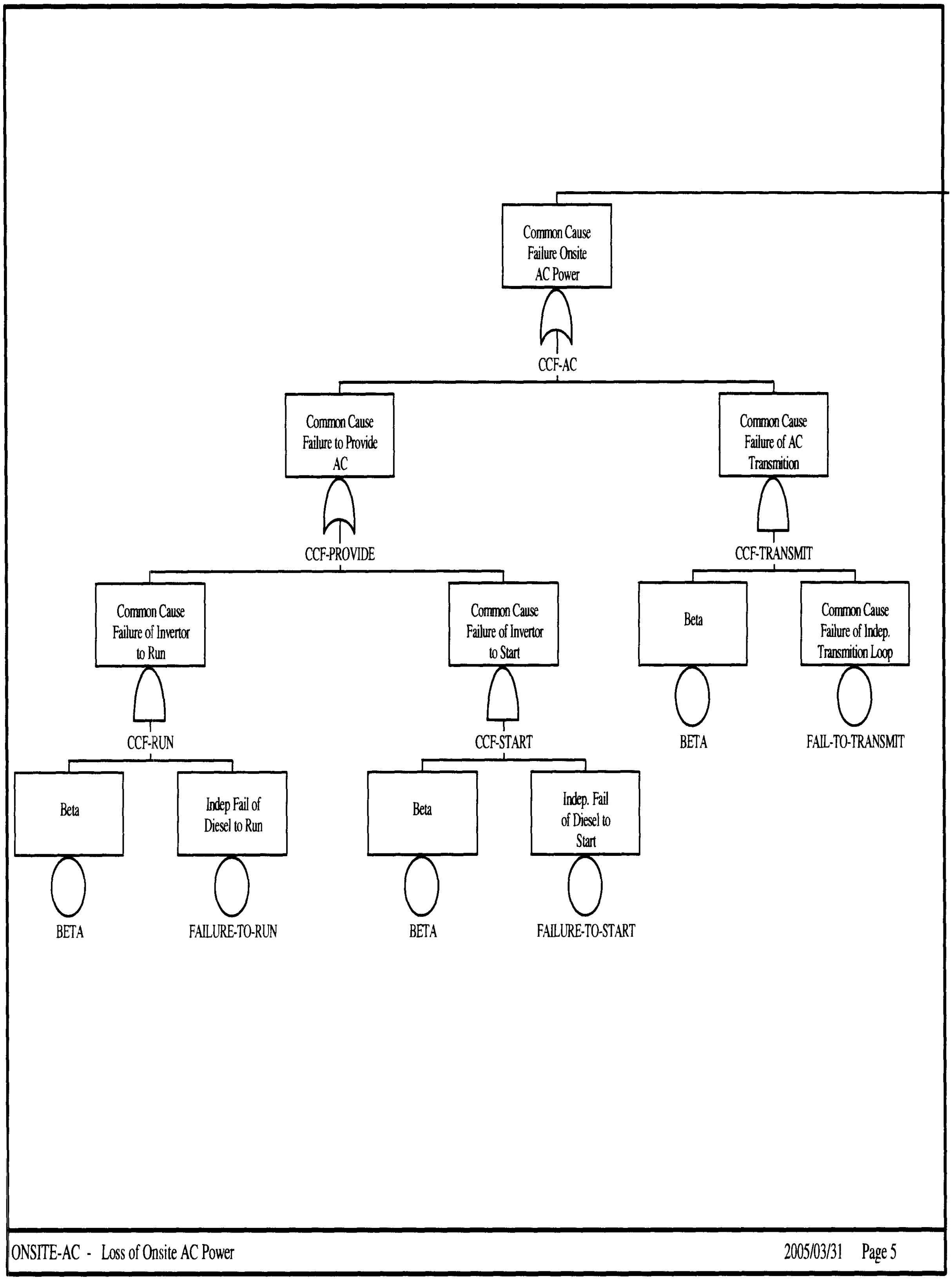

Common Cause Failure Onsite AC Power
CCF-AC
Common Cause Failure to Provide AC
CCF-PROVIDE
Common Cause Failure of AC Transmition
CCF-TRANSMIT
Common Cause Failure of Invertor to Run
CCF-RUN
Common Cause Failure of Invertor to Start
CCF-START
Beta
BETA
Common Cause Failure of Indep. Transmition Loop
FAIL-TO-TRANSMIT
Beta
BETA
Indep Fail of Diesel to Run
FAILURE-TO-RUN
Beta
BETA
Indep. Fail of Diesel to Start
FAILURE-TO-START
ONSITE-AC - Loss of Onsite AC Power
2005/03/31 Page 5

Figure IV-9 Fault Tree for Onsite AC Power in GFR: Zoom 2

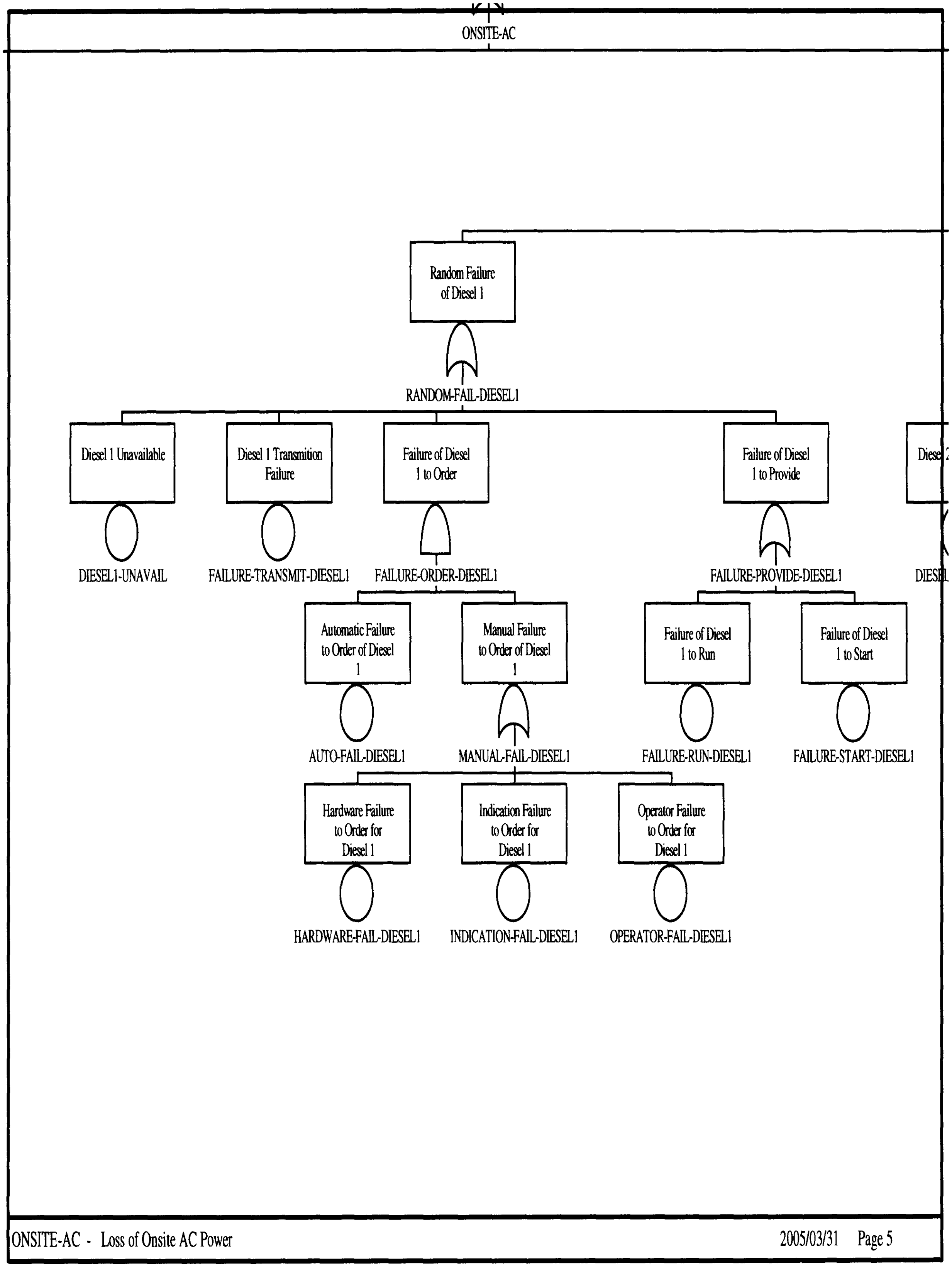

ONSITE-AC
Random Failure of Diesel 1
RANDOM-FAIL-DIESEL1
Diesel 1 Unavailable
DIESEL1-UNAVAIL
Diesel 1 Transmition Failure
FAILURE-TRANSMIT-DIESEL1
Failure of Diesel 1 to Order
FAILURE-ORDER-DIESEL1
Failure of Diesel 1 to Provide
FAILURE-PROVIDE-DIESEL1
Diese
DIES
Automatic Failure to Order of Diesel 1
AUTO-FAIL-DIESEL1
Manual Failure to Order of Diesel 1
MANUAL-FAIL-DIESEL1
Failure of Diesel 1 to Run
FAILURE-RUN-DIESEL1
Failure of Diesel 1 to Start
FAILURE-START-DIESEL1
Hardware Failure to Order for Diesel 1
HARDWARE-FAIL-DIESEL1
Indication Failure to Order for Diesel 1
INDICATION-FAIL-DIESEL1
Operator Failure to Order for Diesel 1
OPERATOR-FAIL-DIESEL1
ONSITE-AC - Loss of Onsite AC Power
2005/03/31 Page 5

Figure IV-10 Fault Tree for Onsite AC Power in GFR: Zoom 3

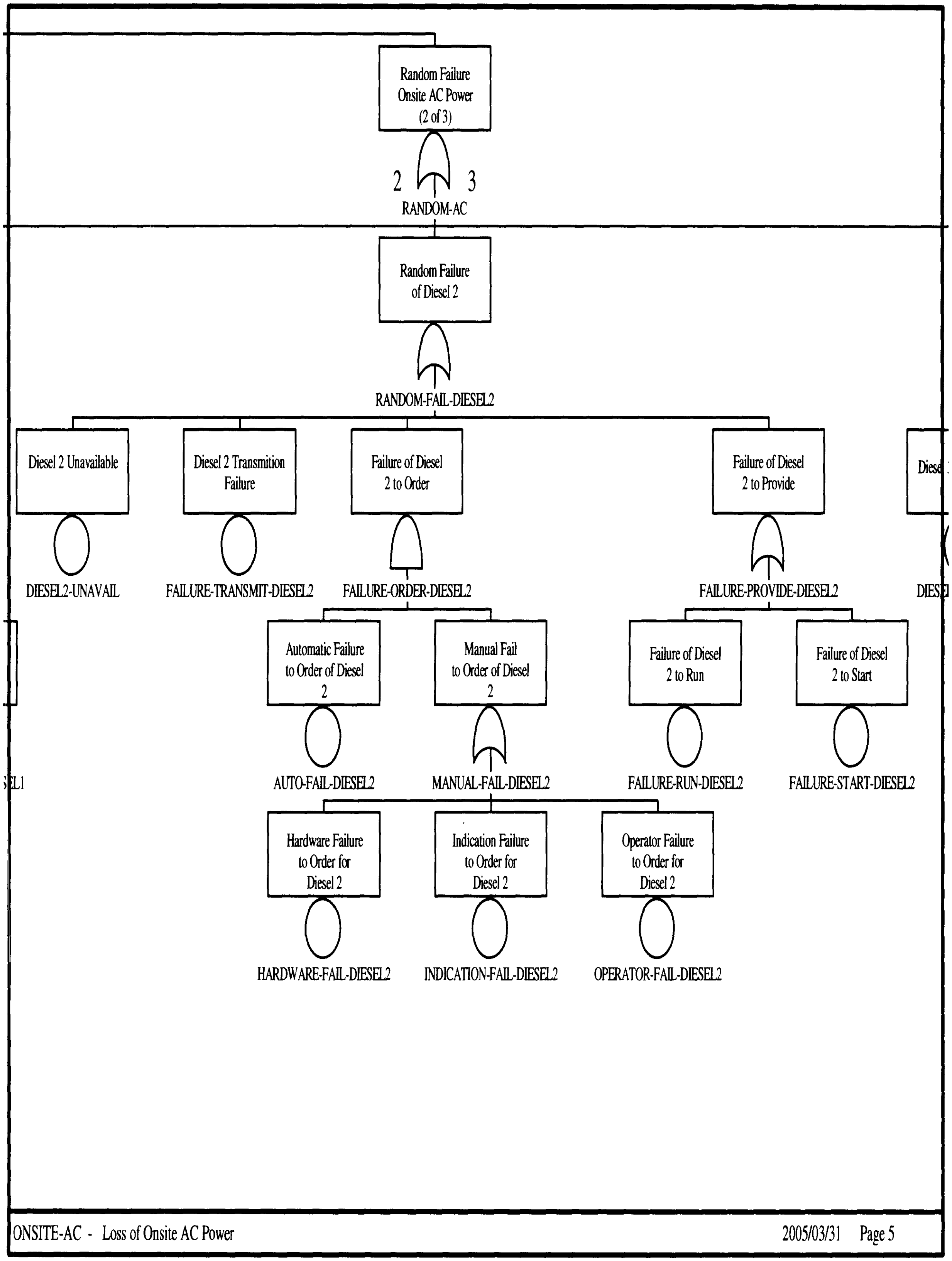


Figure IV-11 Fault Tree for Onsite AC Power in GFR: Zoom 4

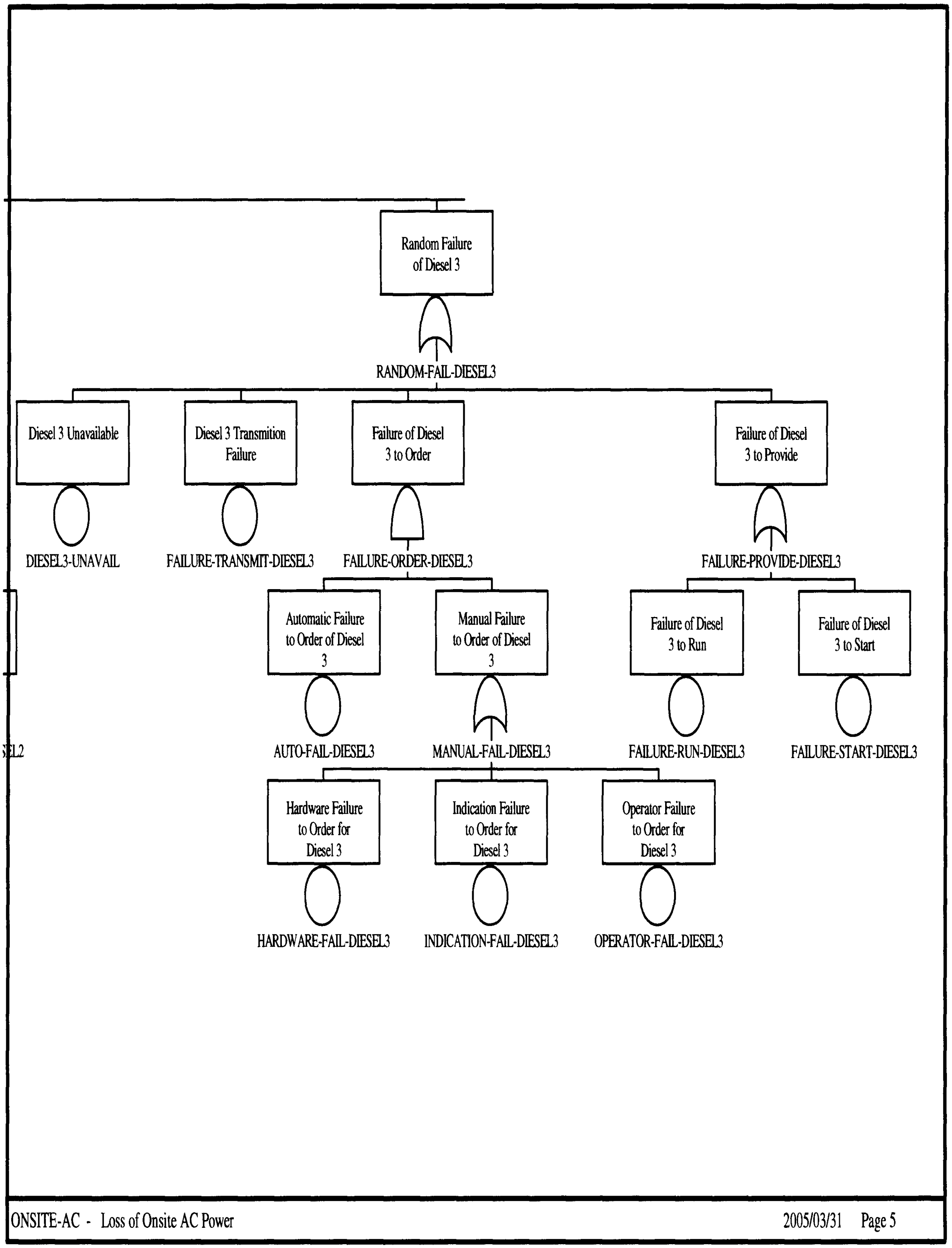

Random Failure of Diesel 3
RANDOM-FAIL-DIESEL3
Diesel 3 Unavailable
DIESEL3-UNAVAIL
Diesel 3 Transmition Failure
FAILURE-TRANSMIT-DIESEL3
Failure of Diesel 3 to Order
FAILURE-ORDER-DIESEL3
Failure of Diesel 3 to Provide
FAILURE-PROVIDE-DIESEL3
Automatic Failure to Order of Diesel 3
AUTO-FAIL-DIESEL3
Manual Failure to Order of Diesel 3
MANUAL-FAIL-DIESEL3
Failure of Diesel 3 to Run
FAILURE-RUN-DIESEL3
Failure of Diesel 3 to Start
FAILURE-START-DIESEL3
Hardware Failure to Order for Diesel 3
HARDWARE-FAIL-DIESEL3
Indication Failure to Order for Diesel 3
INDICATION-FAIL-DIESEL3
Operator Failure to Order for Diesel 3
OPERATOR-FAIL-DIESEL3
ONSITE-AC - Loss of Onsite AC Power
2005/03/31 Page 5

Figure IV-12 Fault Tree for Onsite AC Power in GFR: Zoom 5

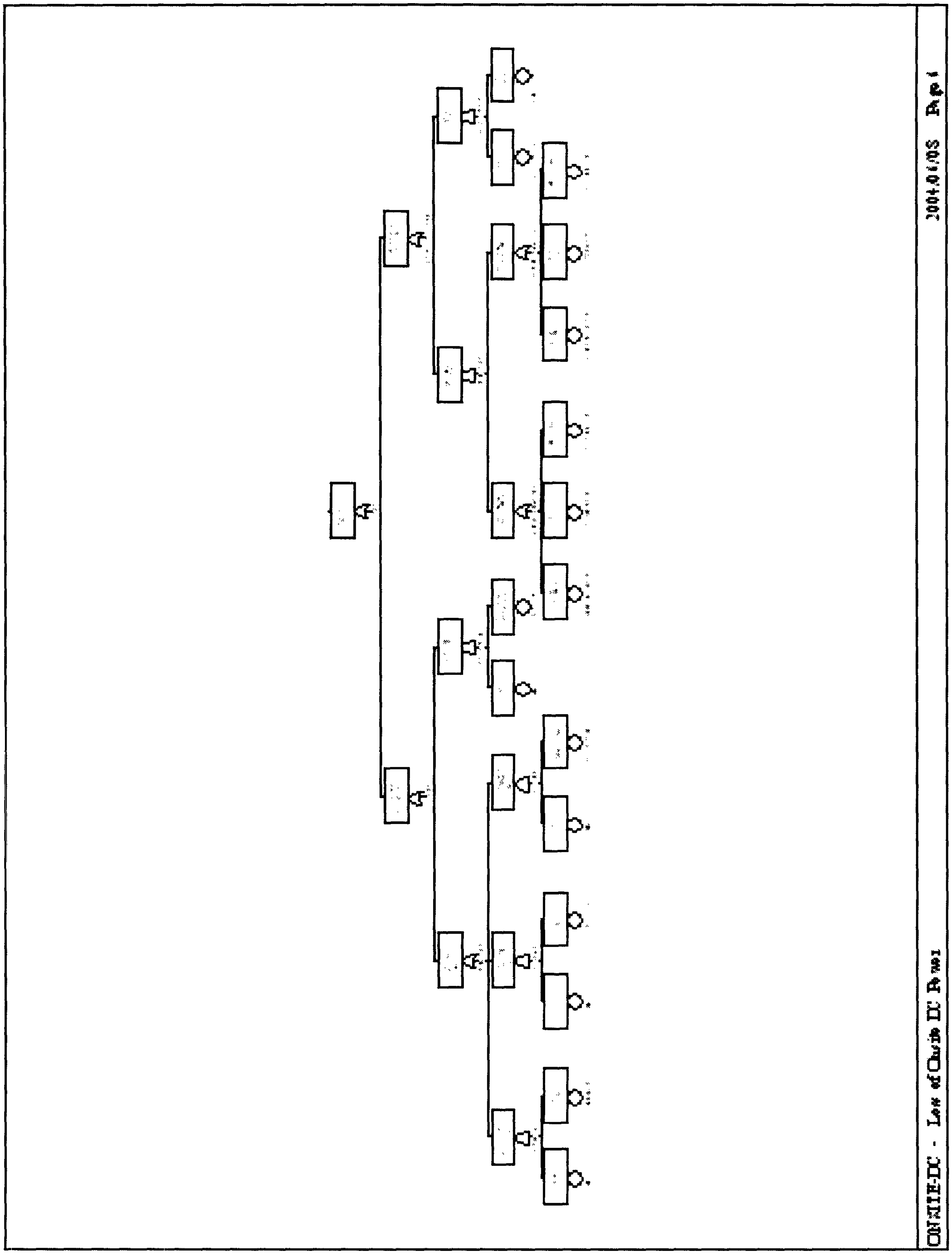


Figure IV-13 Fault Tree for Onsite DC Power in GFR: Following “Zoomed In” Figures for enlarged, readable sections of the Fault Tree

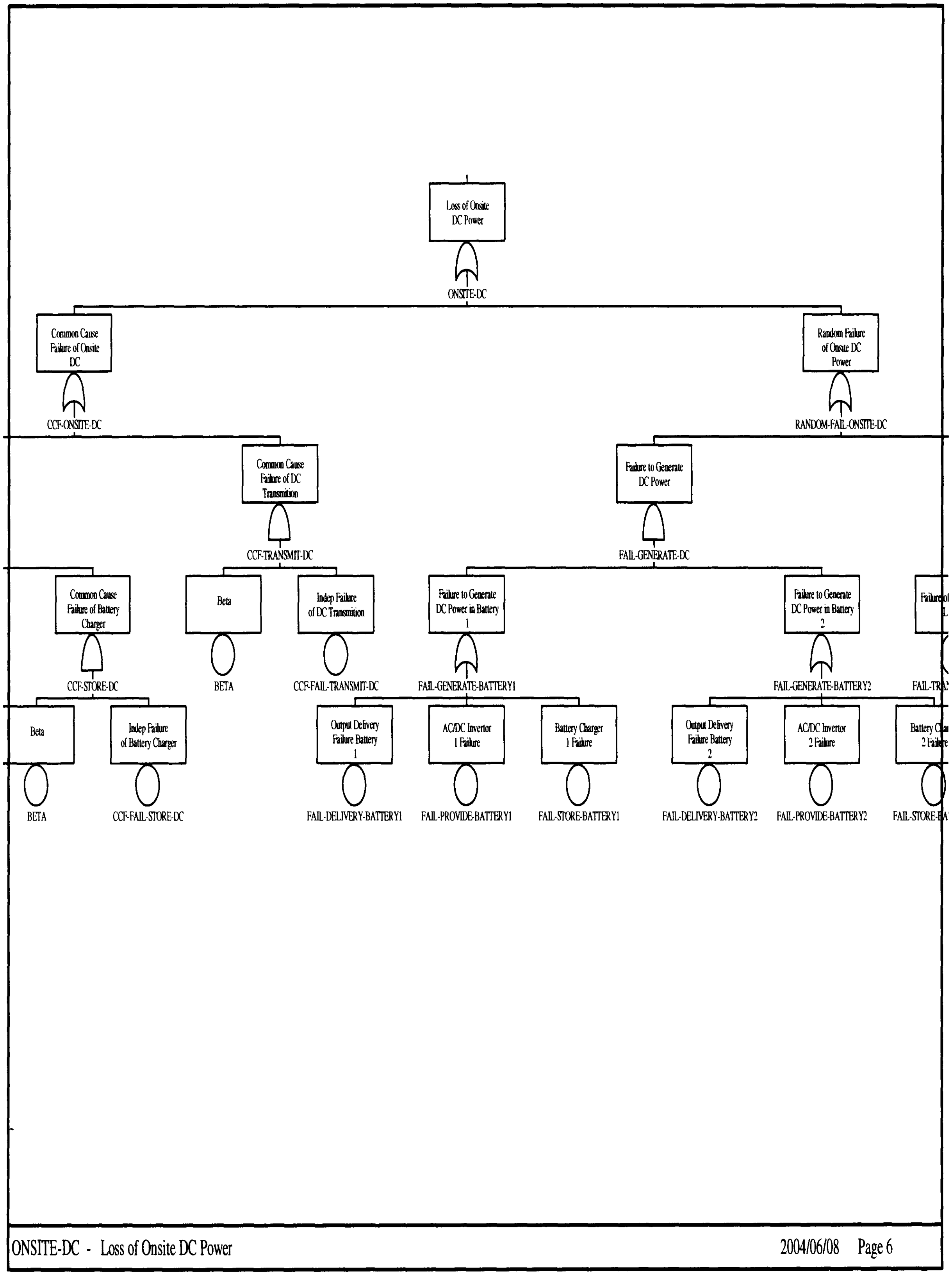

Loss of Onsite DC Power
ONSITE-DC
Common Cause Failure of Onsite DC
CCF-ONSITE-DC
Random Failure of Onsite DC Power
RANDOM-FAIL-ONSITE-DC
Common Cause Failure of DC Transmition
CCF-TRANSMIT-DC
Failure to Generate DC Power
FAIL-GENERATE-DC
Common Cause Failure of Battery Charger
CCF-STORE-DC
Beta
BETA
Indep Failure of DC Transmition
CCF-FAIL-TRANSMIT-DC
Failure to Generate DC Power in Battery 1
FAIL-GENERATE-BATTERY1
Failure to Generate DC Power in Battery 2
FAIL-GENERATE-BATTERY2
Failure of
FAIL-TRA
Beta
BETA
Indep Failure of Battery Charger
CCF-FAIL-STORE-DC
Output Delivery Failure Battery 1
FAIL-DELIVERY-BATTERY1
AC/DC Invertor 1 Failure
FAIL-PROVIDE-BATTERY1
Battery Charger 1 Failure
FAIL-STORE-BATTERY1
Output Delivery Failure Battery 2
FAIL-DELIVERY-BATTERY2
AC/DC Invertor 2 Failure
FAIL-PROVIDE-BATTERY2
Battery Char 2 Failure
FAIL-STORE-BA
ONSITE-DC - Loss of Onsite DC Power
2004/06/08 Page 6

Figure IV-14 Fault Tree for Onsite DC Power in GFR: Zoom 1

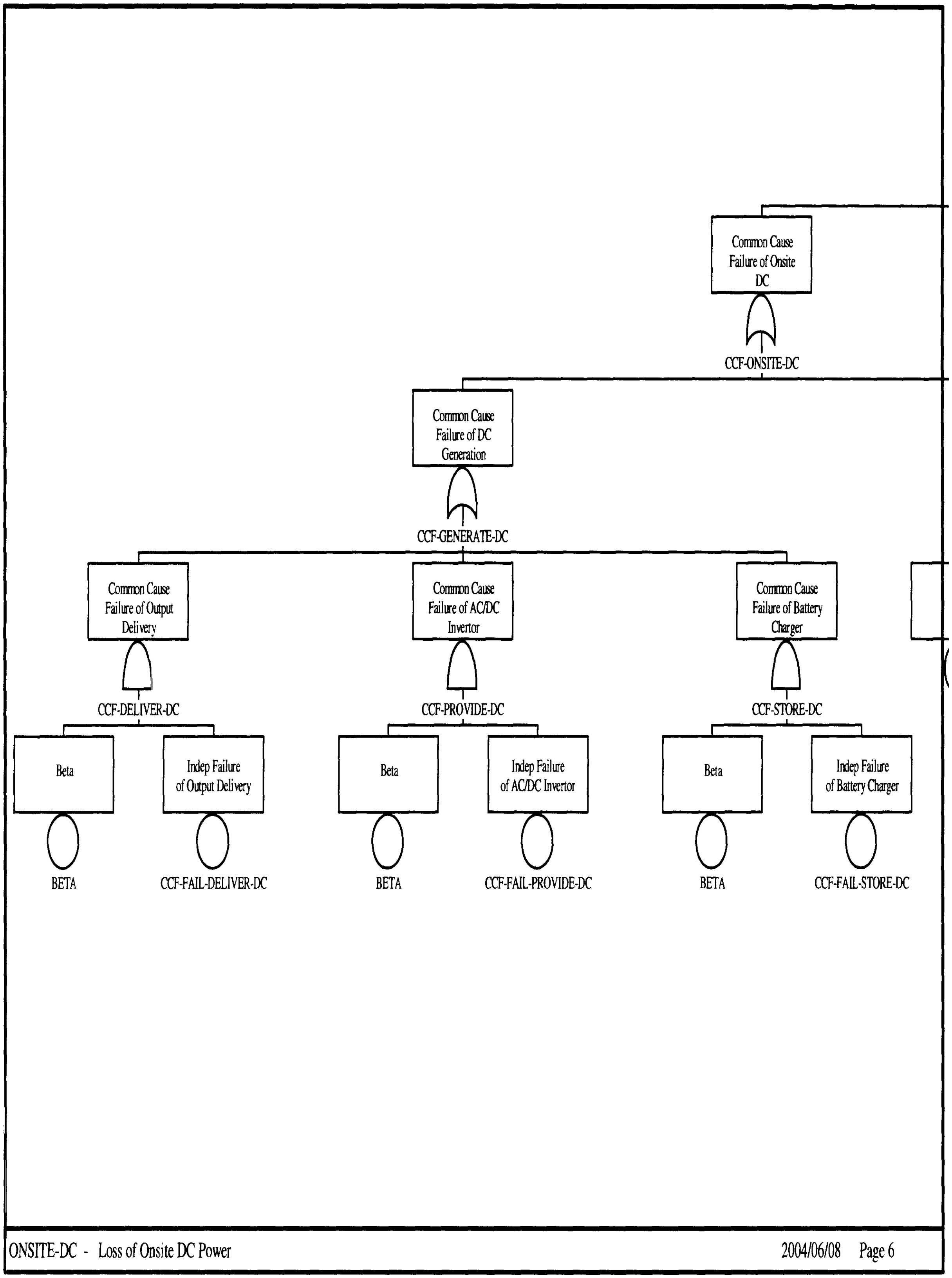

Common Cause Failure of Onsite DC
CCF-ONSITE-DC
Common Cause Failure of DC Generation
CCF-GENERATE-DC
Common Cause Failure of Output Delivery
CCF-DELIVER-DC
Common Cause Failure of AC/DC Invertor
CCF-PROVIDE-DC
Common Cause Failure of Battery Charger
CCF-STORE-DC
Beta
BETA
Indep Failure of Output Delivery
CCF-FAIL-DELIVER-DC
Beta
BETA
Indep Failure of AC/DC Invertor
CCF-FAIL-PROVIDE-DC
Beta
BETA
Indep Failure of Battery Charger
CCF-FAIL-STORE-DC
ONSITE-DC - Loss of Onsite DC Power
2004/06/08 Page 6

Figure IV-15 Fault Tree for Onsite DC Power in GFR: Zoom 2

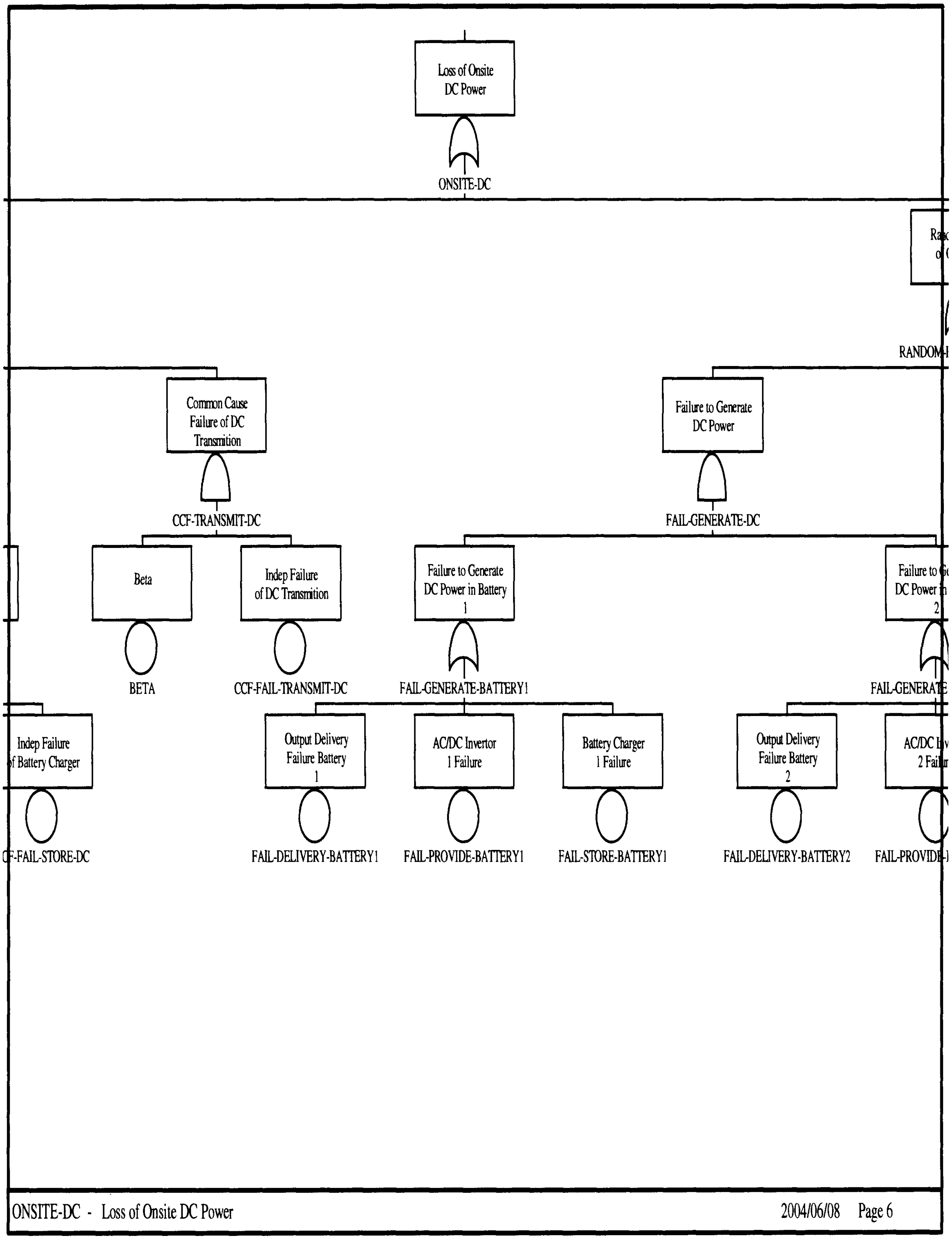

Loss of Onsite DC Power
ONSITE-DC
Ra
o
RANDOM-
Common Cause Failure of DC Transmition
CCF-TRANSMIT-DC
Failure to Generate DC Power
FAIL-GENERATE-DC
Beta
BETA
Indep Failure of DC Transmition
CCF-FAIL-TRANSMIT-DC
Failure to Generate DC Power in Battery 1
FAIL-GENERATE-BATTERY1
Failure to G DC Power in 2
FAIL-GENERATE
Indep Failure f Battery Charger
F-FAIL-STORE-DC
Output Delivery Failure Battery 1
FAIL-DELIVERY-BATTERY1
AC/DC Invertor 1 Failure
FAIL-PROVIDE-BATTERY1
Battery Charger 1 Failure
FAIL-STORE-BATTERY1
Output Delivery Failure Battery 2
FAIL-DELIVERY-BATTERY2
AC/DC I 2 Fail
FAIL-PROVIDE-
ONSITE-DC - Loss of Onsite DC Power
2004/06/08 Page 6

Figure IV-16 Fault Tree for Onsite DC Power in GFR: Zoom 3

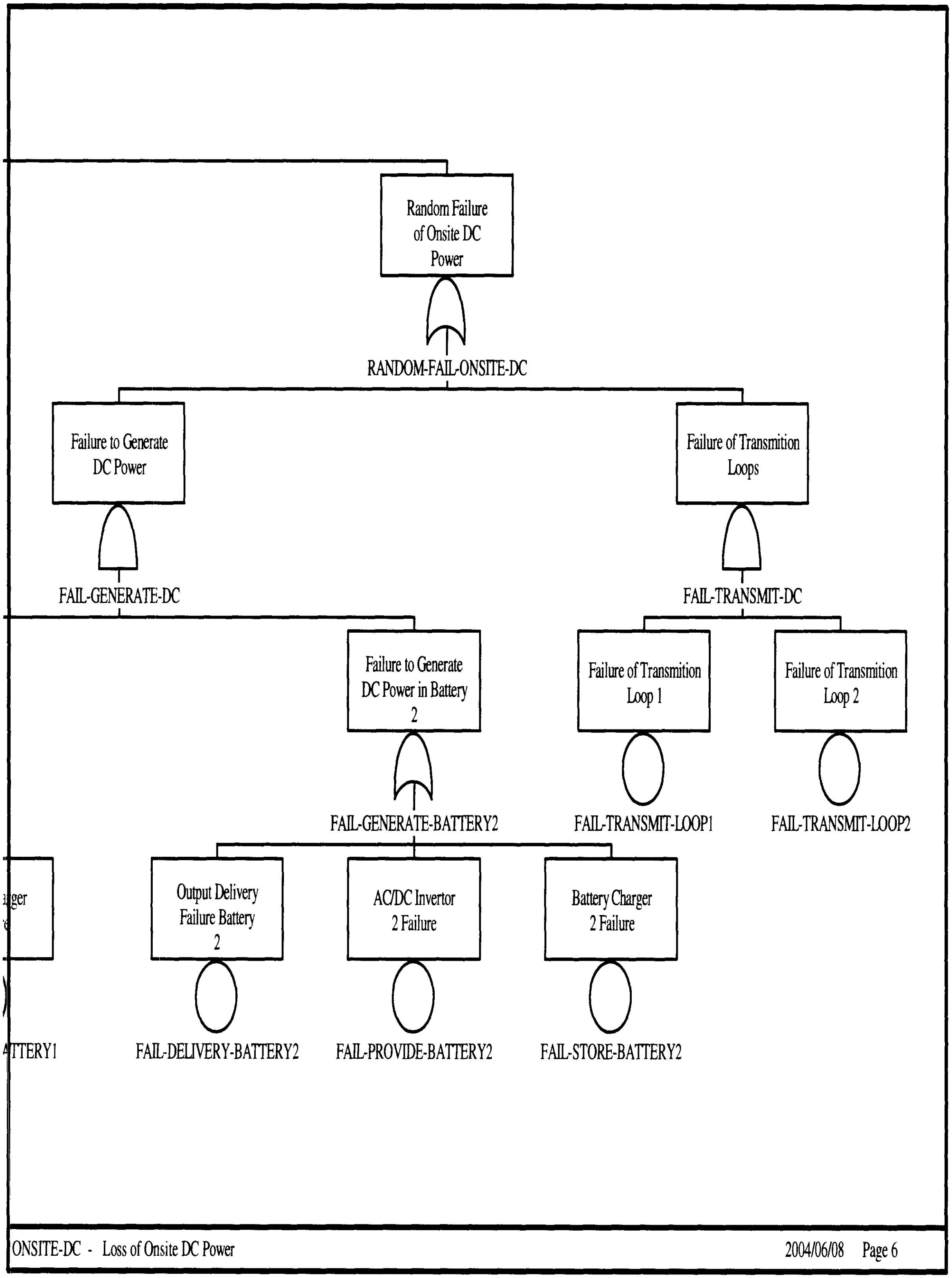

Random Failure of Onsite DC Power
RANDOM-FAIL-ONSITE-DC
Failure to Generate DC Power
FAIL-GENERATE-DC
Failure of Transmition Loops
FAIL-TRANSMIT-DC
Failure to Generate DC Power in Battery 2
FAIL-GENERATE-BATTERY2
Failure of Transmition Loop 1
FAIL-TRANSMIT-LOOP1
Failure of Transmition Loop 2
FAIL-TRANSMIT-LOOP2
ger
TTERY1
Output Delivery Failure Battery 2
FAIL-DELIVERY-BATTERY2
AC/DC Invertor 2 Failure
FAIL-PROVIDE-BATTERY2
Battery Charger 2 Failure
FAIL-STORE-BATTERY2
ONSITE-DC - Loss of Onsite DC Power
2004/06/08 Page 6

Figure IV-17 Fault Tree for Onsite DC Power in GFR: Zoom 4

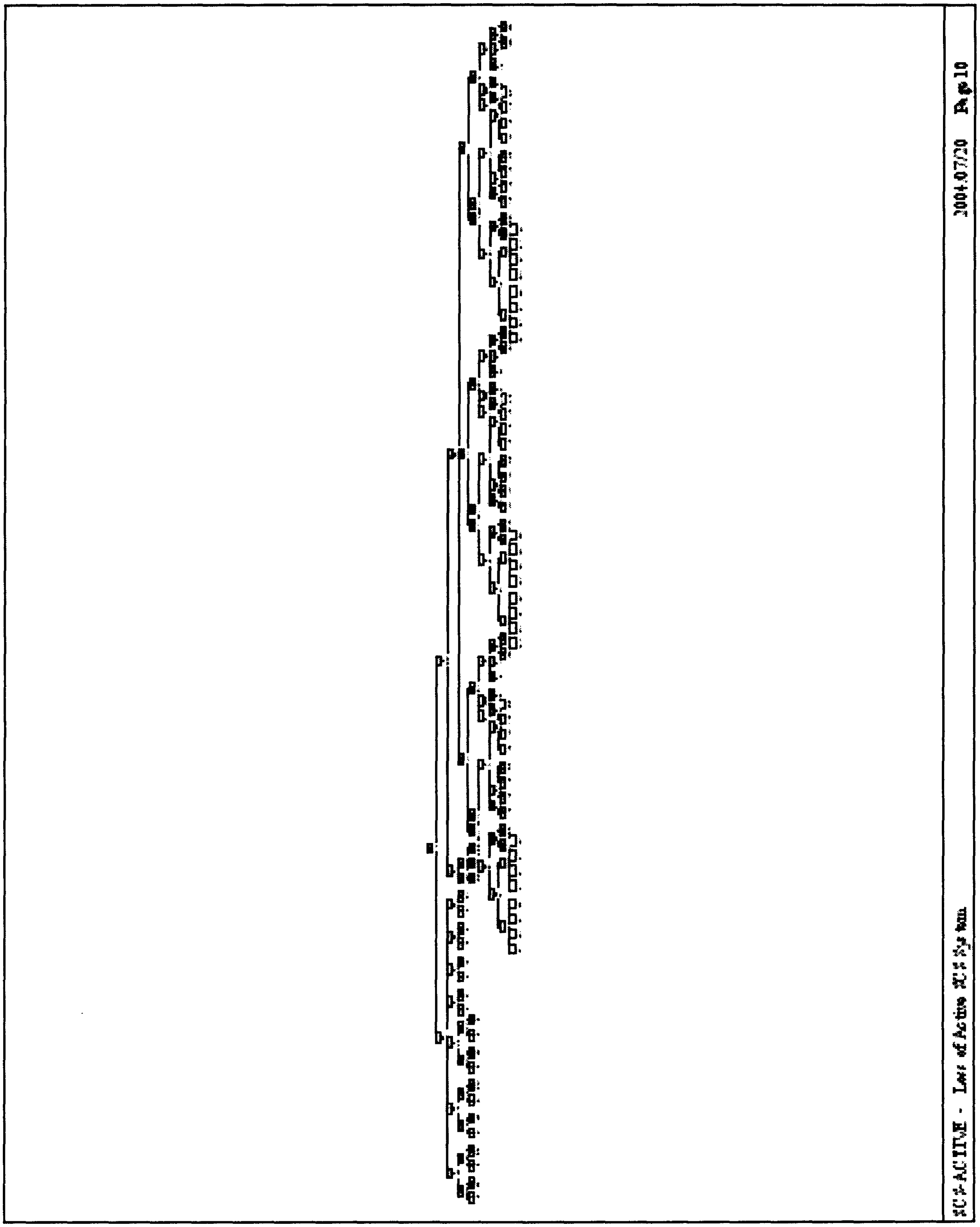


Figure IV-18 Fault Tree for Active SCS System in GFR: Following "Zoomed In" Figures for enlarged, readable sections of the Fault Tree

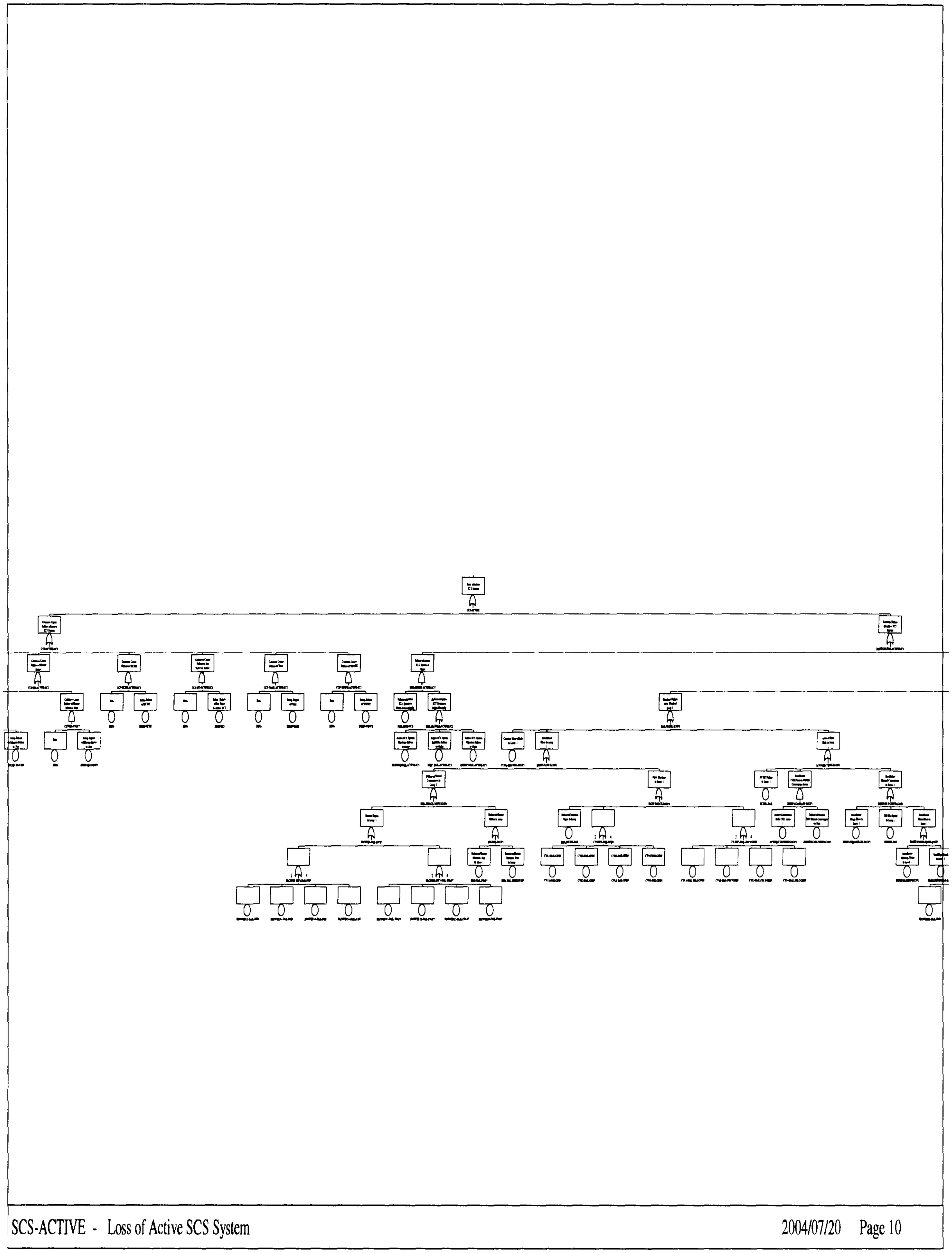


Figure IV-19 Fault Tree for Active SCS System in GFR: Zoom 1

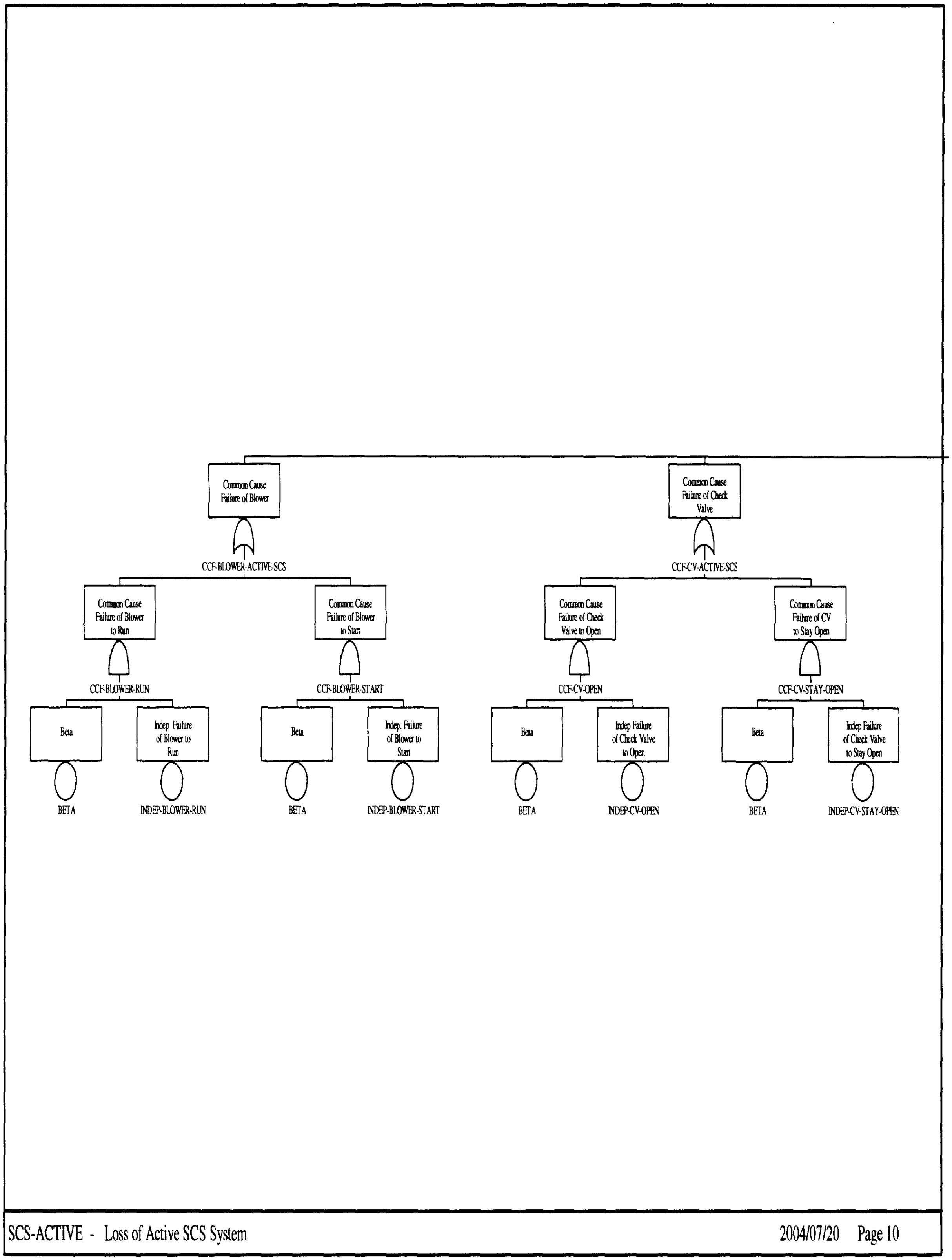

Common Cause Failure of Blower
CCF-BLOWER-ACTIVE-SCS
Common Cause Failure of Check Valve
CCF-CV-ACTIVE-SCS
Common Cause Failure of Blower to Run
CCF-BLOWER-RUN
Common Cause Failure of Blower to Start
CCF-BLOWER-START
Common Cause Failure of Check Valve to Open
CCF-CV-OPEN
Common Cause Failure of CV to Stay Open
CCF-CV-STAY-OPEN
Beta
BETA
Indep Failure of Blower to Run
INDEP-BLOWER-RUN
Beta
BETA
Indep. Failure of Blower to Start
INDEP-BLOWER-START
Beta
BETA
Indep Failure of Check Valve to Open
INDEP-CV-OPEN
Beta
BETA
Indep Failure of Check Valve to Stay Open
INDEP-CV-STAY-OPEN
SCS-ACTIVE - Loss of Active SCS System
2004/07/20 Page 10

Figure IV-20 Fault Tree for Active SCS System in GFR: Zoom 2

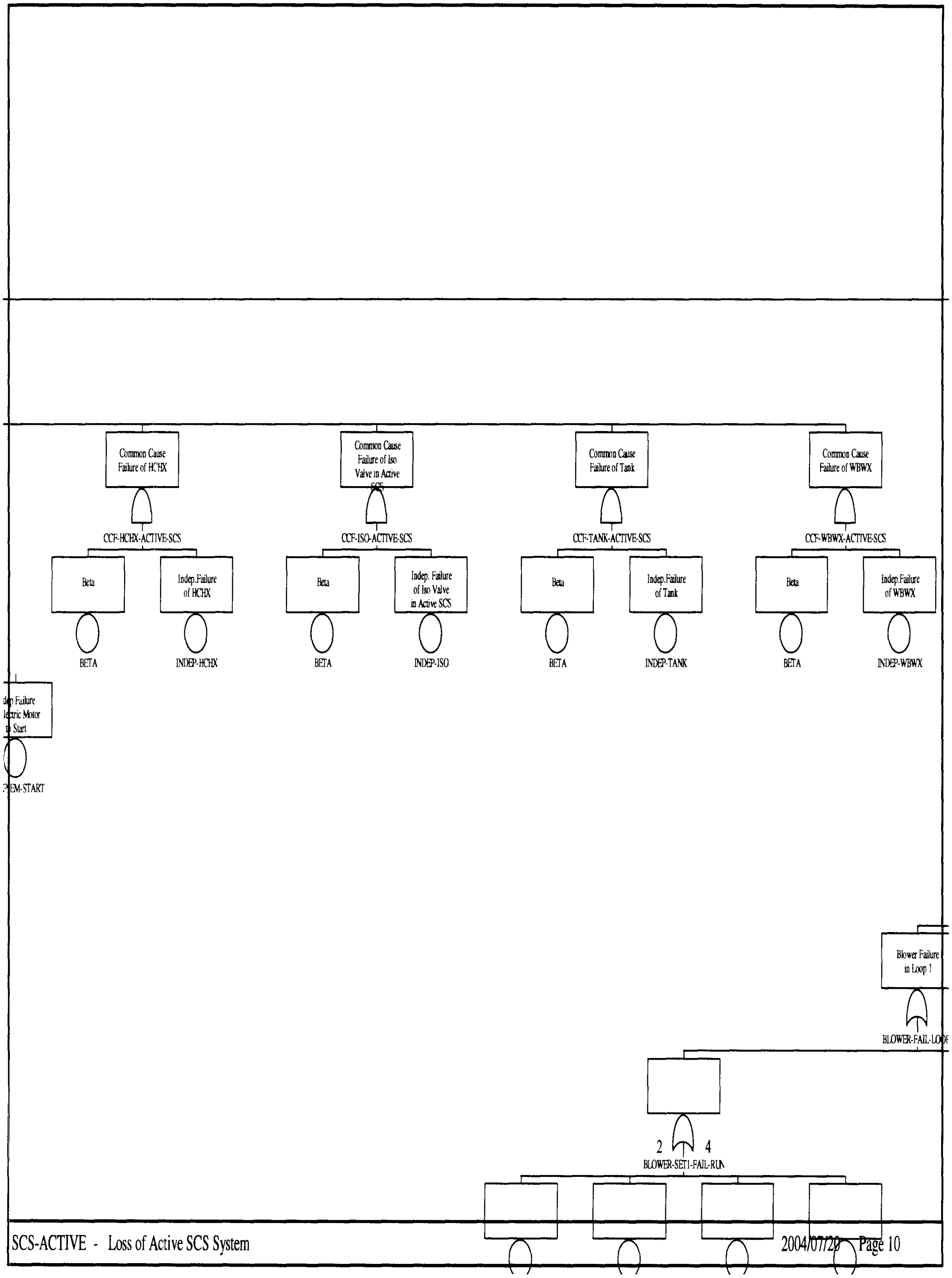


Figure IV-21 Fault Tree for Active SCS System in GFR: Zoom 3

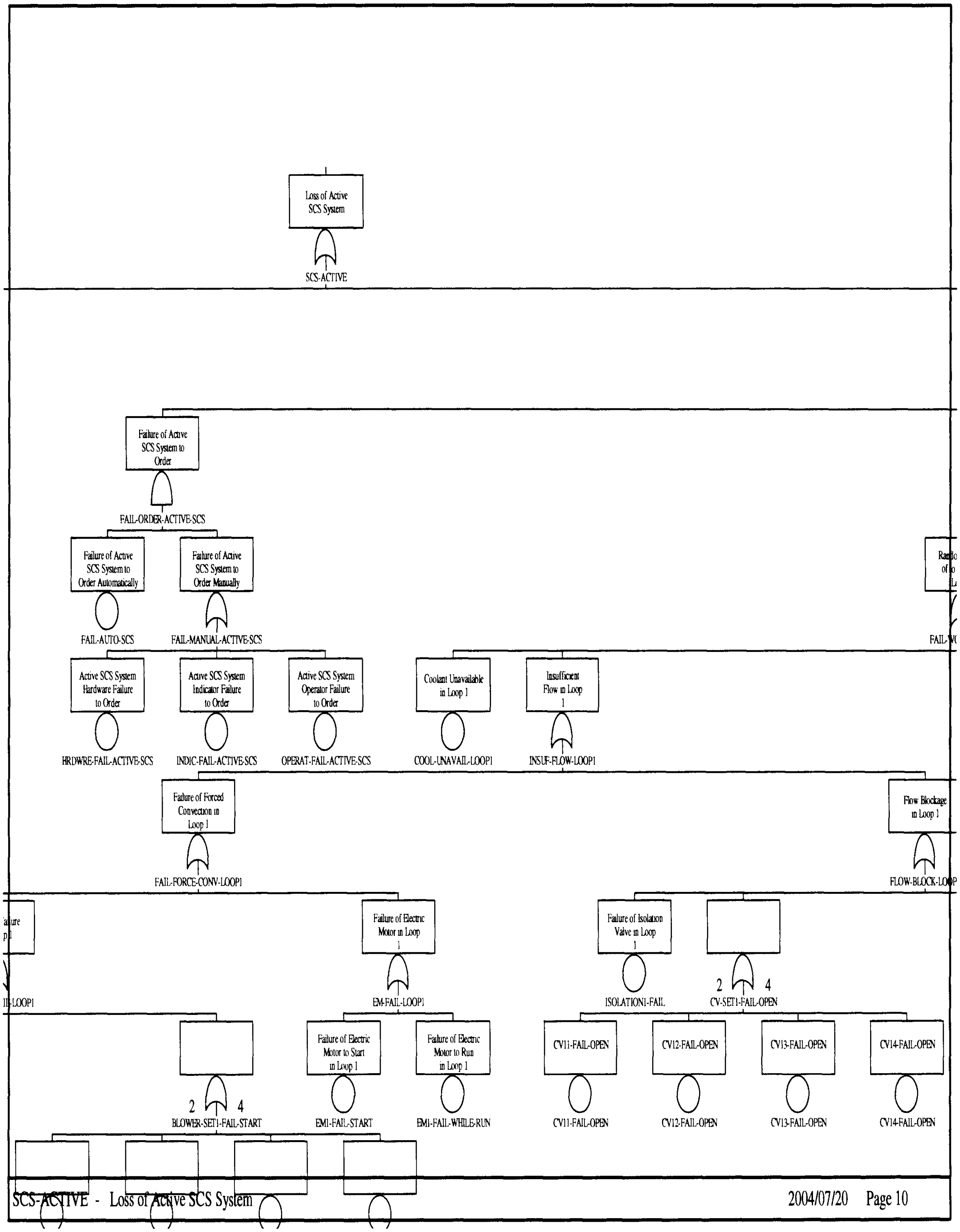

Loss of Active SCS System
SCS-ACTIVE
Failure of Active SCS System to Order
FAIL-ORDER-ACTIVE-SCS
Failure of Active SCS System to Order Automatically
FAIL-AUTO-SCS
Failure of Active SCS System to Order Manually
FAIL-MANUAL-ACTIVE-SCS
Active SCS System Hardware Failure to Order
HRDWRE-FAIL-ACTIVE-SCS
Active SCS System Indicator Failure to Order
INDIC-FAIL-ACTIVE-SCS
Active SCS System Operator Failure to Order
OPERAT-FAIL-ACTIVE-SCS
Coolant Unavailable in Loop 1
COOL-UNAVAIL-LOOP1
Insufficient Flow in Loop 1
INSUF-FLOW-LOOP1
Failure of Forced Convection in Loop 1
FAIL-FORCE-CONV-LOOP1
Flow Blockage in Loop 1
FLOW-BLOCK-LOOP
Failure of Electric Motor in Loop 1
EM-FAIL-LOOP1
Failure of Isolation Valve in Loop 1
ISOLATION1-FAIL
2
4
CV-SET1-FAIL-OPEN
2
4
BLOWER-SET1-FAIL-START
Failure of Electric Motor to Start in Loop 1
EM1-FAIL-START
Failure of Electric Motor to Run in Loop 1
EM1-FAIL-WHILE-RUN
CV11-FAIL-OPEN
CV11-FAIL-OPEN
CV12-FAIL-OPEN
CV12-FAIL-OPEN
CV13-FAIL-OPEN
CV13-FAIL-OPEN
CV14-FAIL-OPEN
CV14-FAIL-OPEN
SCS-ACTIVE - Loss of Active SCS System
2004/07/20 Page 10

Figure IV-22 Fault Tree for Active SCS System in GFR: Zoom 4

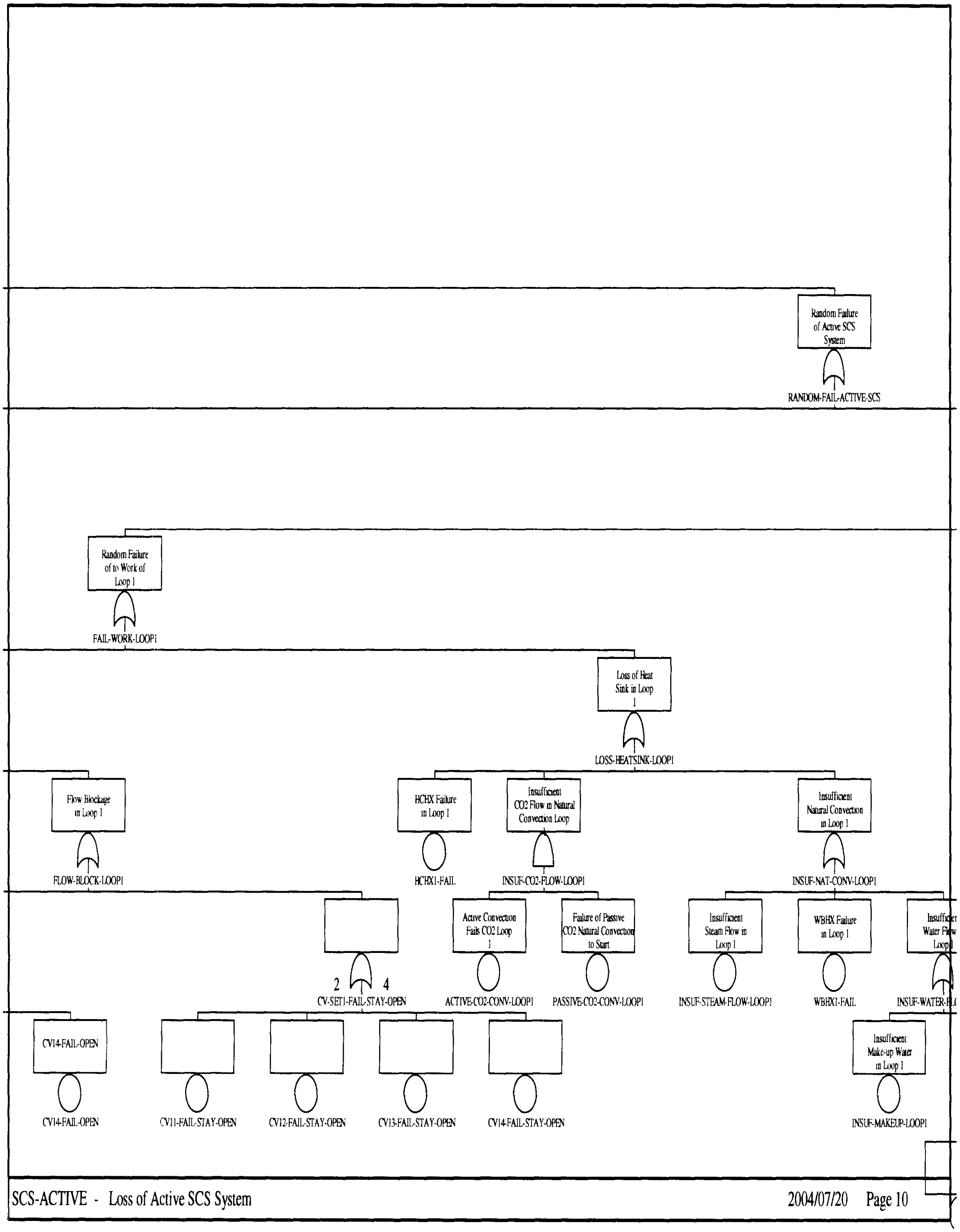


Figure IV-23 Fault Tree for Active SCS System in GFR: Zoom 5

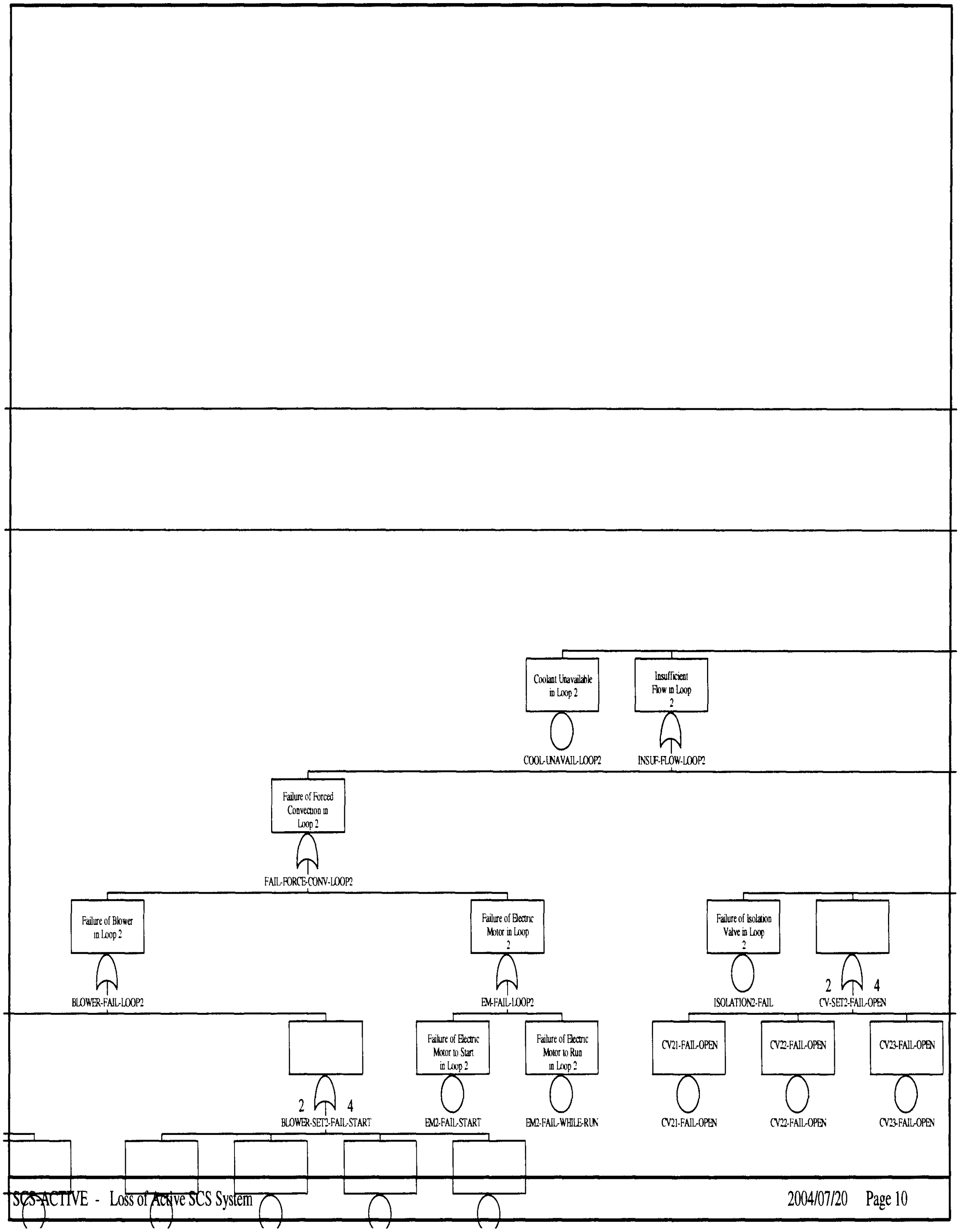

Coolant Unavailable in Loop 2
COOL-UNAVAIL-LOOP2
Insufficient Flow in Loop 2
INSUF-FLOW-LOOP2
Failure of Forced Convection in Loop 2
FAIL-FORCE-CONV-LOOP2
Failure of Blower in Loop 2
BLOWER-FAIL-LOOP2
Failure of Electric Motor in Loop 2
EM-FAIL-LOOP2
Failure of Isolation Valve in Loop 2
ISOLATION2-FAIL
2
4
CV-SET2-FAIL-OPEN
2
4
BLOWER-SET2-FAIL-START
Failure of Electric Motor to Start in Loop 2
EM2-FAIL-START
Failure of Electric Motor to Run in Loop 2
EM2-FAIL-WHILE-RUN
CV21-FAIL-OPEN
CV21-FAIL-OPEN
CV22-FAIL-OPEN
CV22-FAIL-OPEN
CV23-FAIL-OPEN
CV23-FAIL-OPEN
SCS-ACTIVE - Loss of Active SCS System
2004/07/20 Page 10

Figure IV-24 Fault Tree for Active SCS System in GFR: Zoom 6

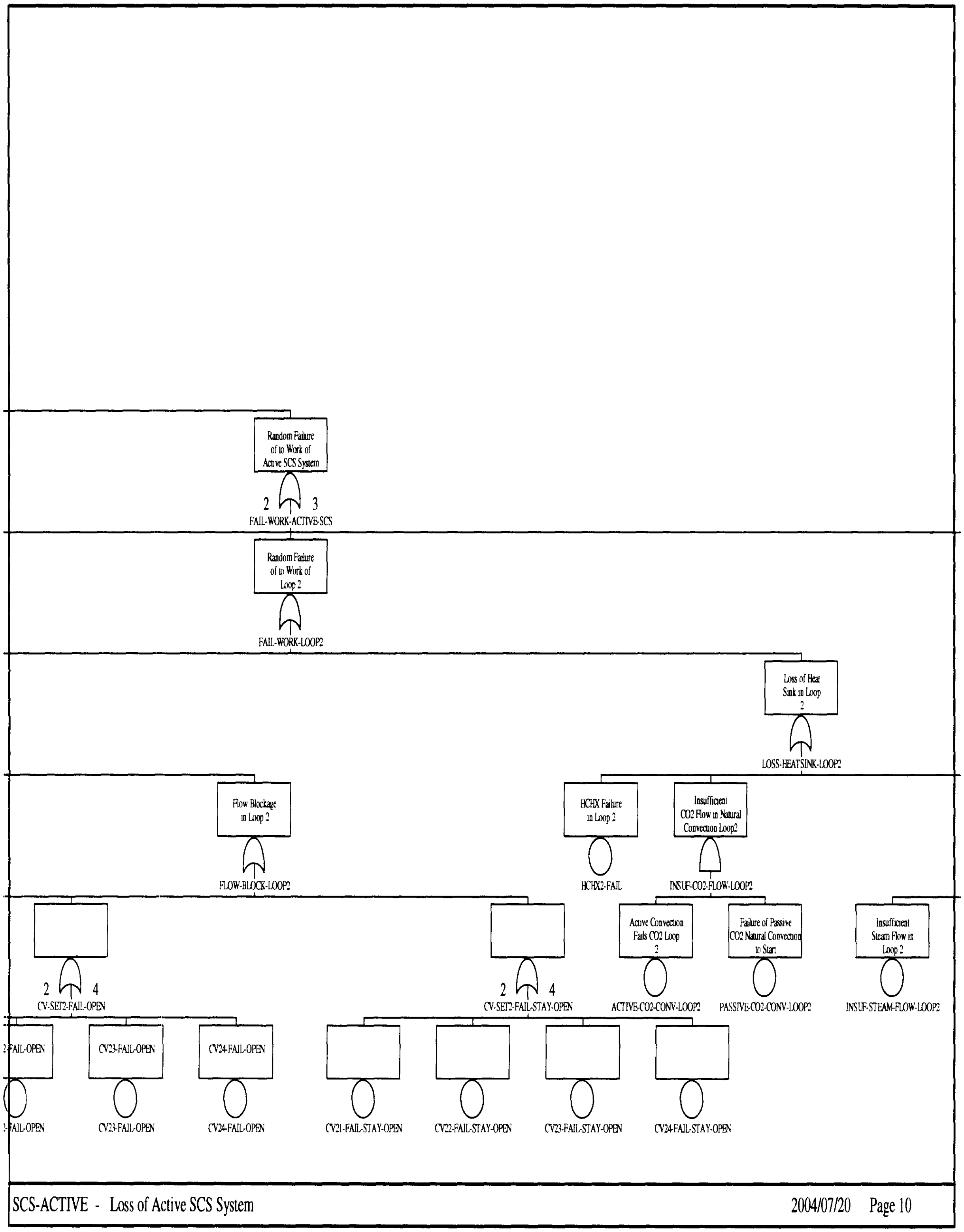


Figure IV-25 Fault Tree for Active SCS System in GFR: Zoom 7

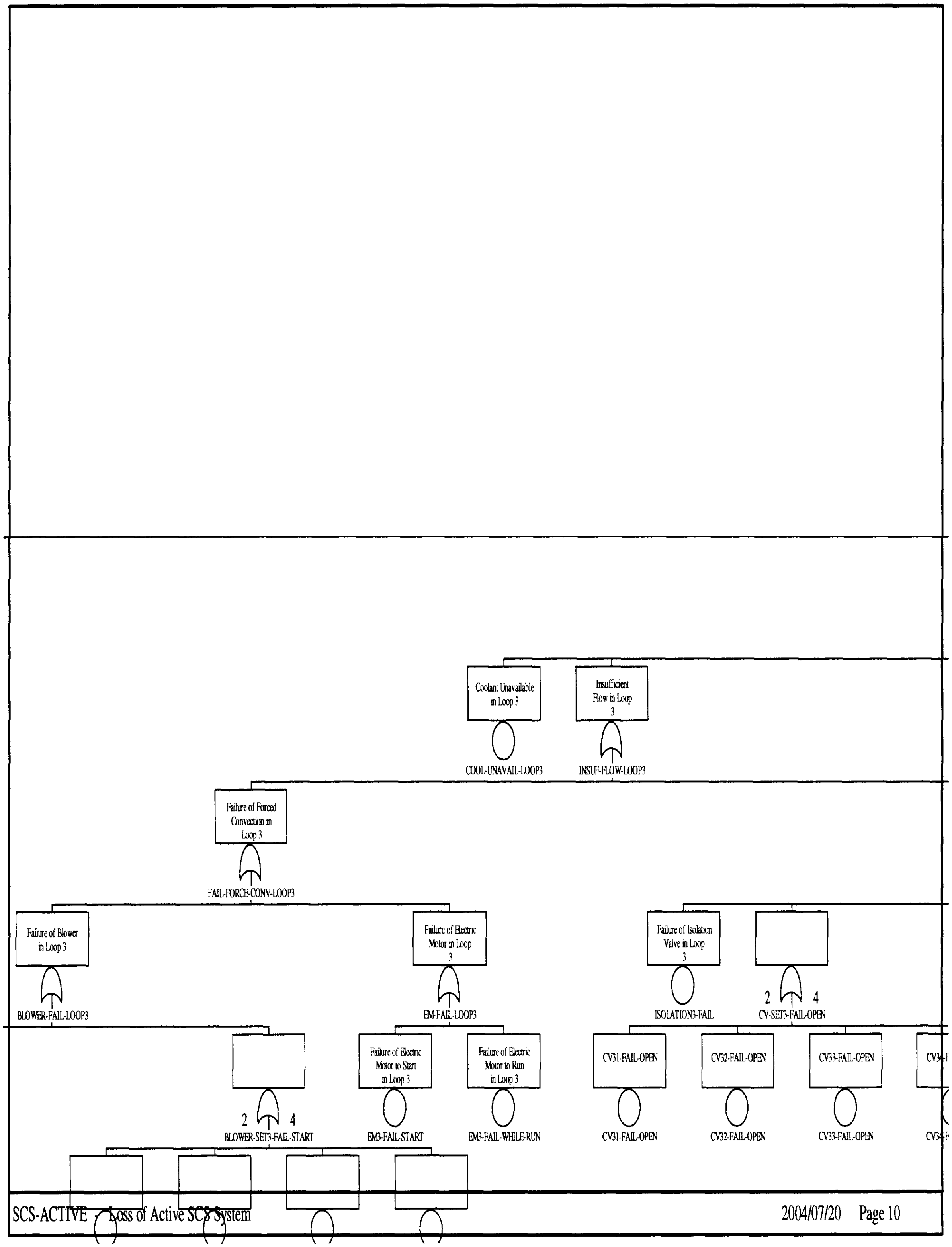

Coolant Unavailable in Loop 3
Insufficient Flow in Loop 3
COOL-UNAVAIL-LOOP3
INSUF-FLOW-LOOP3
Failure of Forced Convection in Loop 3
FAIL-FORCE-CONV-LOOP3
Failure of Blower in Loop 3
Failure of Electric Motor in Loop 3
Failure of Isolation Valve in Loop 3
2
4
BLOWER-FAIL-LOOP3
EM-FAIL-LOOP3
ISOLATION3-FAIL
CV-SET3-FAIL-OPEN
Failure of Electric Motor to Start in Loop 3
Failure of Electric Motor to Run in Loop 3
CV31-FAIL-OPEN
CV32-FAIL-OPEN
CV33-FAIL-OPEN
CV3
2
4
BLOWER-SET3-FAIL-START
EM3-FAIL-START
EM3-FAIL-WHILE-RUN
CV31-FAIL-OPEN
CV32-FAIL-OPEN
CV33-FAIL-OPEN
CV3
SCS-ACTIVE - Loss of Active SCS System
2004/07/20 Page 10

Figure IV-26 Fault Tree for Active SCS System in GFR: Zoom 8

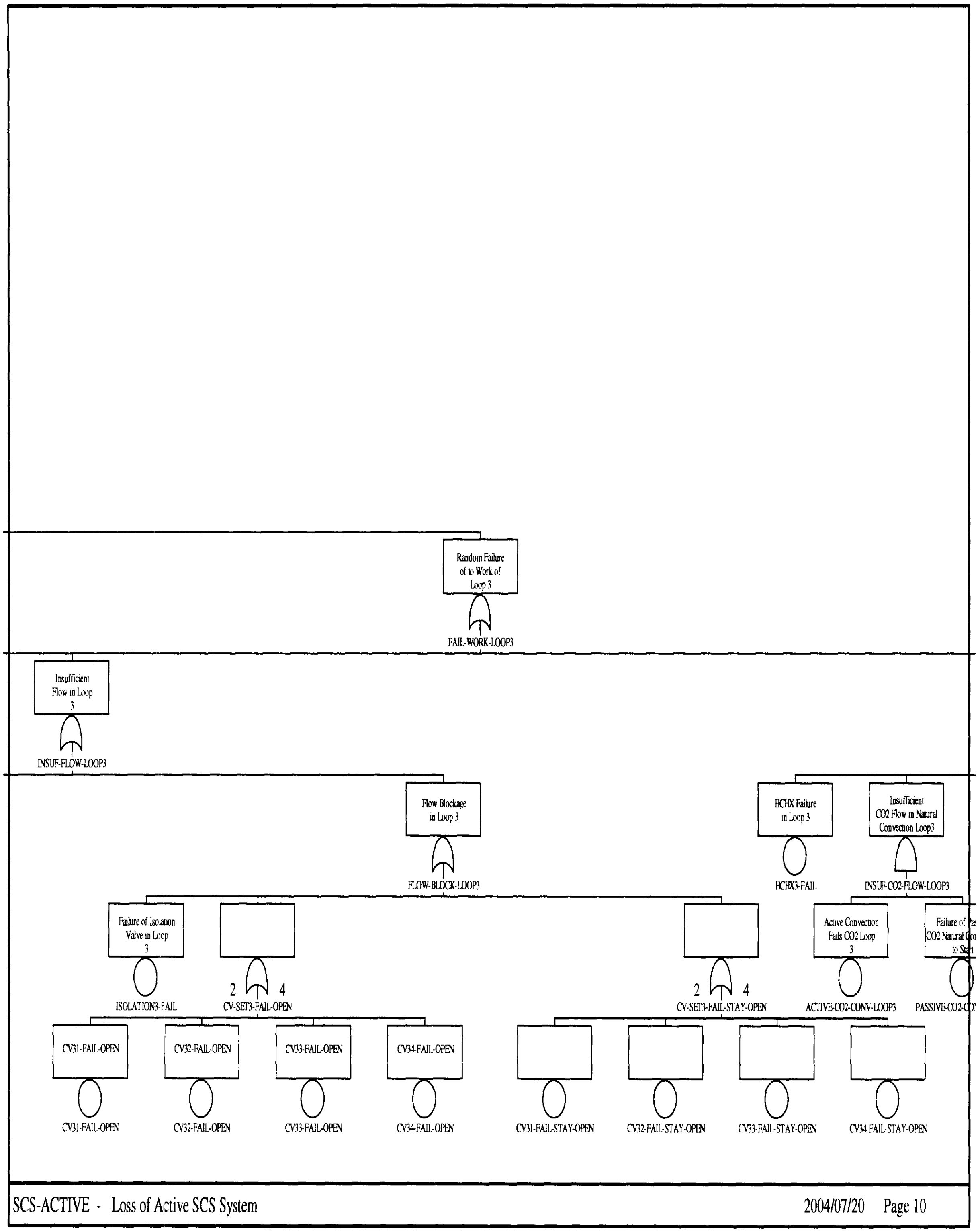


Figure IV-27 Fault Tree for Active SCS System in GFR: Zoom 9

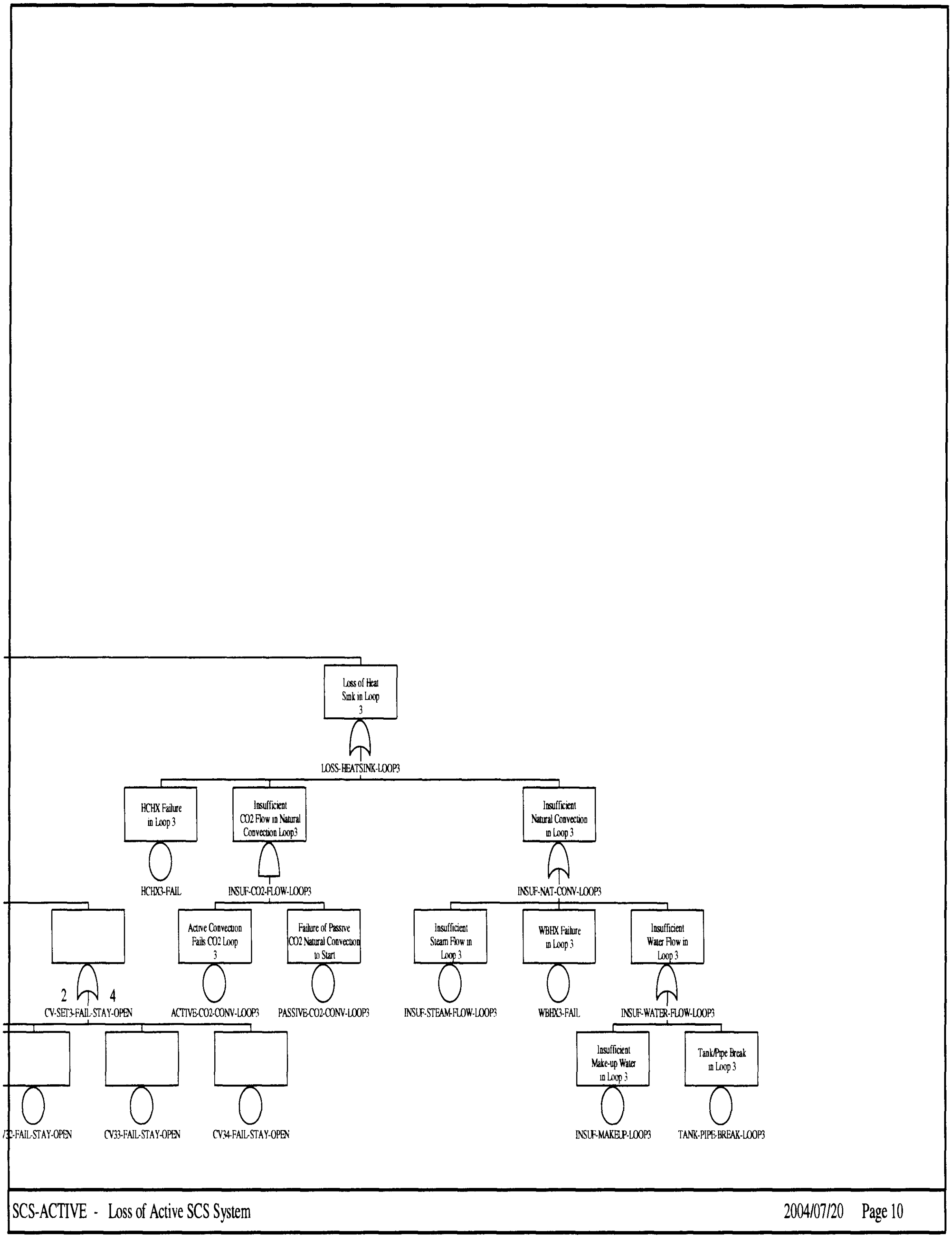

Loss of Heat Sink in Loop 3
LOSS-HEATSINK-LOOP3
HCHX Failure in Loop 3
HCHX3-FAIL
Insufficient CO2 Flow in Natural Convection Loop3
INSUF-CO2-FLOW-LOOP3
Insufficient Natural Convection in Loop 3
INSUF-NAT-CONV-LOOP3
2
4
CV-SET3-FAIL-STAY-OPEN
Active Convection Fails CO2 Loop 3
ACTIVE-CO2-CONV-LOOP3
Failure of Passive CO2 Natural Convection to Start
PASSIVE-CO2-CONV-LOOP3
Insufficient Steam Flow in Loop 3
INSUF-STEAM-FLOW-LOOP3
WBHX Failure in Loop 3
WBHX3-FAIL
Insufficient Water Flow in Loop 3
INSUF-WATER-FLOW-LOOP3
/32-FAIL-STAY-OPEN
CV33-FAIL-STAY-OPEN
CV34-FAIL-STAY-OPEN
Insufficient Make-up Water in Loop 3
INSUF-MAKEUP-LOOP3
Tank/Pipe Break in Loop 3
TANK-PIPE-BREAK-LOOP3
SCS-ACTIVE - Loss of Active SCS System
2004/07/20 Page 10

Figure IV-28 Fault Tree for Active SCS System in GFR: Zoom 10

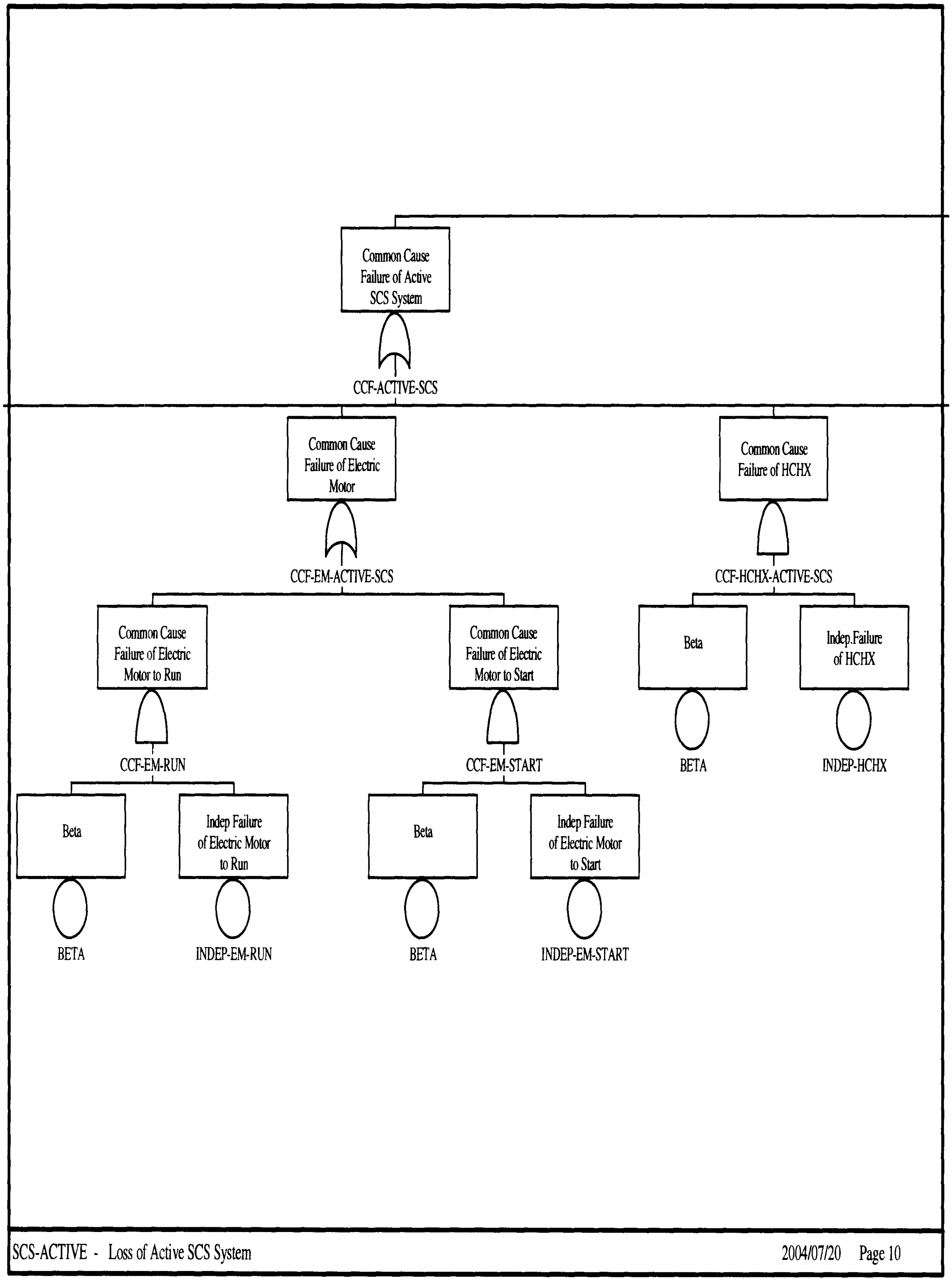

Common Cause Failure of Active SCS System
CCF-ACTIVE-SCS
Common Cause Failure of Electric Motor
CCF-EM-ACTIVE-SCS
Common Cause Failure of HCHX
CCF-HCHX-ACTIVE-SCS
Common Cause Failure of Electric Motor to Run
CCF-EM-RUN
Common Cause Failure of Electric Motor to Start
CCF-EM-START
Beta
BETA
Indep.Failure of HCHX
INDEP-HCHX
Beta
BETA
Indep Failure of Electric Motor to Run
INDEP-EM-RUN
Beta
BETA
Indep Failure of Electric Motor to Start
INDEP-EM-START
SCS-ACTIVE - Loss of Active SCS System
2004/07/20 Page 10

Figure IV-29 Fault Tree for Active SCS System in GFR: Zoom 11

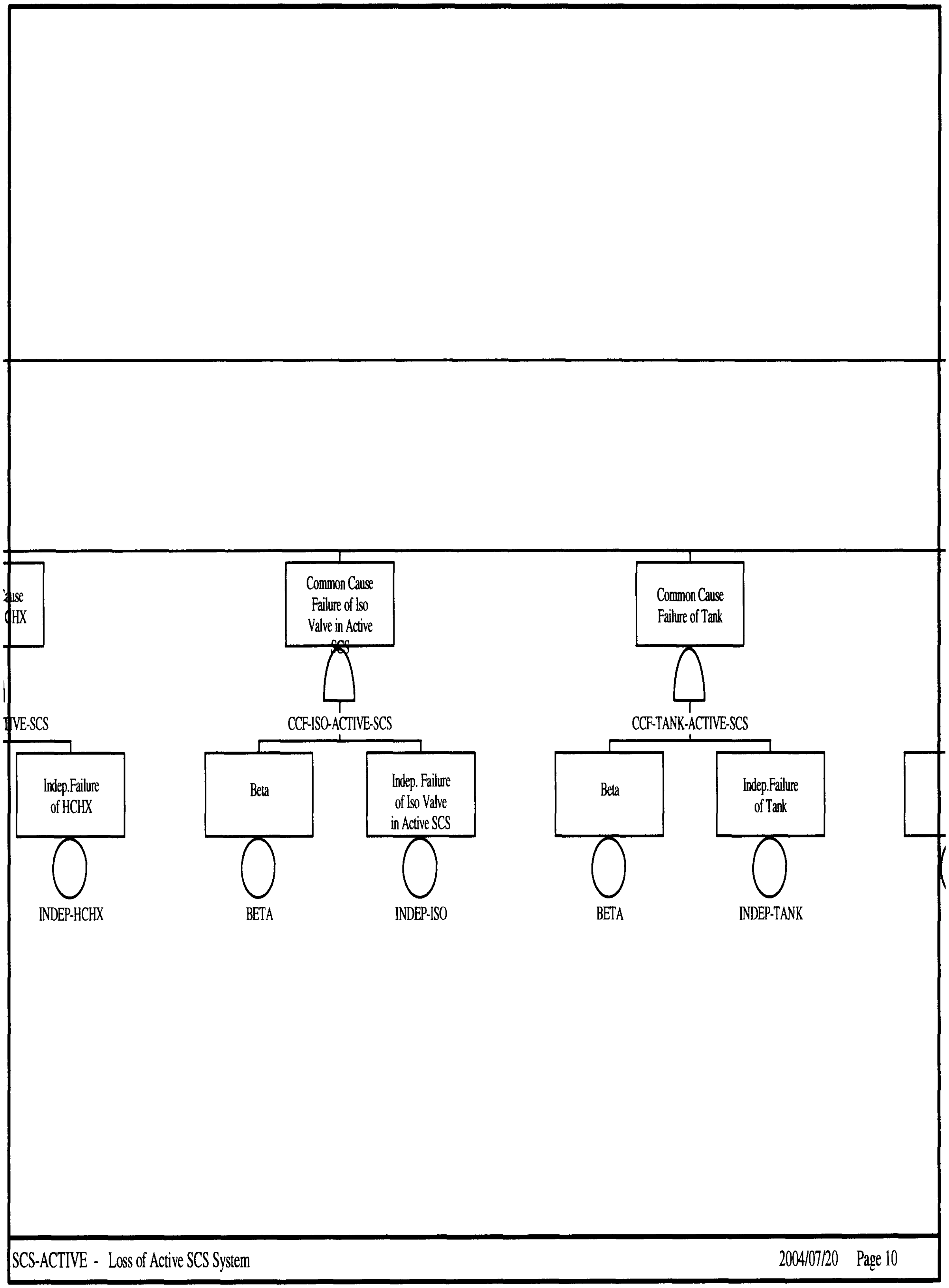


Figure IV-30 Fault Tree for Active SCS System in GFR: Zoom 12

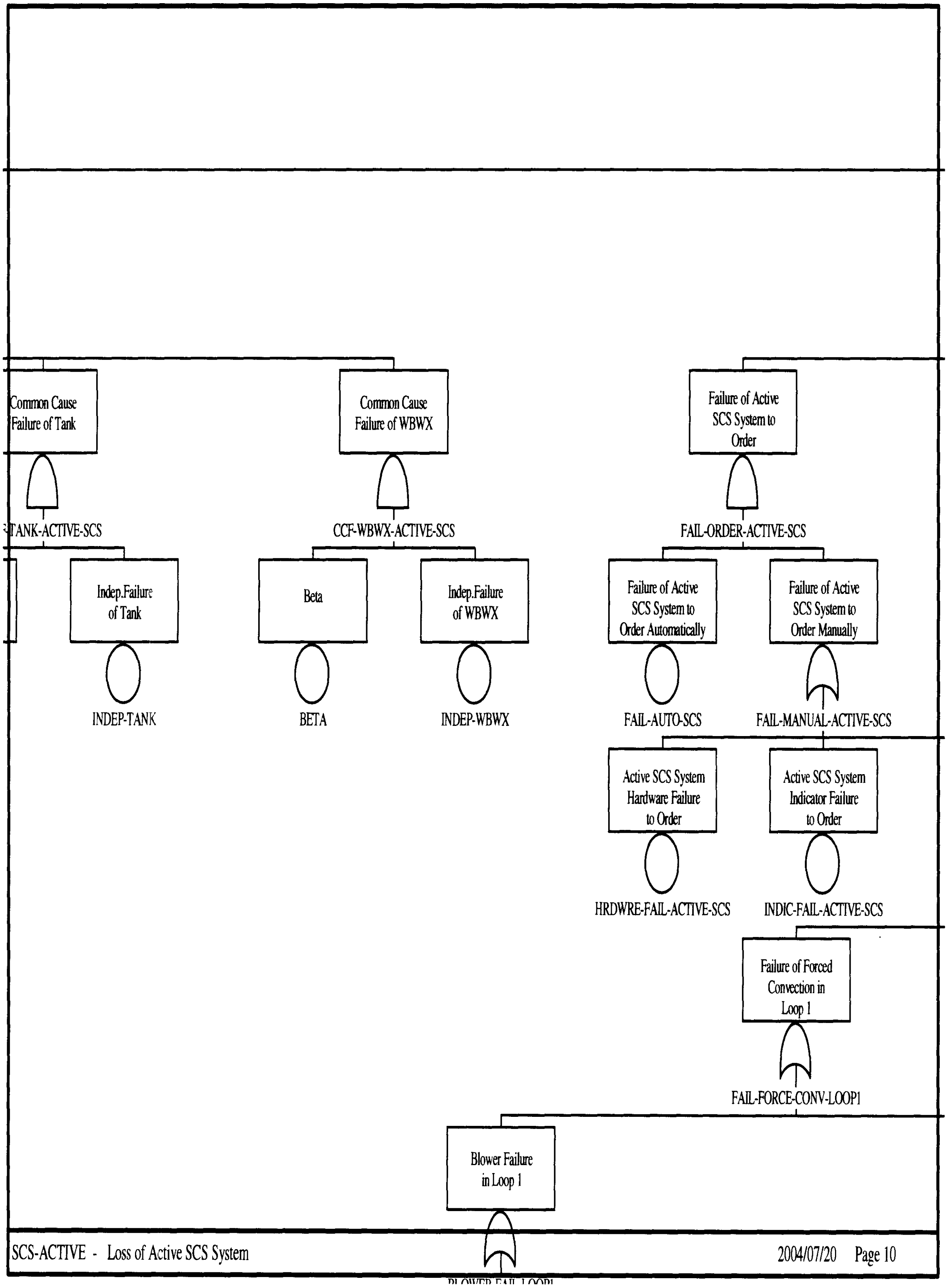

Common Cause Failure of Tank
TANK-ACTIVE-SCS
Common Cause Failure of WBWX
CCF-WBWX-ACTIVE-SCS
Failure of Active SCS System to Order
FAIL-ORDER-ACTIVE-SCS
Indep.Failure of Tank
INDEP-TANK
Beta
BETA
Indep.Failure of WBWX
INDEP-WBWX
Failure of Active SCS System to Order Automatically
FAIL-AUTO-SCS
Failure of Active SCS System to Order Manually
FAIL-MANUAL-ACTIVE-SCS
Active SCS System Hardware Failure to Order
HRDWRE-FAIL-ACTIVE-SCS
Active SCS System Indicator Failure to Order
INDIC-FAIL-ACTIVE-SCS
Failure of Forced Convection in Loop 1
FAIL-FORCE-CONV-LOOP1
Blower Failure in Loop 1
SCS-ACTIVE - Loss of Active SCS System
2004/07/20 Page 10

Figure IV-31 Fault Tree for Active SCS System in GFR: Zoom 13

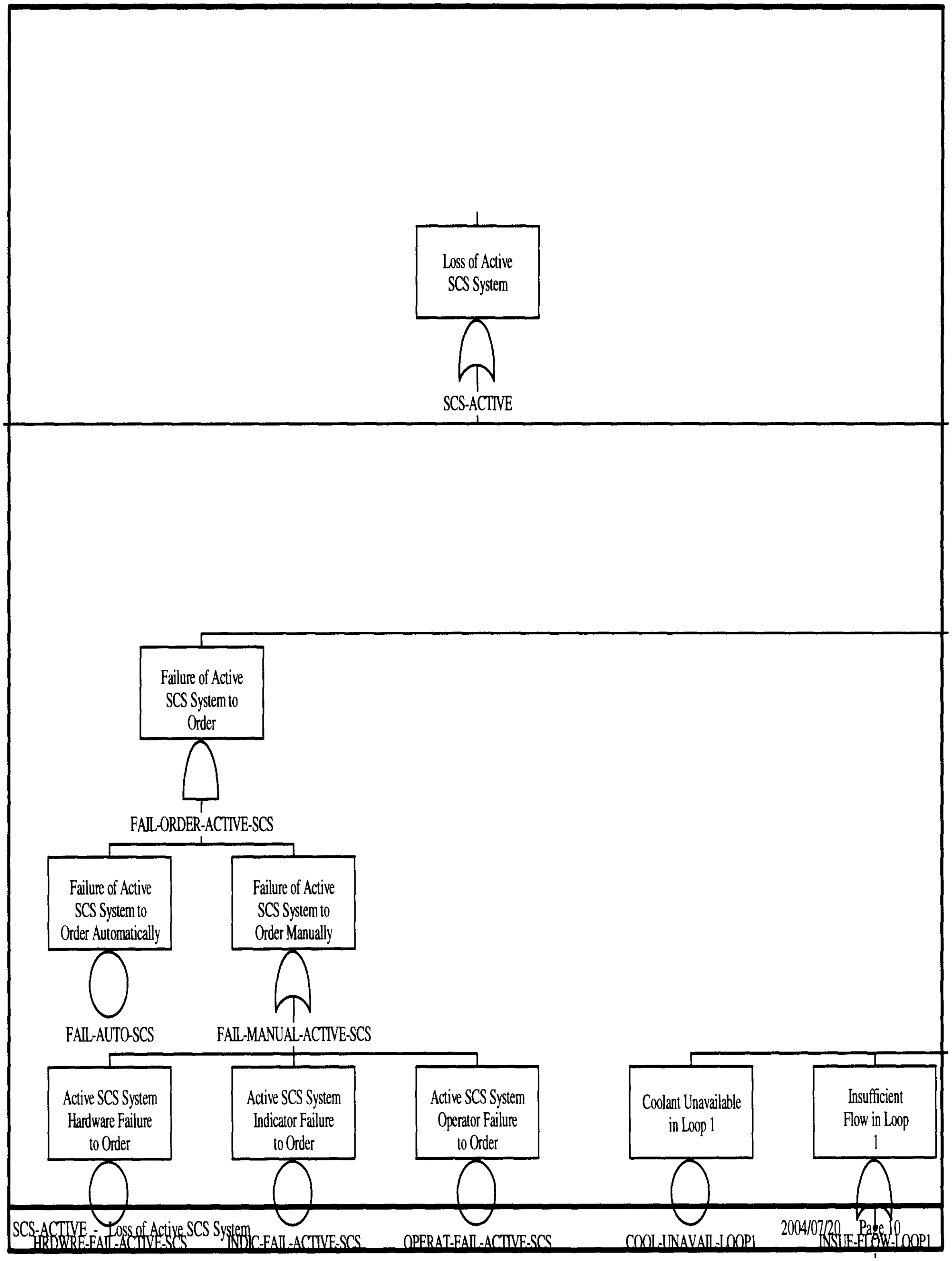

Loss of Active SCS System
SCS-ACTIVE
Failure of Active SCS System to Order
FAIL-ORDER-ACTIVE-SCS
Failure of Active SCS System to Order Automatically
FAIL-AUTO-SCS
Failure of Active SCS System to Order Manually
FAIL-MANUAL-ACTIVE-SCS
Active SCS System Hardware Failure to Order
HRDWRE-FAIL-ACTIVE-SCS
Active SCS System Indicator Failure to Order
INDIC-FAIL-ACTIVE-SCS
Active SCS System Operator Failure to Order
OPERAT-FAIL-ACTIVE-SCS
Coolant Unavailable in Loop 1
COOL-UNAVAIL-LOOP1
Insufficient Flow in Loop 1
INSUF-FLOW-LOOP1
SCS-ACTIVE - Loss of Active SCS System
2004/07/20 Page 10

Figure IV-32 Fault Tree for Active SCS System in GFR: Zoom 14

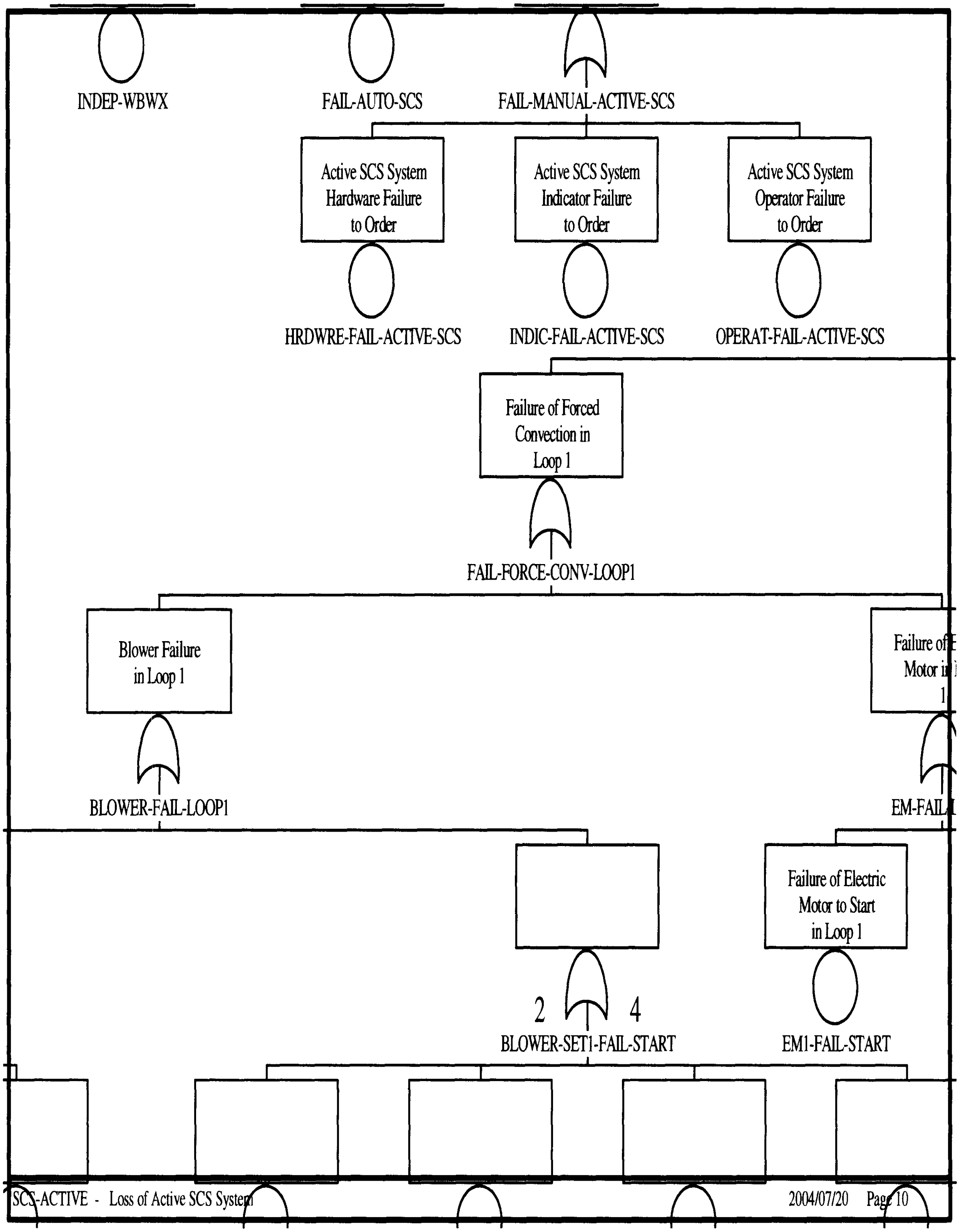


Figure IV-33 Fault Tree for Active SCS System in GFR: Zoom 15

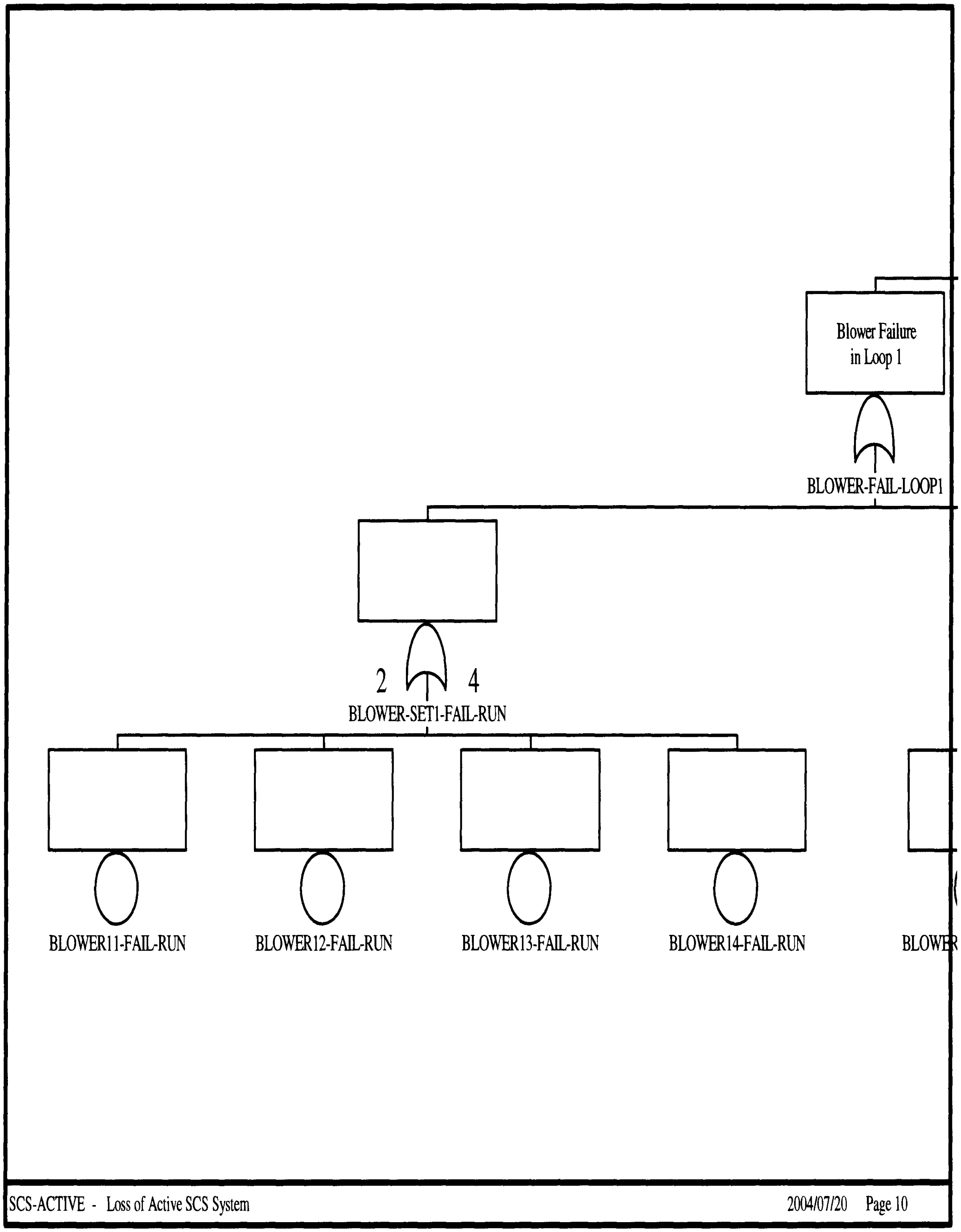


Figure IV-34 Fault Tree for Active SCS System in GFR: Zoom 16

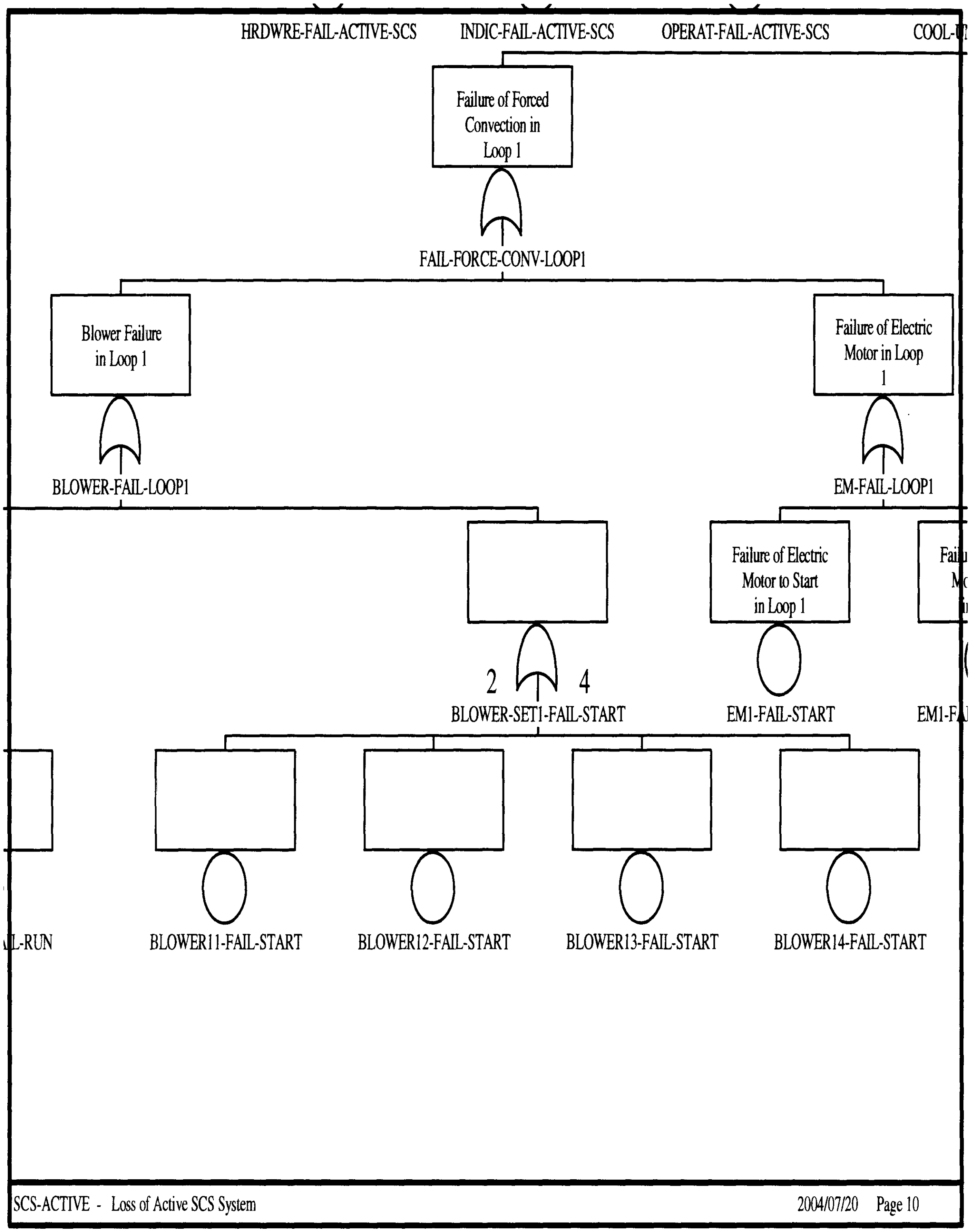


Figure IV-35 Fault Tree for Active SCS System in GFR: Zoom 17

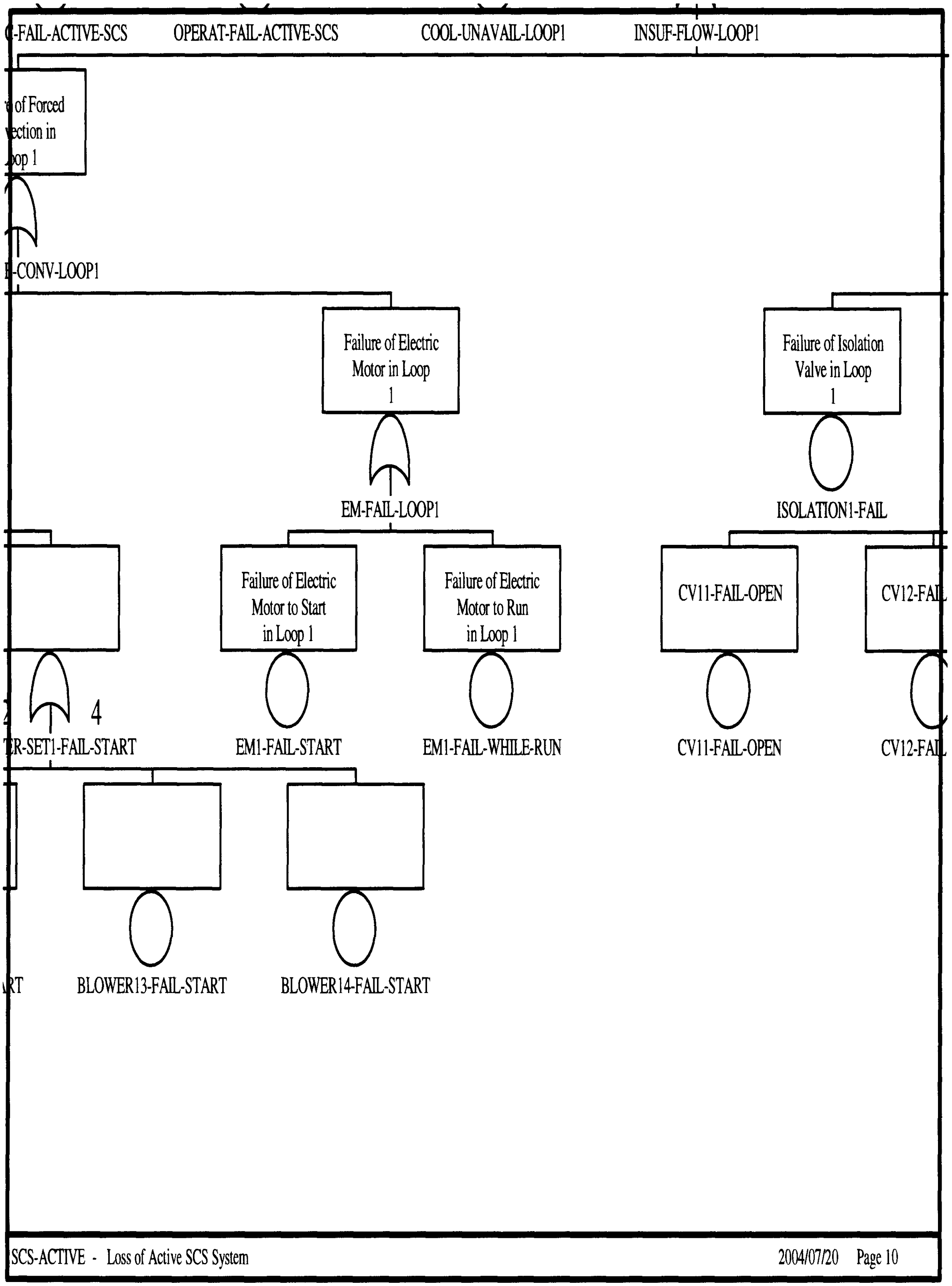


Figure IV-36 Fault Tree for Active SCS System in GFR: Zoom 18

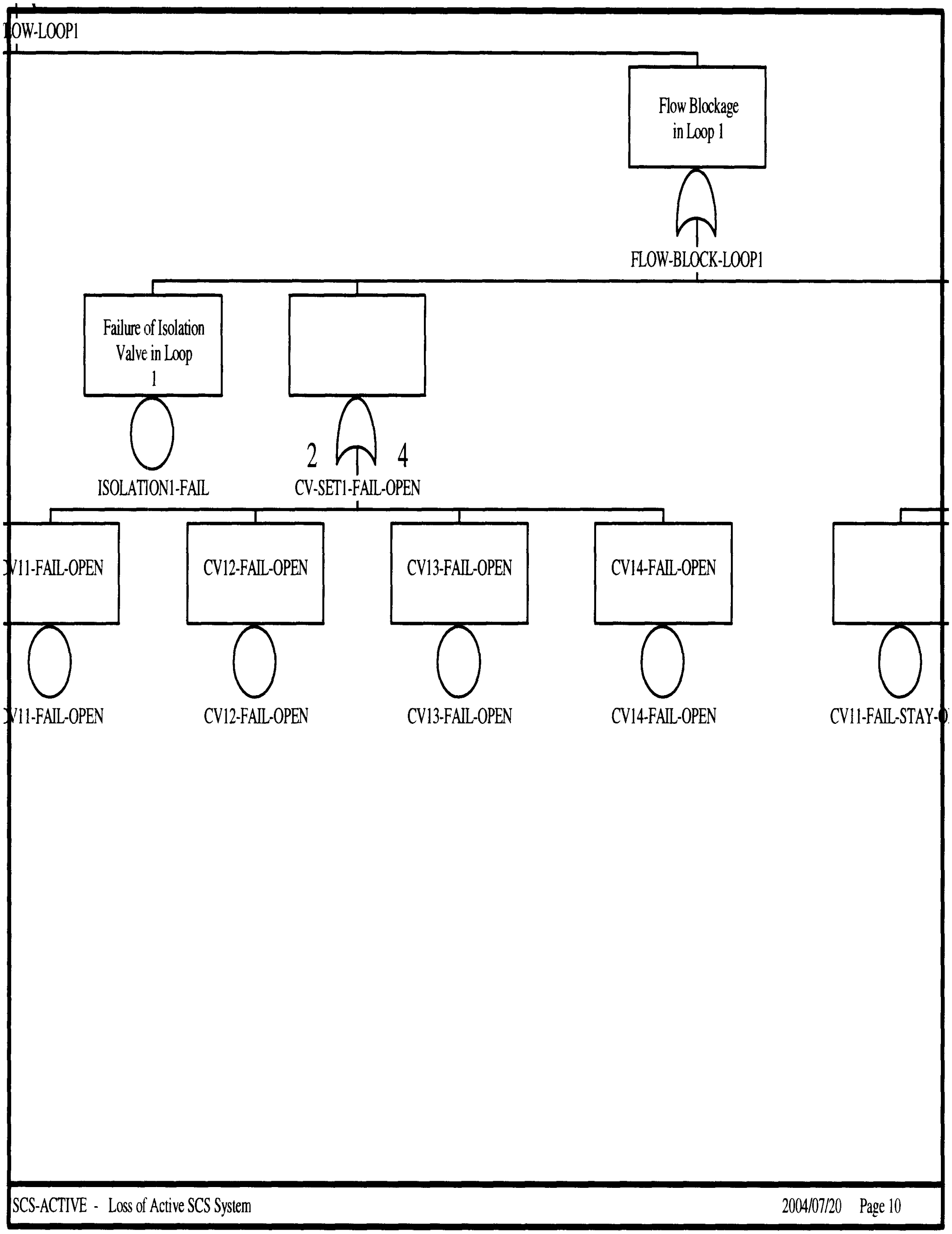


Figure IV-37 Fault Tree for Active SCS System in GFR: Zoom 19

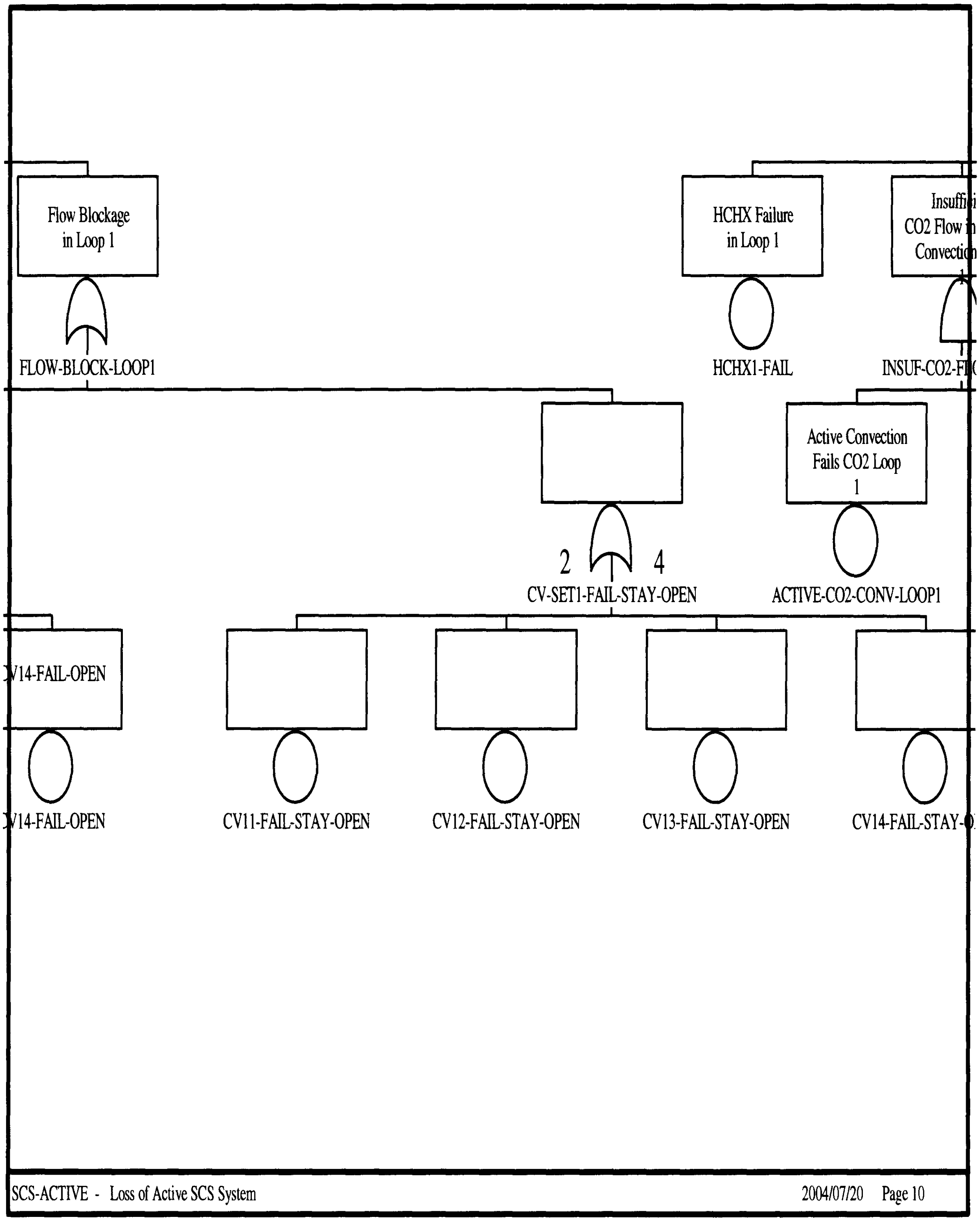


Figure IV-38 Fault Tree for Active SCS System in GFR: Zoom 20

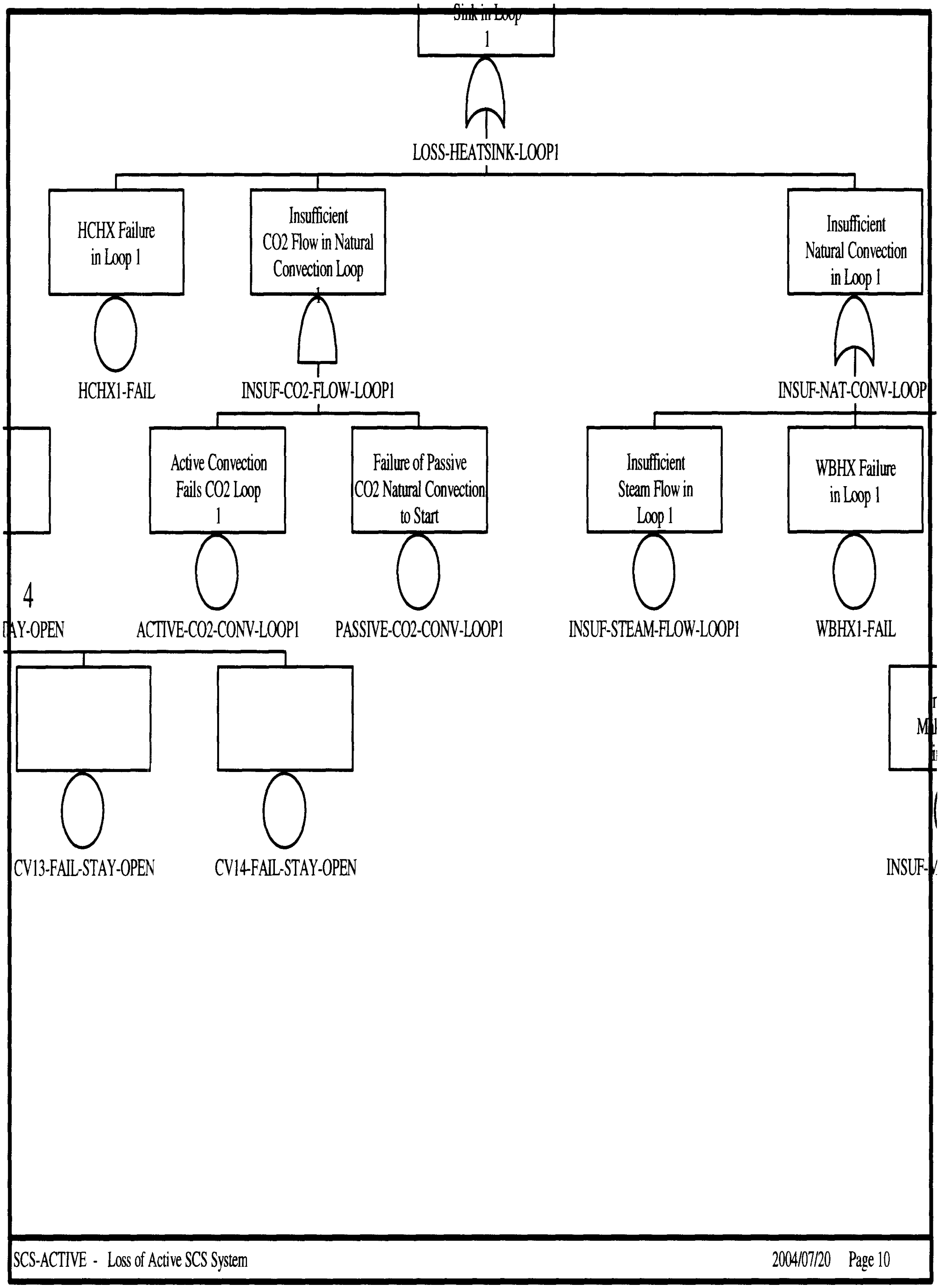


Figure IV-39 Fault Tree for Active SCS System in GFR: Zoom 21

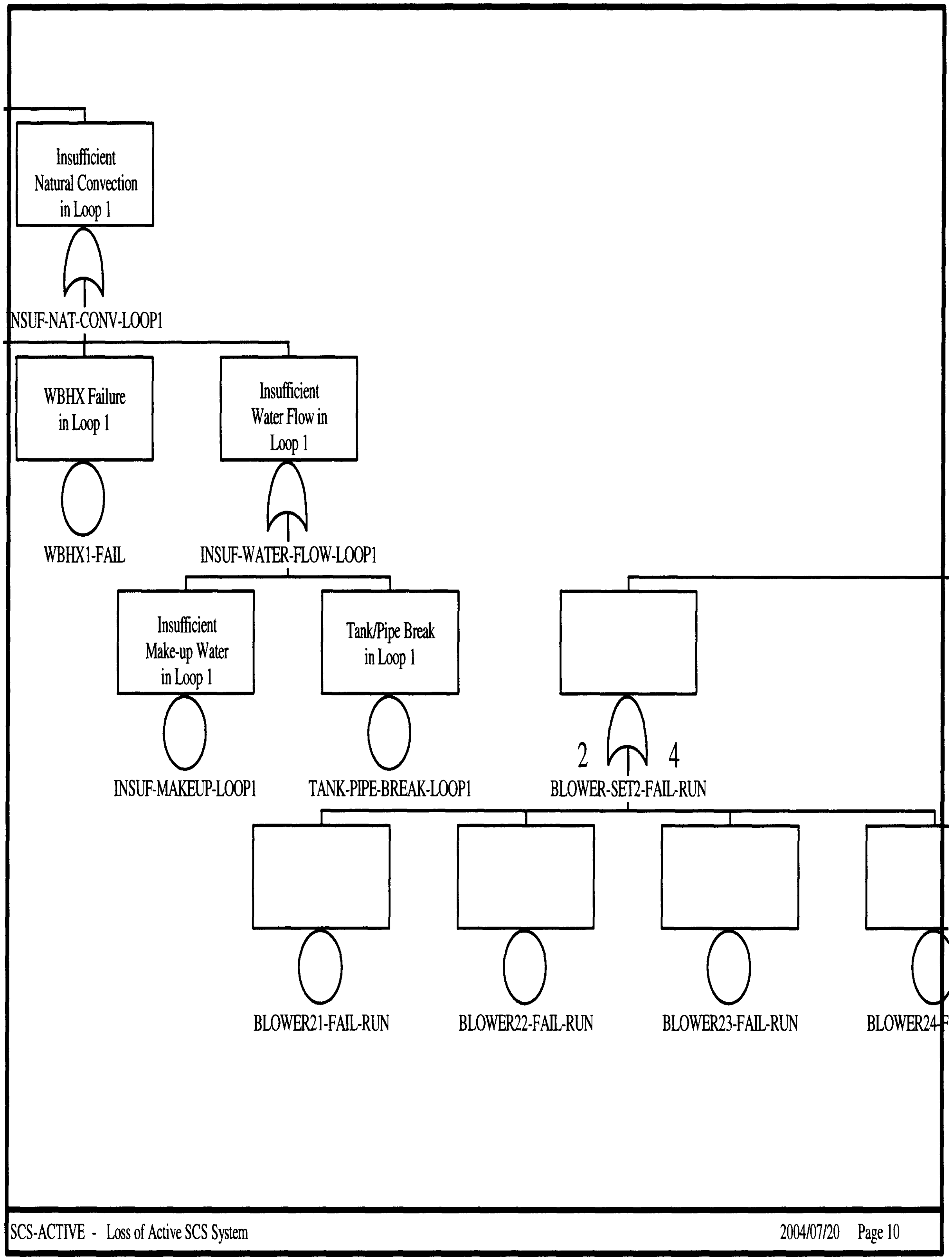


Figure IV-40 Fault Tree for Active SCS System in GFR: Zoom 22

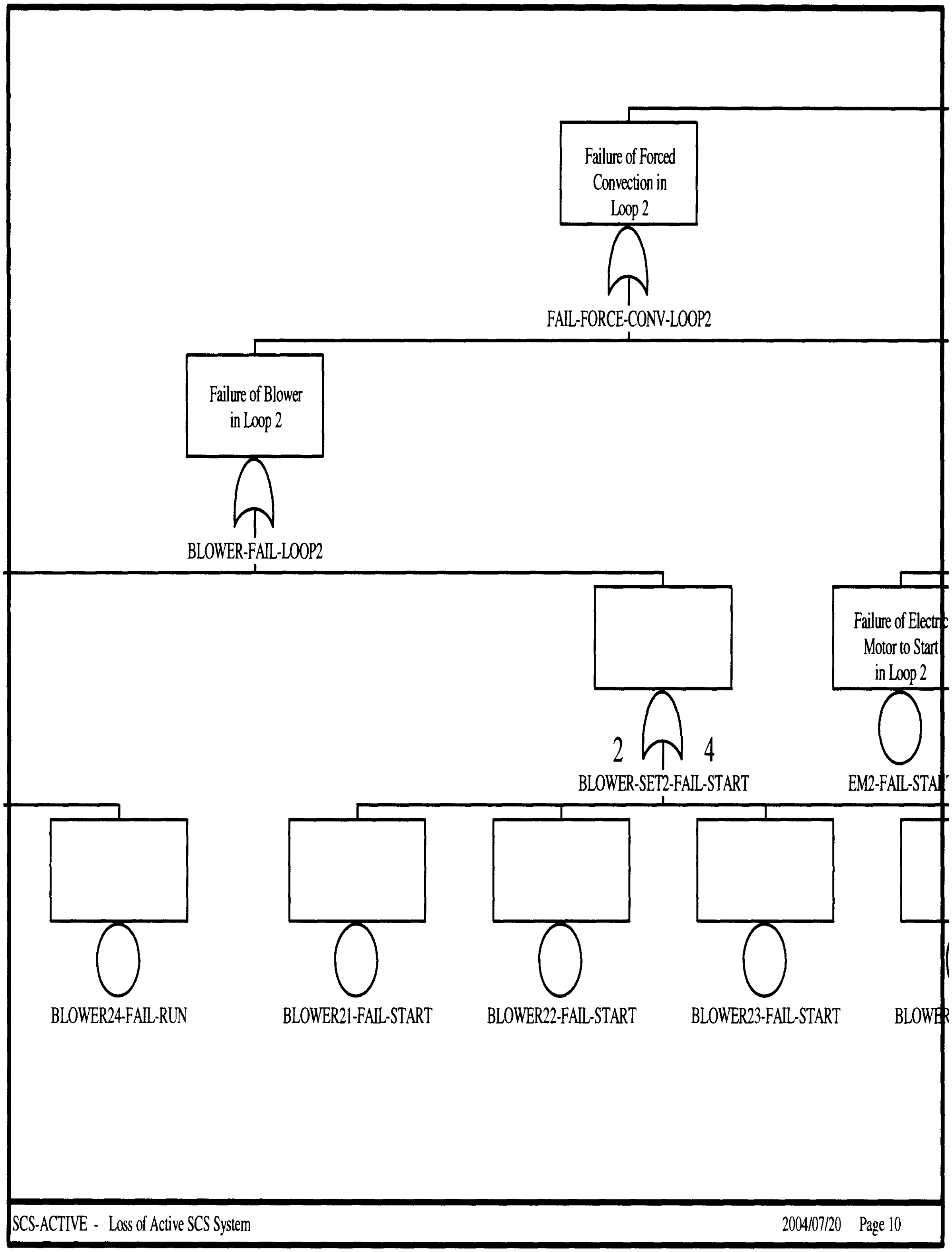


Figure IV-41 Fault Tree for Active SCS System in GFR: Zoom 23

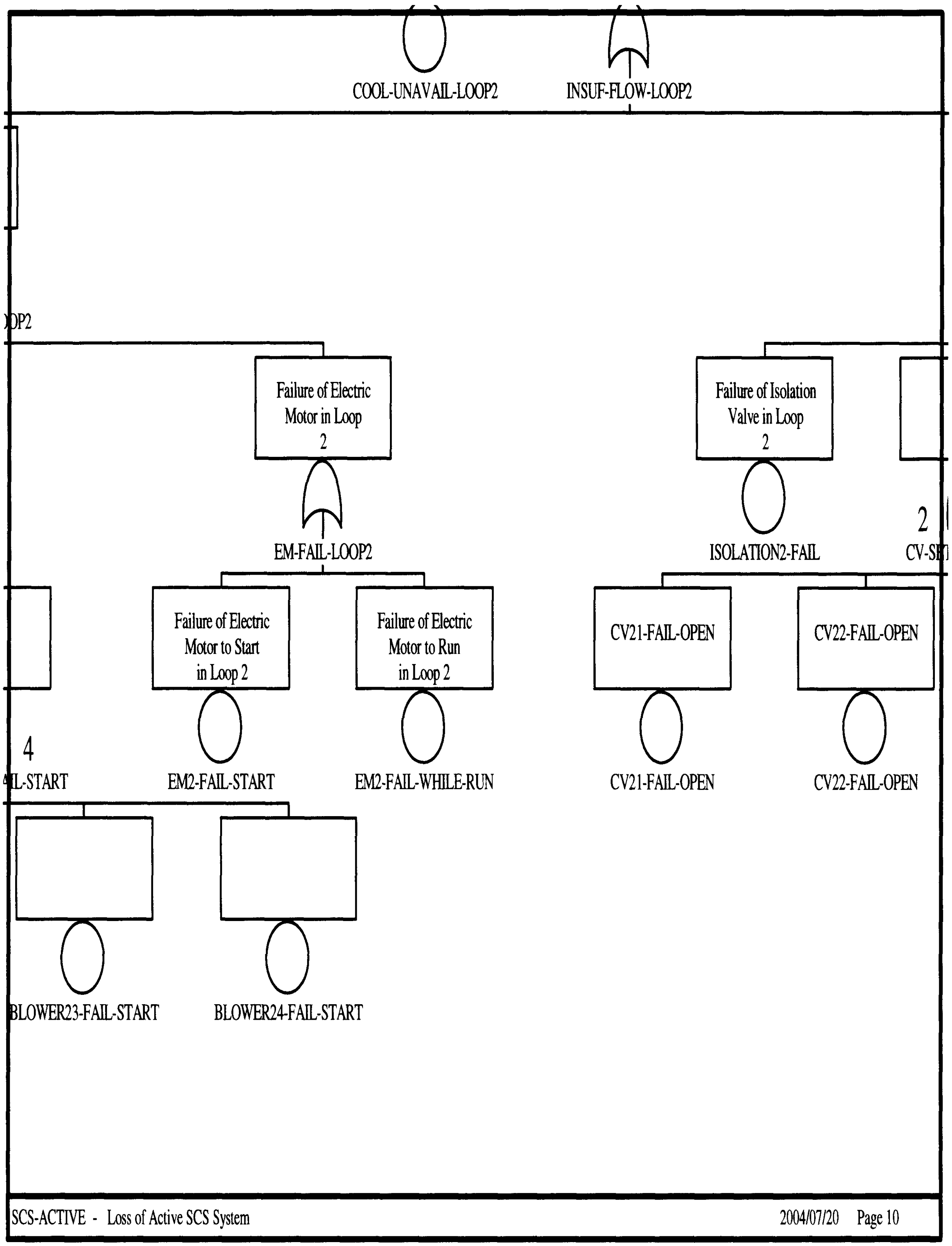


Figure IV-42 Fault Tree for Active SCS System in GFR: Zoom 24

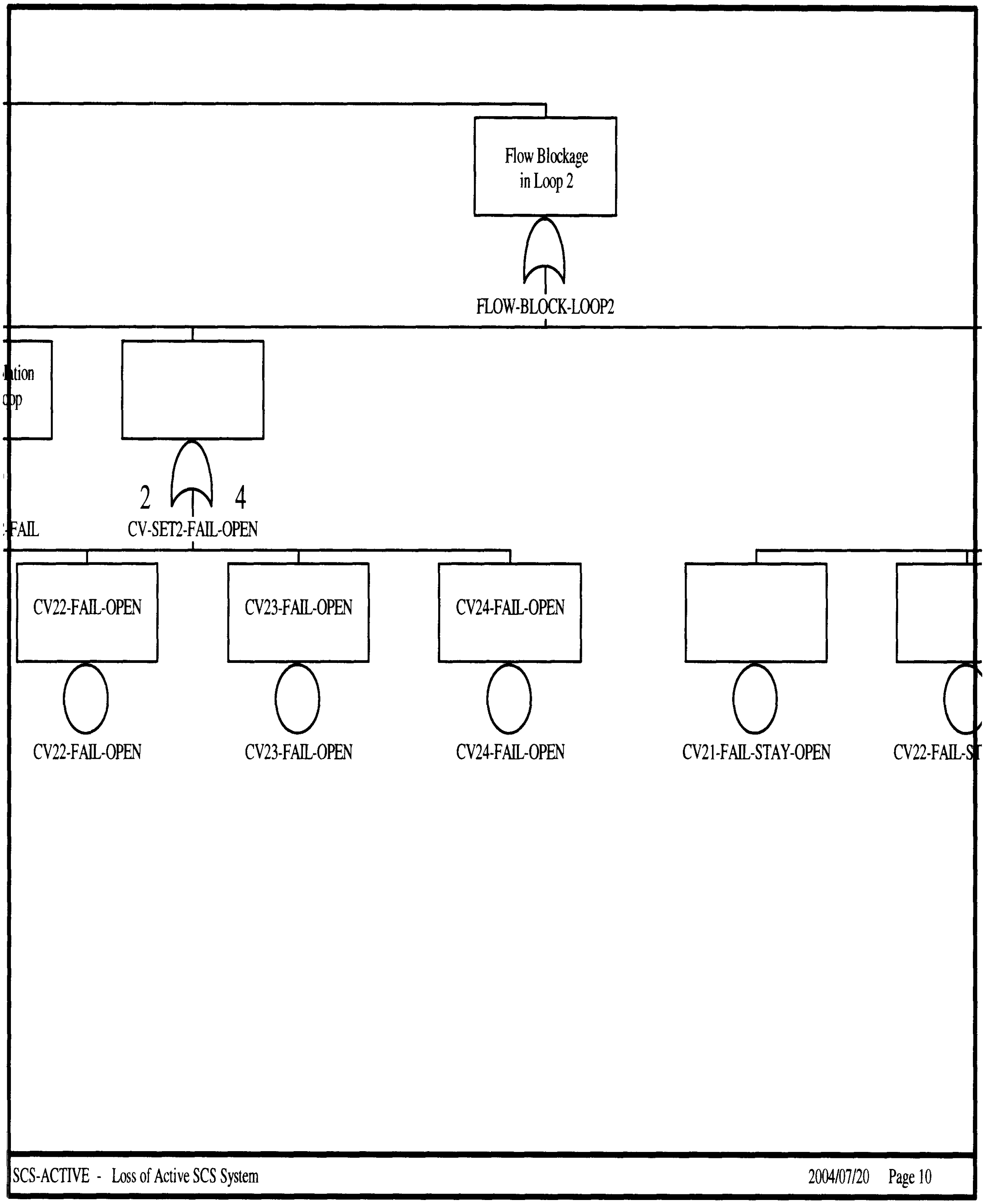


Figure IV-43 Fault Tree for Active SCS System in GFR: Zoom 25

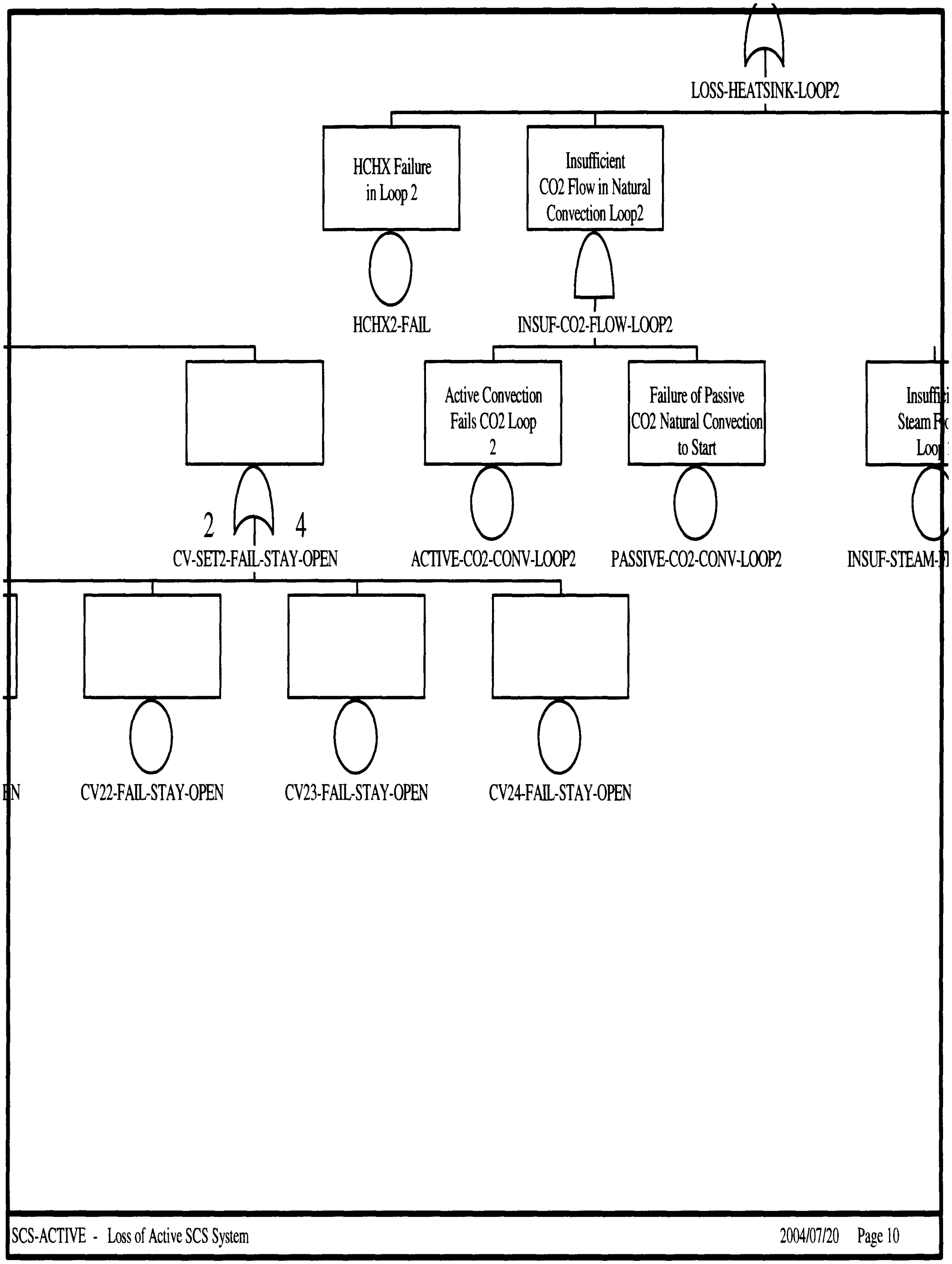


Figure IV-44 Fault Tree for Active SCS System in GFR: Zoom 26

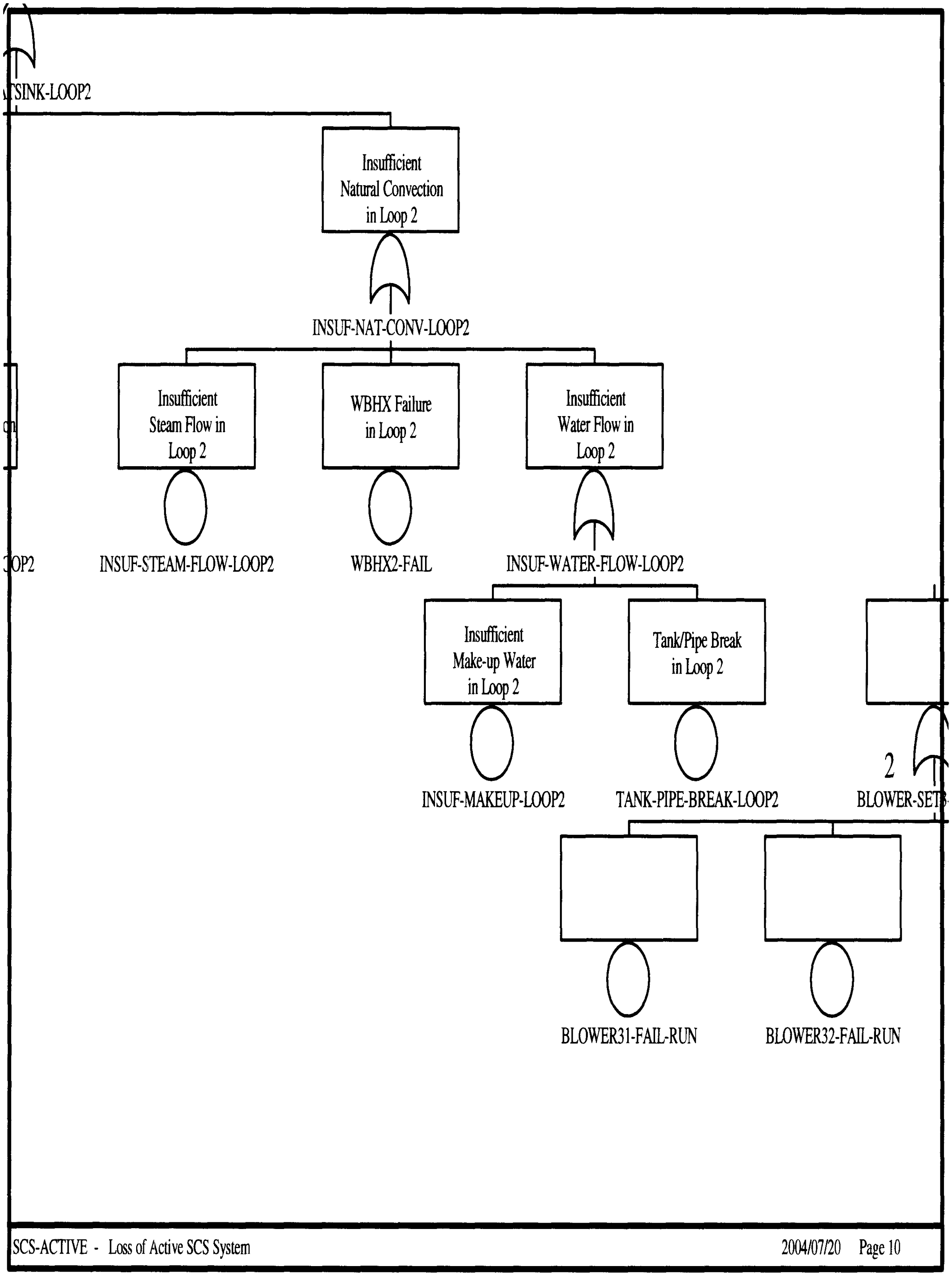


Figure IV-45 Fault Tree for Active SCS System in GFR: Zoom 27

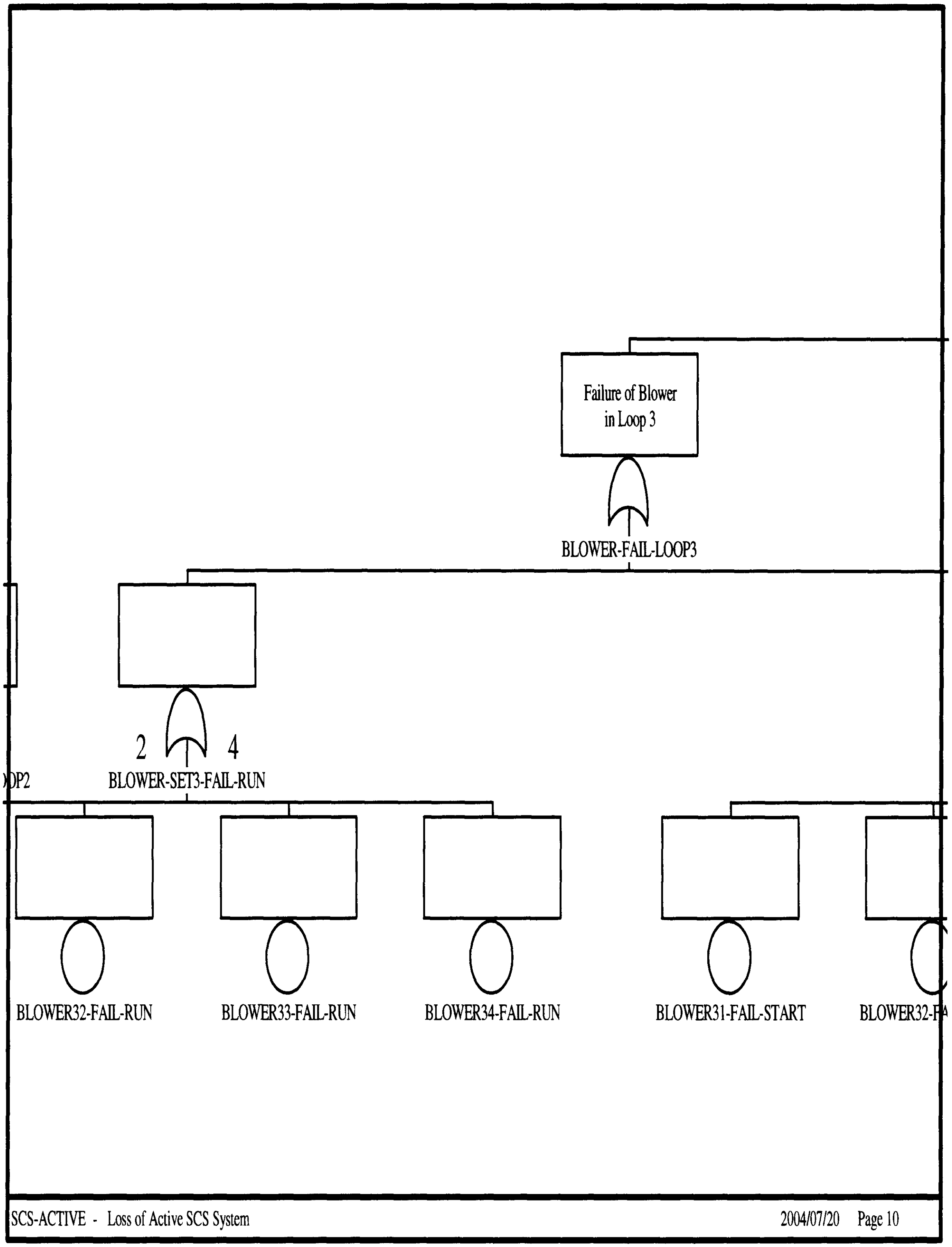


Figure IV-46 Fault Tree for Active SCS System in GFR: Zoom 28

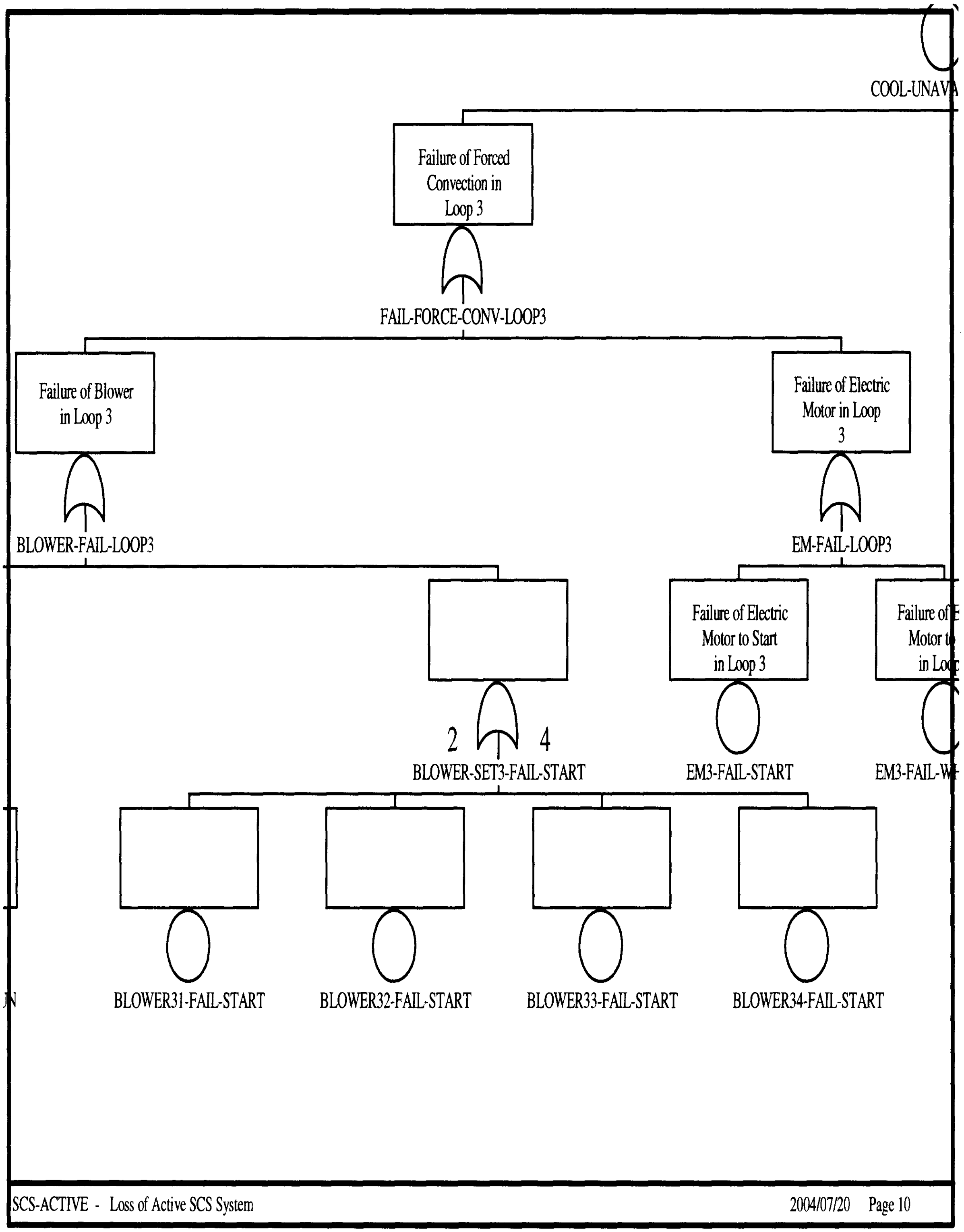

COOL-UNAVA
Failure of Forced Convection in Loop 3
FAIL-FORCE-CONV-LOOP3
Failure of Blower in Loop 3
BLOWER-FAIL-LOOP3
Failure of Electric Motor in Loop 3
EM-FAIL-LOOP3
2
4
BLOWER-SET3-FAIL-START
Failure of Electric Motor to Start in Loop 3
EM3-FAIL-START
Failure of E Motor t in Loo
EM3-FAIL-W
BLOWER31-FAIL-START
BLOWER32-FAIL-START
BLOWER33-FAIL-START
BLOWER34-FAIL-START
SCS-ACTIVE - Loss of Active SCS System
2004/07/20 Page 10

Figure IV-47 Fault Tree for Active SCS System in GFR: Zoom 29

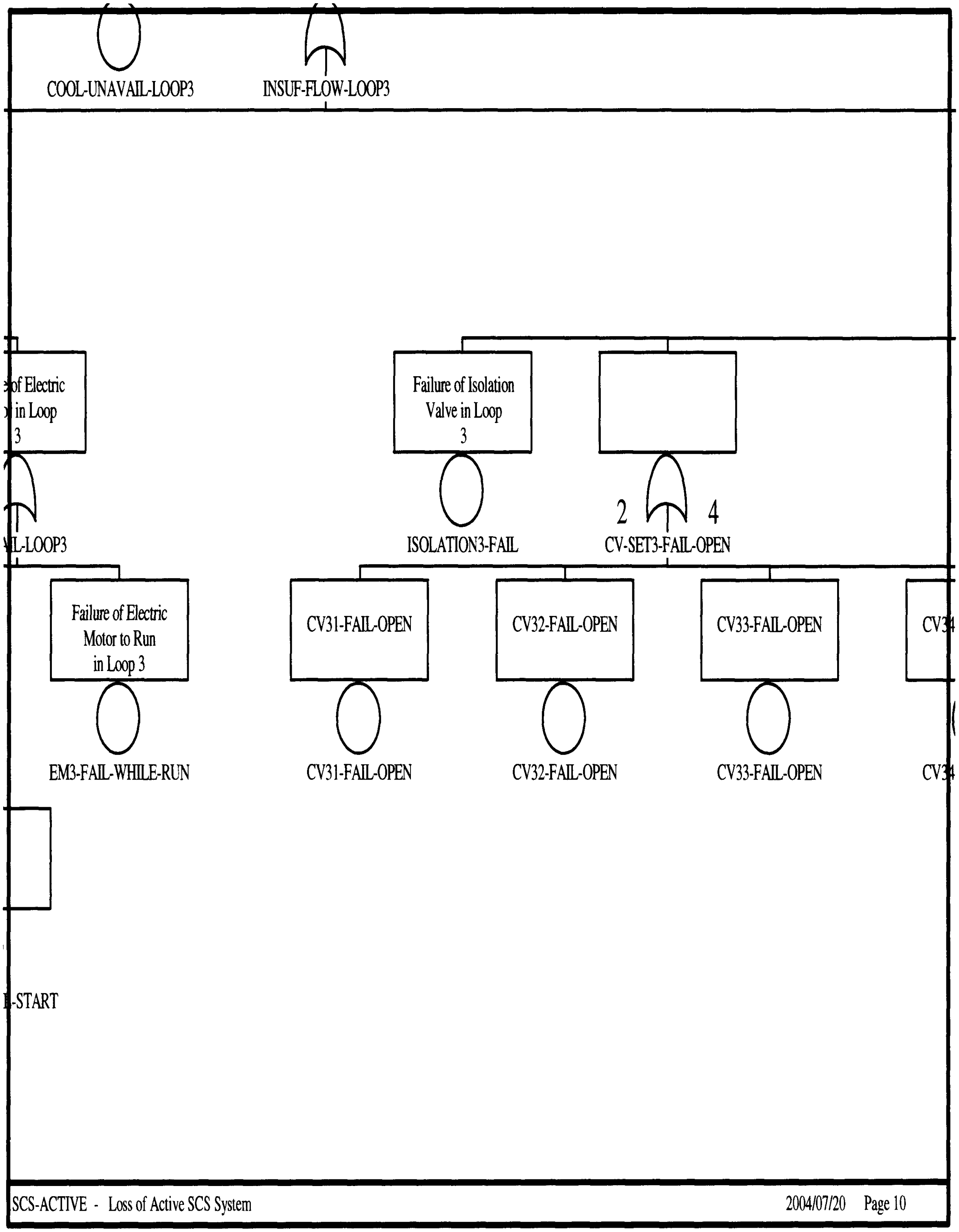


Figure IV-48 Fault Tree for Active SCS System in GFR: Zoom 30

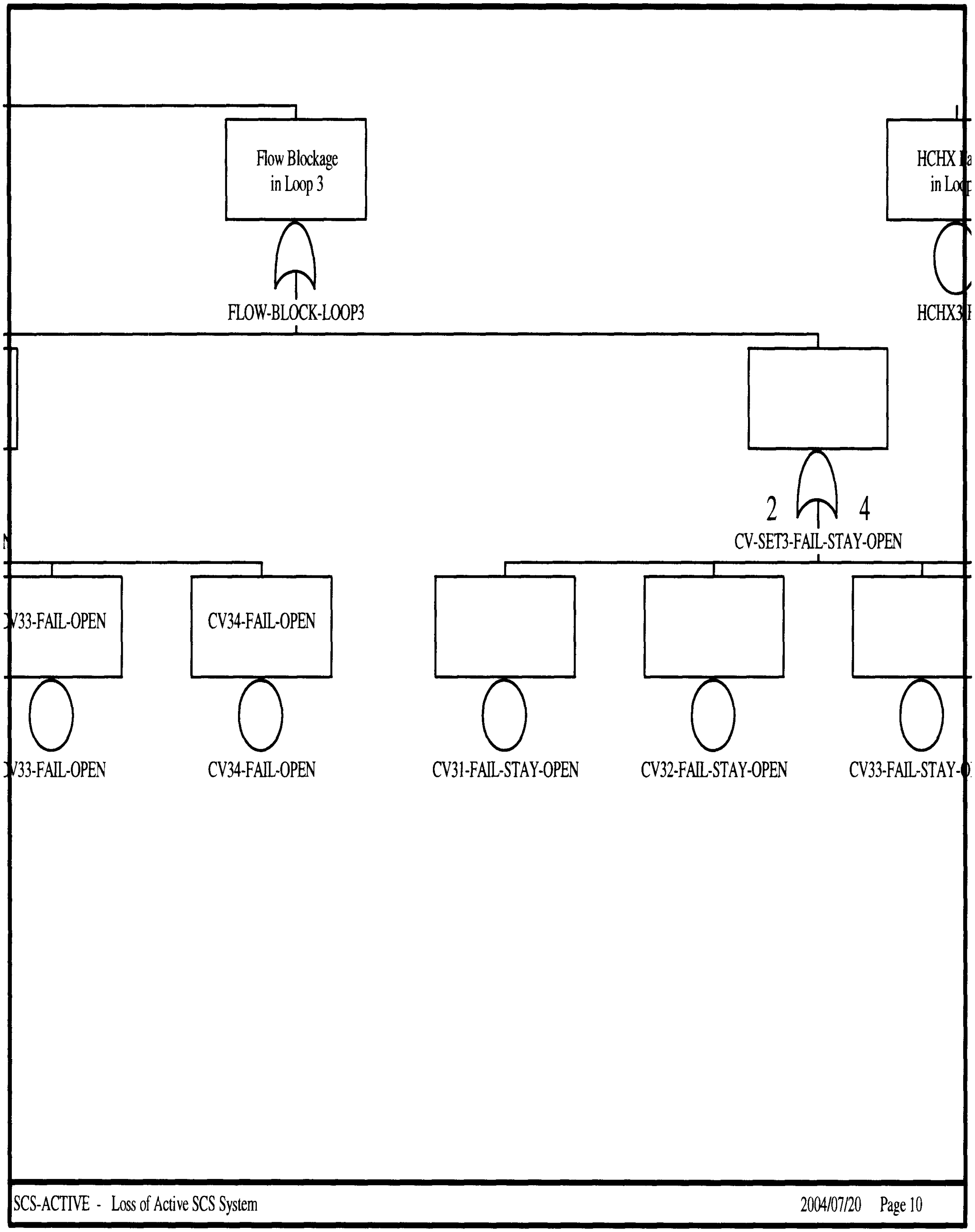


Figure IV-49 Fault Tree for Active SCS System in GFR: Zoom 31

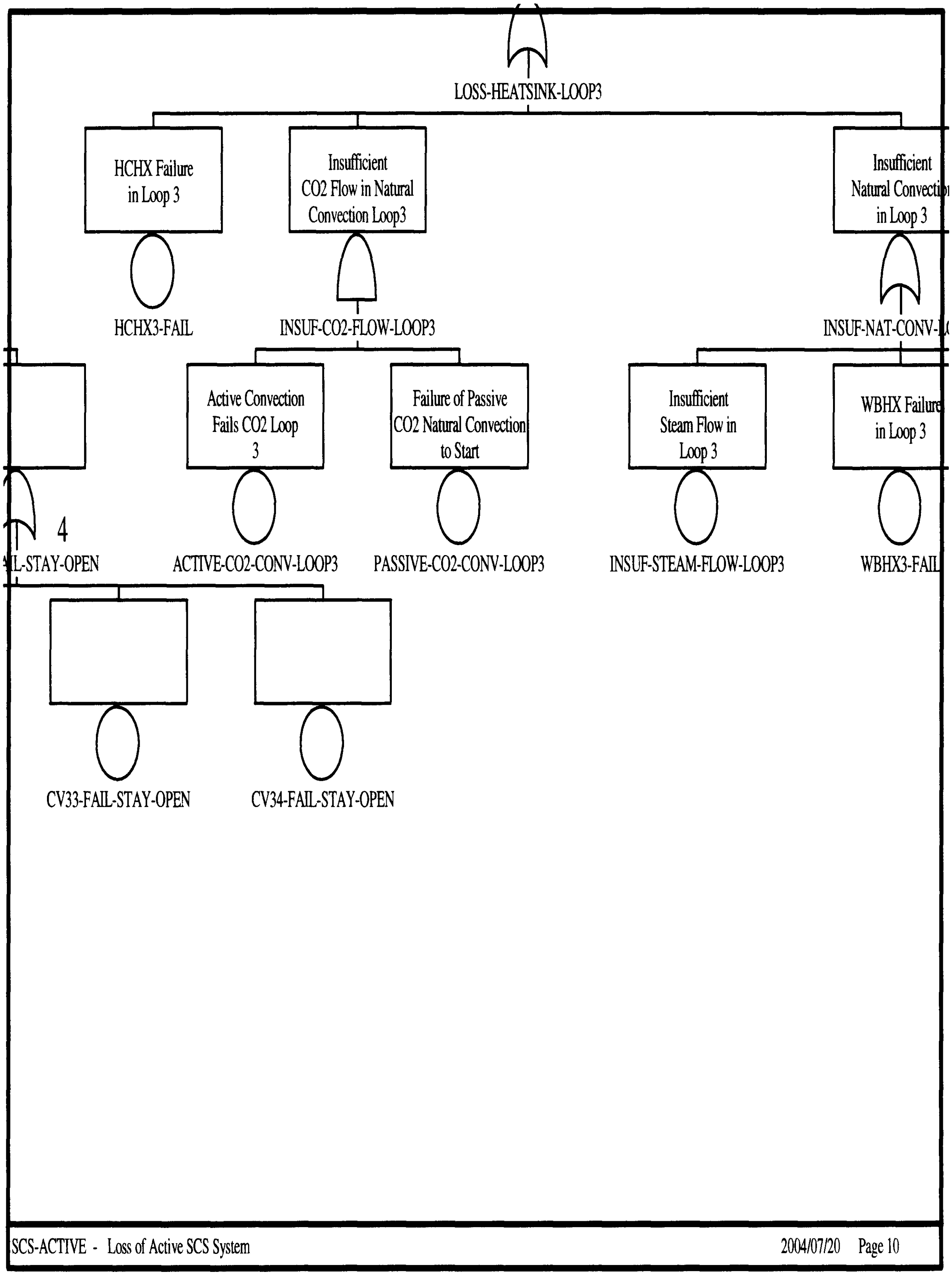


Figure IV-50 Fault Tree for Active SCS System in GFR: Zoom 32

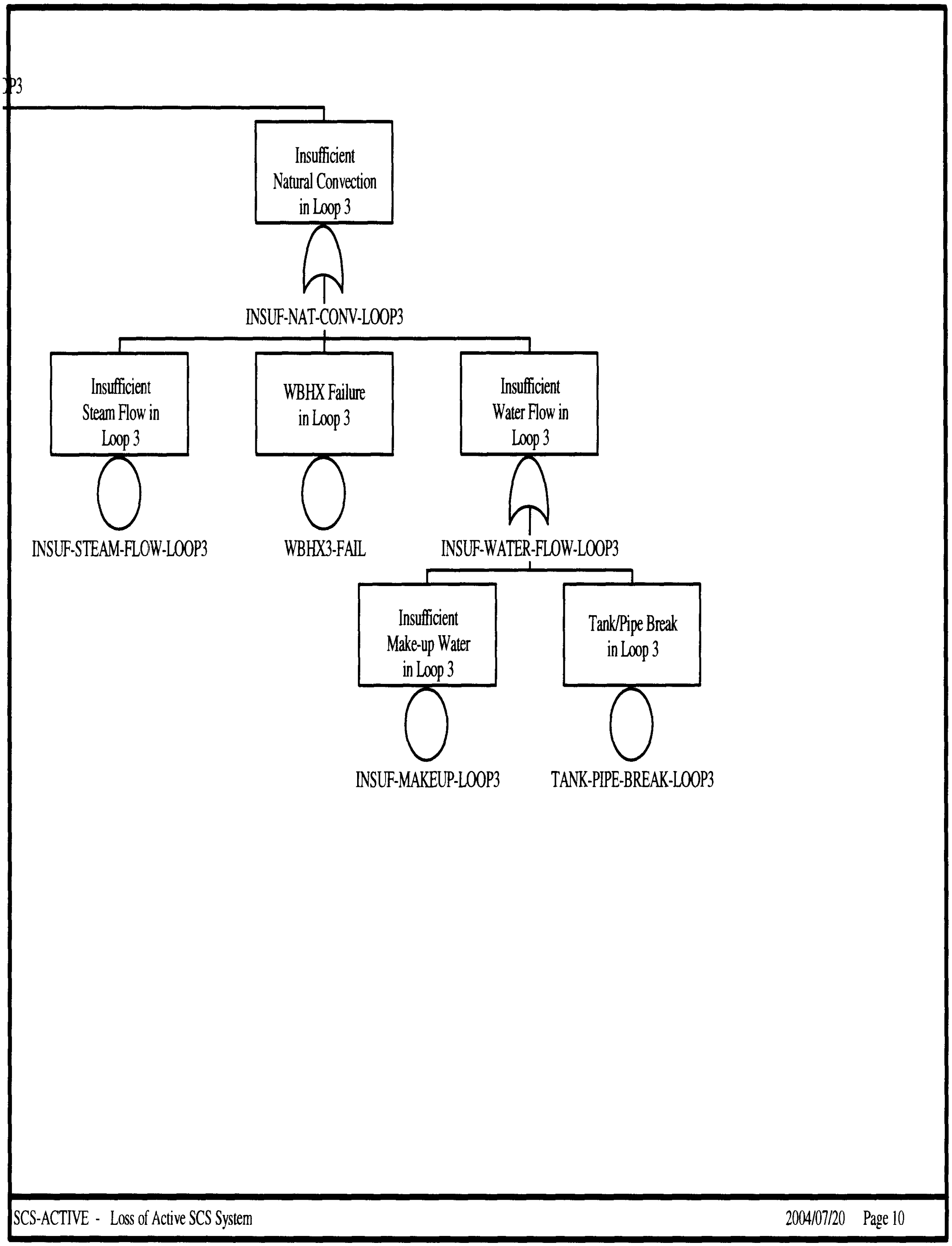

P3
Insufficient Natural Convection in Loop 3
INSUF-NAT-CONV-LOOP3
Insufficient Steam Flow in Loop 3
WBHX Failure in Loop 3
Insufficient Water Flow in Loop 3
INSUF-STEAM-FLOW-LOOP3
WBHX3-FAIL
INSUF-WATER-FLOW-LOOP3
Insufficient Make-up Water in Loop 3
Tank/Pipe Break in Loop 3
INSUF-MAKEUP-LOOP3
TANK-PIPE-BREAK-LOOP3
SCS-ACTIVE - Loss of Active SCS System
2004/07/20 Page 10

Figure IV-51 Fault Tree for Active SCS System in GFR: Zoom 33

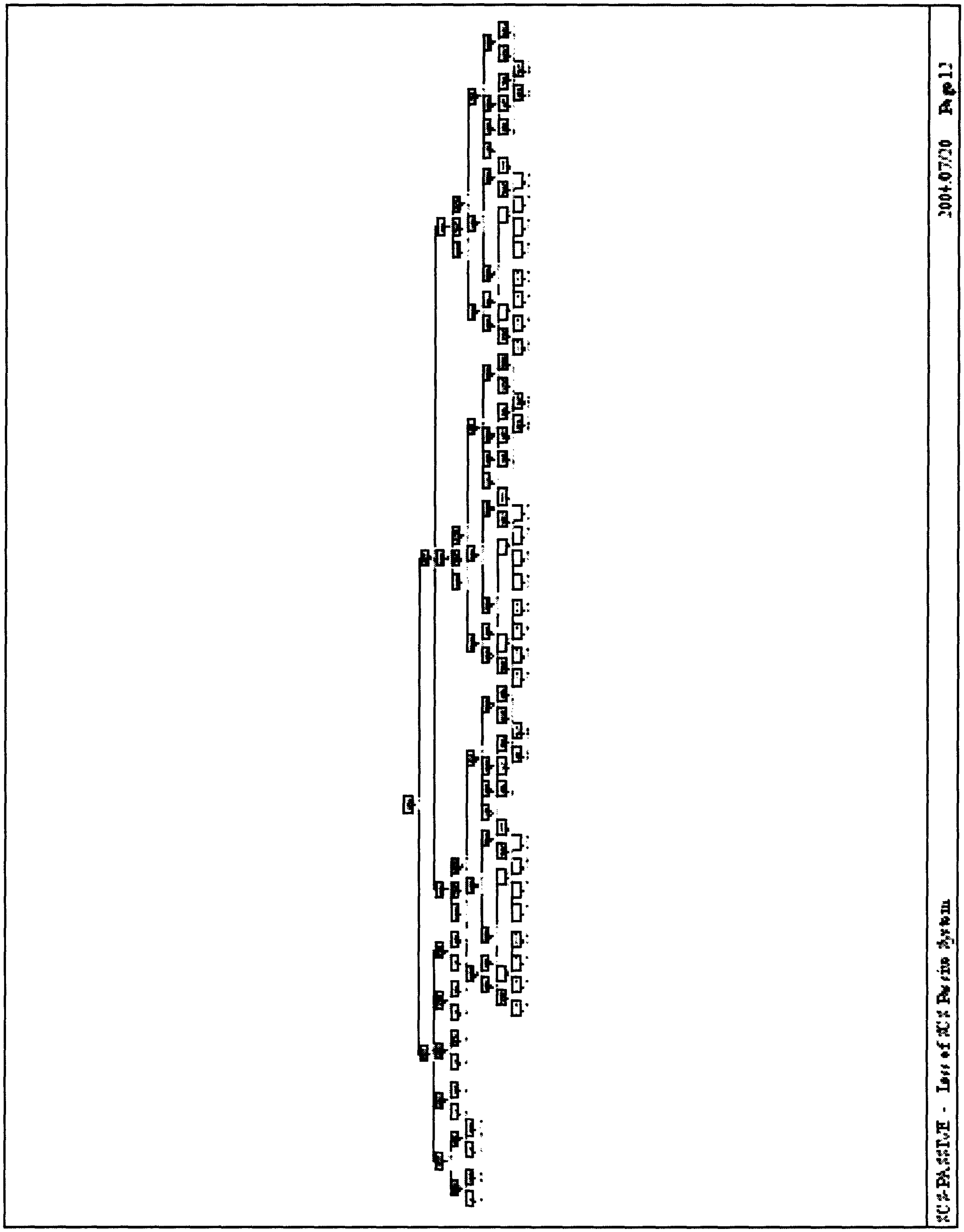


Figure IV-52 Fault Tree for Passive SCS System in GFR: Following "Zoomed In" Figures for enlarged, readable sections of the Fault Tree

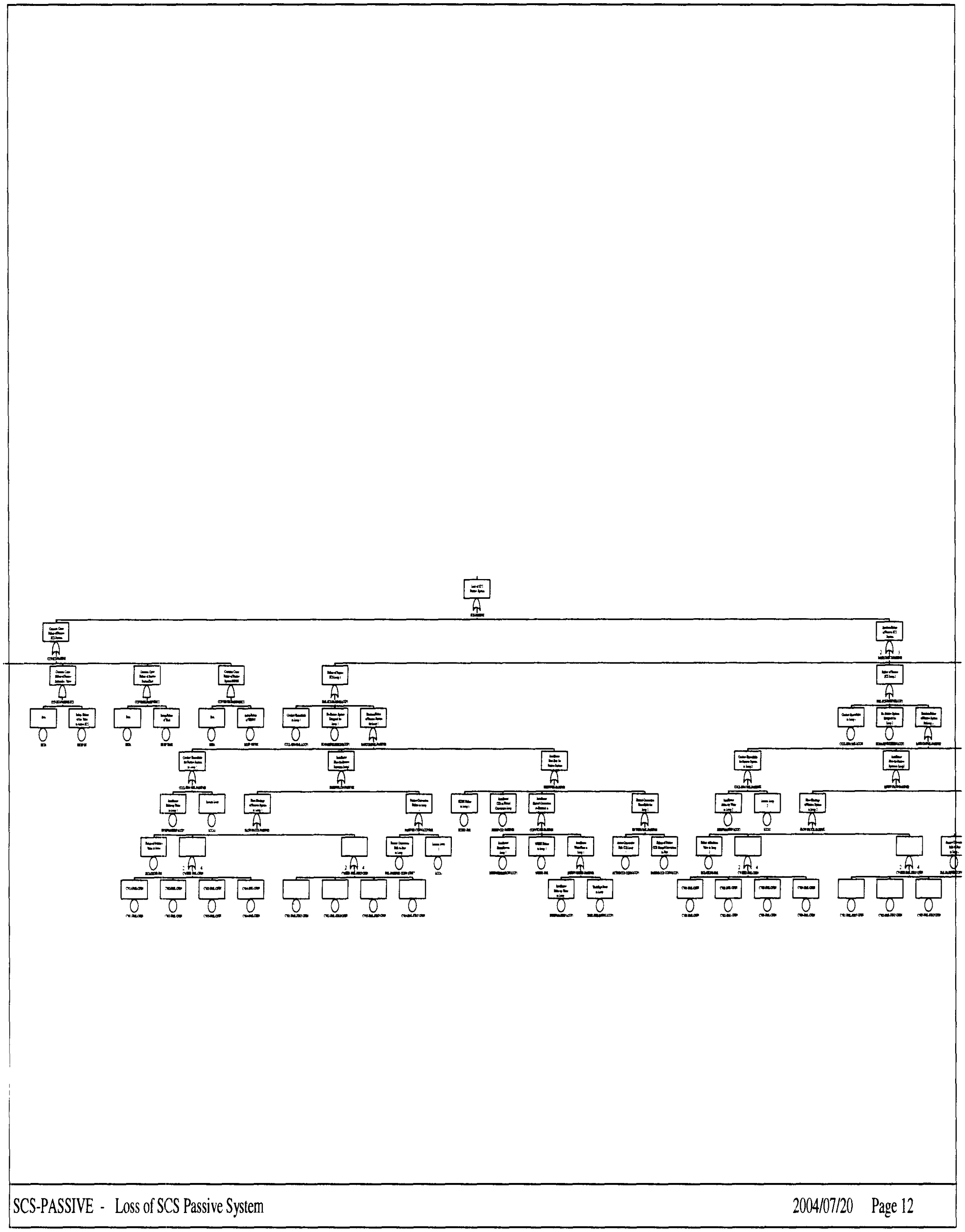


Figure IV-53 Fault Tree for Passive SCS System in GFR: Zoom 1

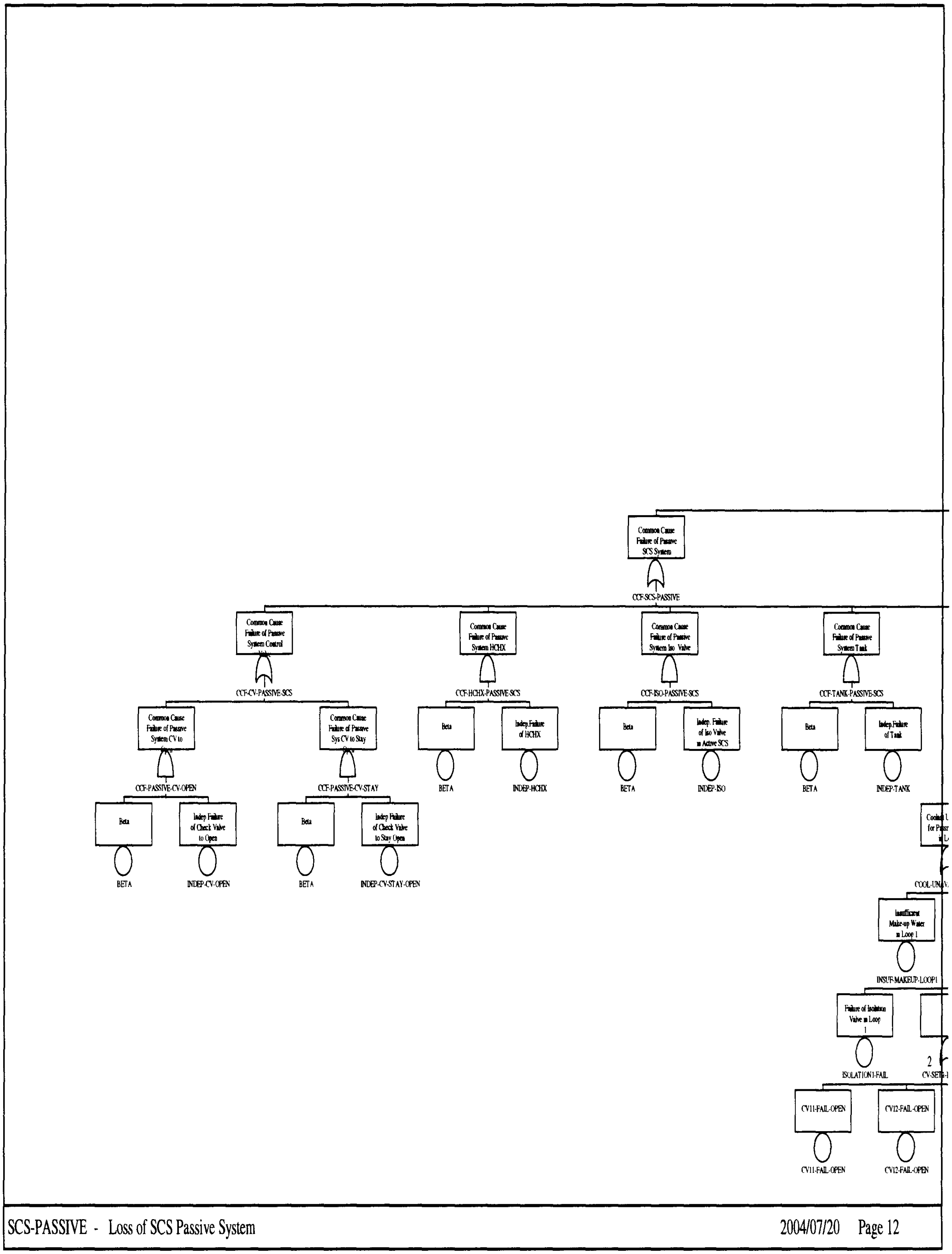

Common Cause Failure of Passive SCS System
CCF-SCS-PASSIVE
Common Cause Failure of Passive System Control Valve
CCF-CV-PASSIVE-SCS
Common Cause Failure of Passive System HCHX
CCF-HCHX-PASSIVE-SCS
Common Cause Failure of Passive System Iso Valve
CCF-ISO-PASSIVE-SCS
Common Cause Failure of Passive System Tank
CCF-TANK-PASSIVE-SCS
Common Cause Failure of Passive System CV to Open
CCF-PASSIVE-CV-OPEN
Common Cause Failure of Passive Sys CV to Stay Open
CCF-PASSIVE-CV-STAY
Beta
BETA
Indep.Failure of HCHX
INDEP-HCHX
Beta
BETA
Indep. Failure of Iso Valve in Active SCS
INDEP-ISO
Beta
BETA
Indep.Failure of Tank
INDEP-TANK
Beta
BETA
Indep Failure of Check Valve to Open
INDEP-CV-OPEN
Beta
BETA
Indep Failure of Check Valve to Stay Open
INDEP-CV-STAY-OPEN
COOL-UNAV
Insufficient Make-up Water in Loop 1
INSUF-MAKEUP-LOOP1
Failure of Isolation Valve in Loop 1
ISOLATION1-FAIL
2
CV-SET
CV11-FAIL-OPEN
CV11-FAIL-OPEN
CV12-FAIL-OPEN
CV12-FAIL-OPEN
SCS-PASSIVE - Loss of SCS Passive System
2004/07/20 Page 12

Figure IV-54 Fault Tree for Passive SCS System in GFR: Zoom 2

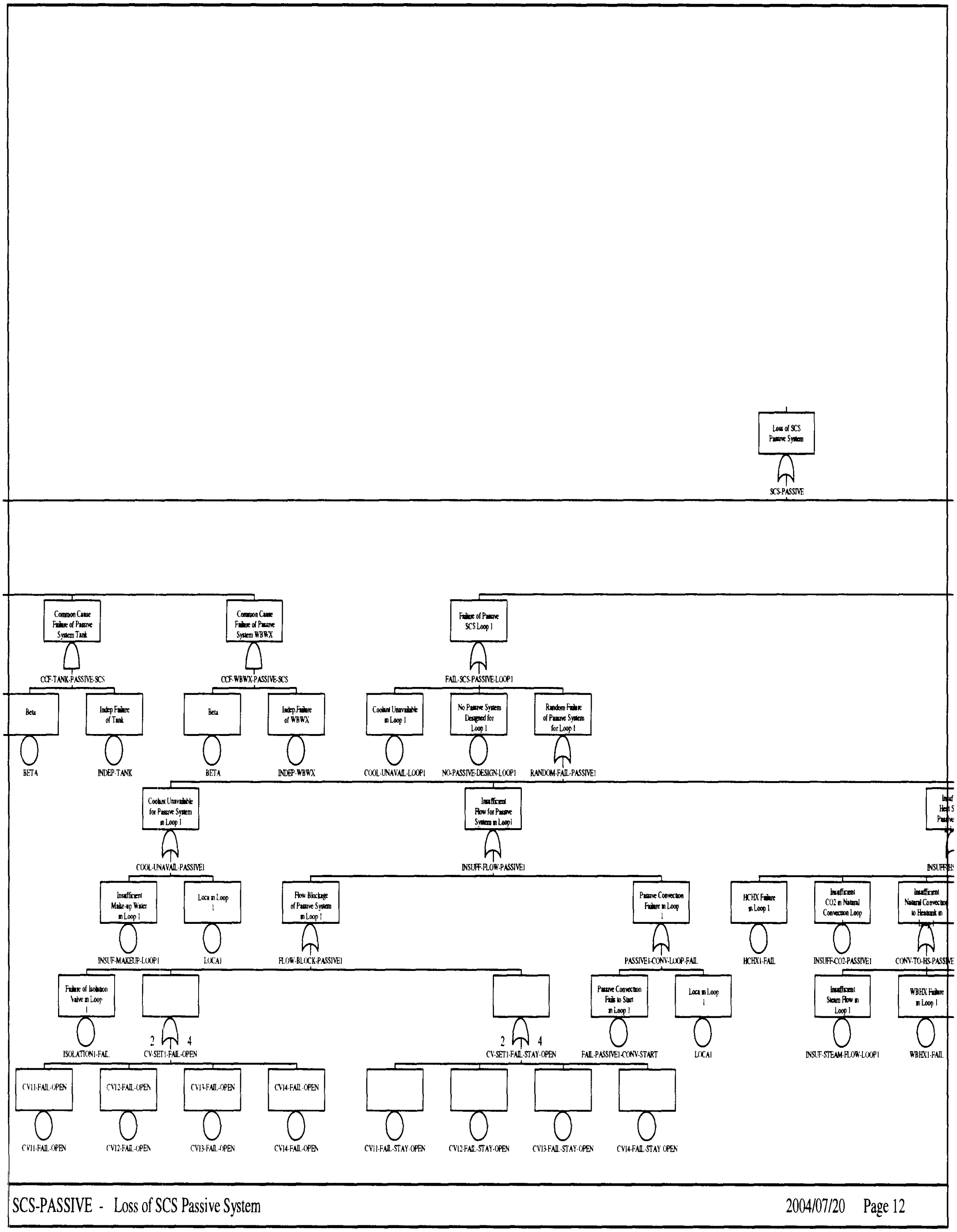


Figure IV-55 Fault Tree for Passive SCS System in GFR: Zoom 3

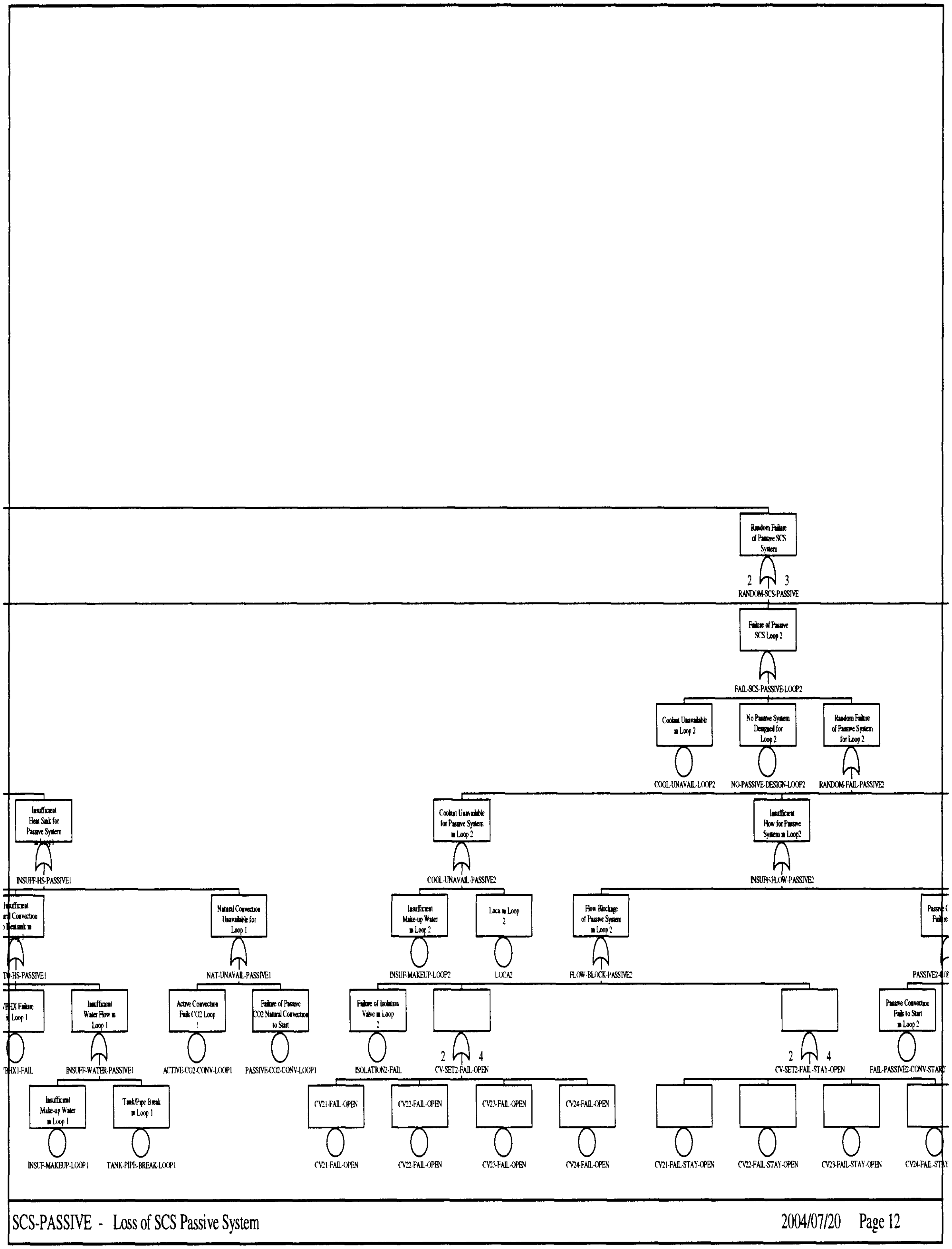

Random Failure of Passive SCS System
2
3
RANDOM-SCS-PASSIVE
Failure of Passive SCS Loop 2
FAIL-SCS-PASSIVE-LOOP2
Coolant Unavailable in Loop 2
COOL-UNAVAIL-LOOP2
No Passive System Designed for Loop 2
NO-PASSIVE-DESIGN-LOOP2
Random Failure of Passive System for Loop 2
RANDOM-FAIL-PASSIVE2
Insufficient Heat Sink for Passive System in Loop1
INSUFF-HS-PASSIVE1
Coolant Unavailable for Passive System in Loop 2
COOL-UNAVAIL-PASSIVE2
Insufficient Flow for Passive System in Loop2
INSUFF-FLOW-PASSIVE2
Insufficient ural Convection Heatsink in Loop 1
TO-HS-PASSIVE1
Natural Convection Unavailable for Loop 1
NAT-UNAVAIL-PASSIVE1
Insufficient Make-up Water in Loop 2
INSUF-MAKEUP-LOOP2
Loca in Loop 2
LOCA2
Flow Blockage of Passive System in Loop 2
FLOW-BLOCK-PASSIVE2
Passive C Failure
PASSIVE2-
/BHX Failure in Loop 1
BHX1-FAIL
Insufficient Water Flow in Loop 1
INSUFF-WATER-PASSIVE1
Active Convection Fails CO2 Loop 1
ACTIVE-CO2-CONV-LOOP1
Failure of Passive CO2 Natural Convection to Start
PASSIVE-CO2-CONV-LOOP1
Failure of Isolation Valve in Loop 2
ISOLATION2-FAIL
2
4
CV-SET2-FAIL-OPEN
2
4
CV-SET2-FAIL-STAY-OPEN
Passive Convection Fails to Start in Loop 2
FAIL-PASSIVE2-CONV-START
Insufficient Make-up Water in Loop 1
INSUF-MAKEUP-LOOP1
Tank/Pipe Break in Loop 1
TANK-PIPE-BREAK-LOOP1
CV21-FAIL-OPEN
CV21-FAIL-OPEN
CV22-FAIL-OPEN
CV22-FAIL-OPEN
CV23-FAIL-OPEN
CV23-FAIL-OPEN
CV24-FAIL-OPEN
CV24-FAIL-OPEN
CV21-FAIL-STAY-OPEN
CV22-FAIL-STAY-OPEN
CV23-FAIL-STAY-OPEN
CV24-FAIL-STAY
SCS-PASSIVE - Loss of SCS Passive System
2004/07/20 Page 12

Figure IV-56 Fault Tree for Passive SCS System in GFR: Zoom 4

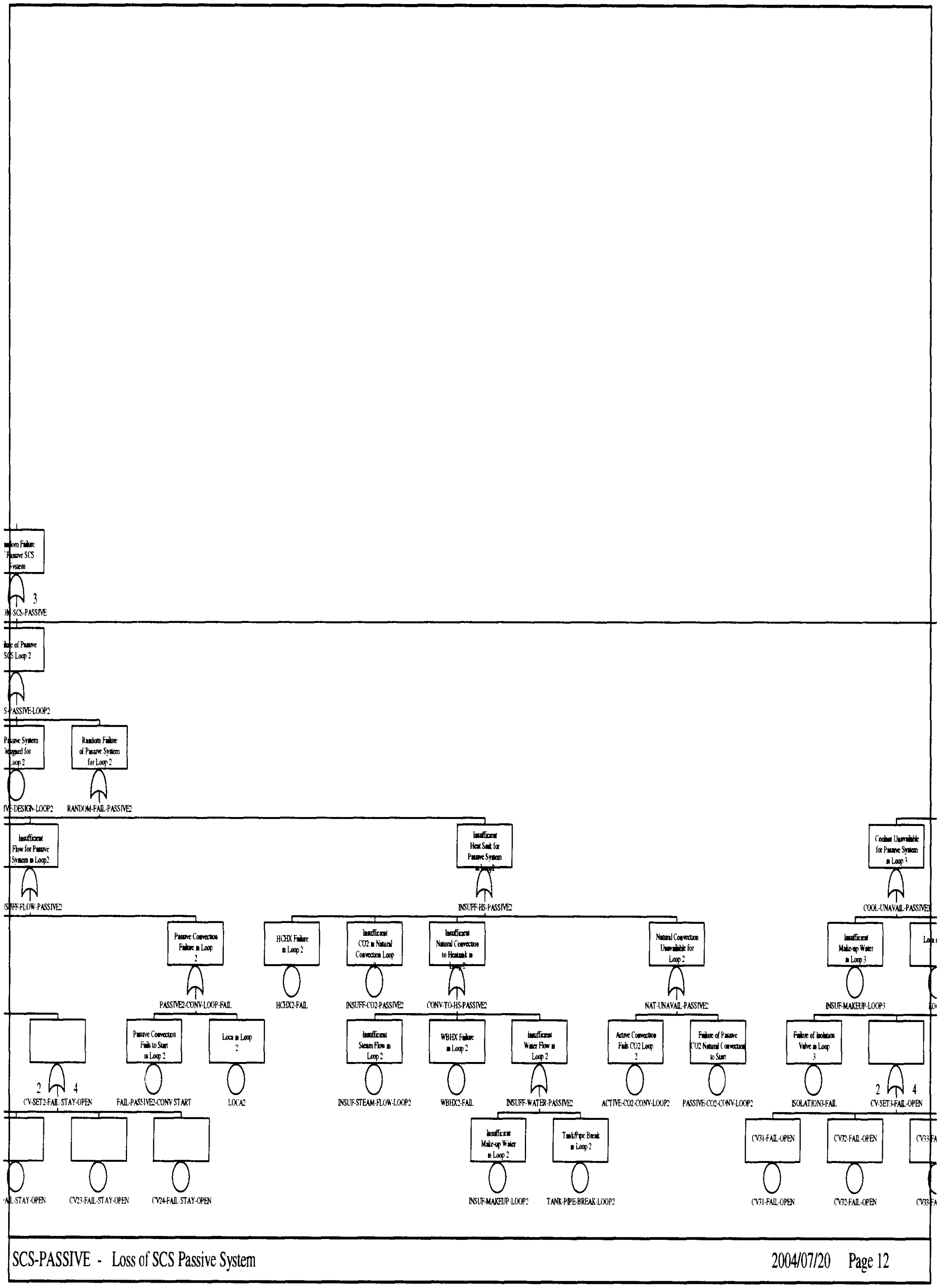


Figure IV-57 Fault Tree for Passive SCS System in GFR: Zoom 5

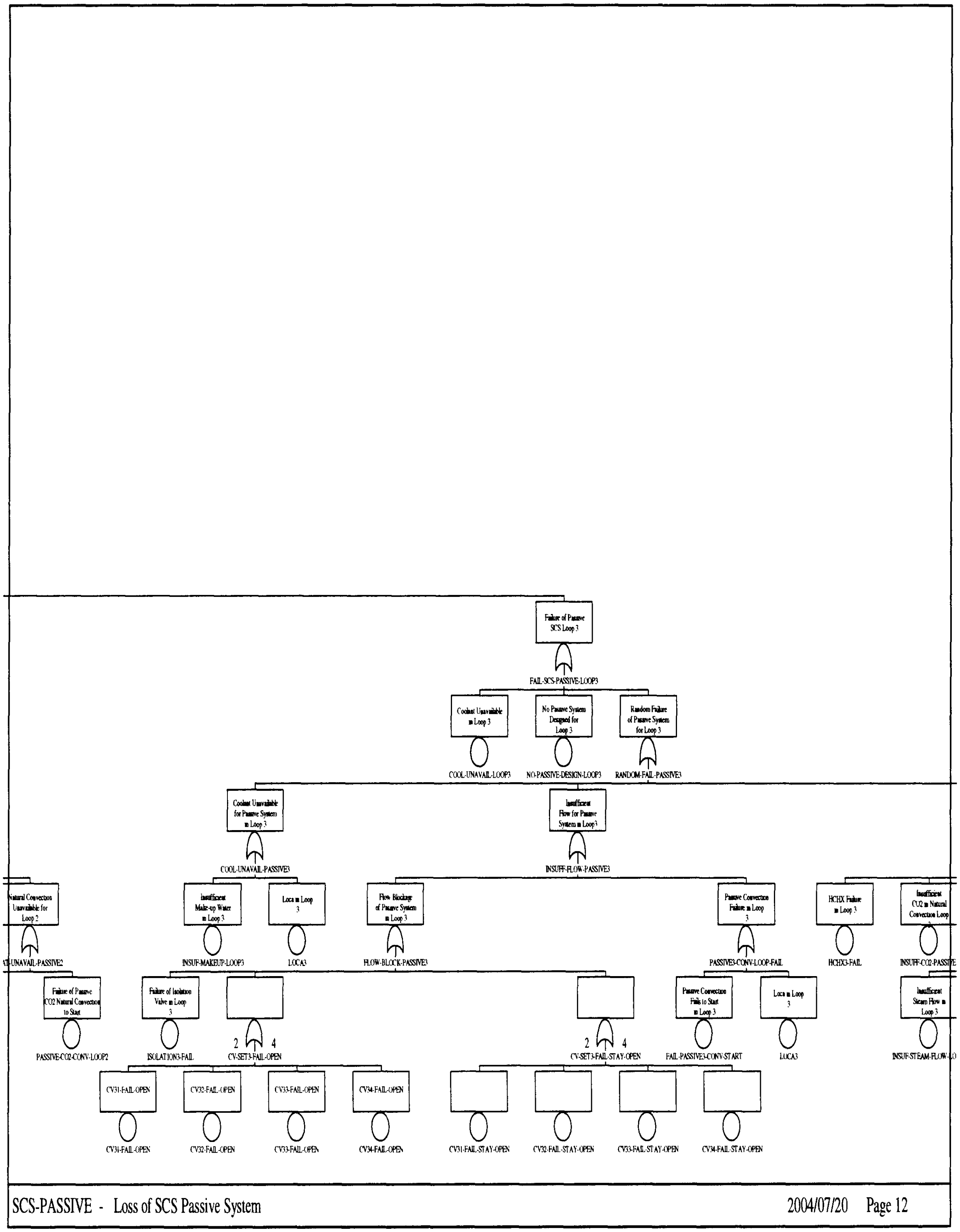

Failure of Passive SCS Loop 3
FAIL-SCS-PASSIVE-LOOP3
Coolant Unavailable in Loop 3
COOL-UNAVAIL-LOOP3
No Passive System Designed for Loop 3
NO-PASSIVE-DESIGN-LOOP3
Random Failure of Passive System for Loop 3
RANDOM-FAIL-PASSIVE3
Coolant Unavailable for Passive System in Loop 3
COOL-UNAVAIL-PASSIVE3
Insufficent Flow for Passive System in Loop3
INSUFF-FLOW-PASSIVE3
Natural Convection Unavailable for Loop 2
AT-UNAVAIL-PASSIVE2
Failure of Passive CO2 Natural Convection to Start
PASSIVE-CO2-CONV-LOOP2
Insufficent Make-up Water in Loop 3
INSUF-MAKEUP-LOOP3
Loca in Loop 3
LOCA3
Failure of Isolation Valve in Loop 3
ISOLATION3-FAIL
2
4
CV-SET3-FAIL-OPEN
CV31-FAIL-OPEN
CV32-FAIL-OPEN
CV33-FAIL-OPEN
CV34-FAIL-OPEN
CV31-FAIL-OPEN
CV32-FAIL-OPEN
CV33-FAIL-OPEN
CV34-FAIL-OPEN
Flow Blockage of Passive System in Loop 3
FLOW-BLOCK-PASSIVE3
2
4
CV-SET3-FAIL-STAY-OPEN
CV31-FAIL-STAY-OPEN
CV32-FAIL-STAY-OPEN
CV33-FAIL-STAY-OPEN
CV34-FAIL-STAY-OPEN
Passive Convection Failure in Loop 3
PASSIVE3-CONV-LOOP-FAIL
Passive Convection Fails to Start in Loop 3
FAIL-PASSIVE3-CONV-START
Loca in Loop 3
LUCA3
HCHX Failure in Loop 3
HCHX3-FAIL
Insufficent CO2 in Natural Convection Loop
INSUFF-CO2-PASSIVE
Insufficent Steam Flow in Loop 3
INSUF-STEAM-FLOW-LO
SCS-PASSIVE - Loss of SCS Passive System
2004/07/20
Page 12

Figure IV-58 Fault Tree for Passive SCS System in GFR: Zoom 6

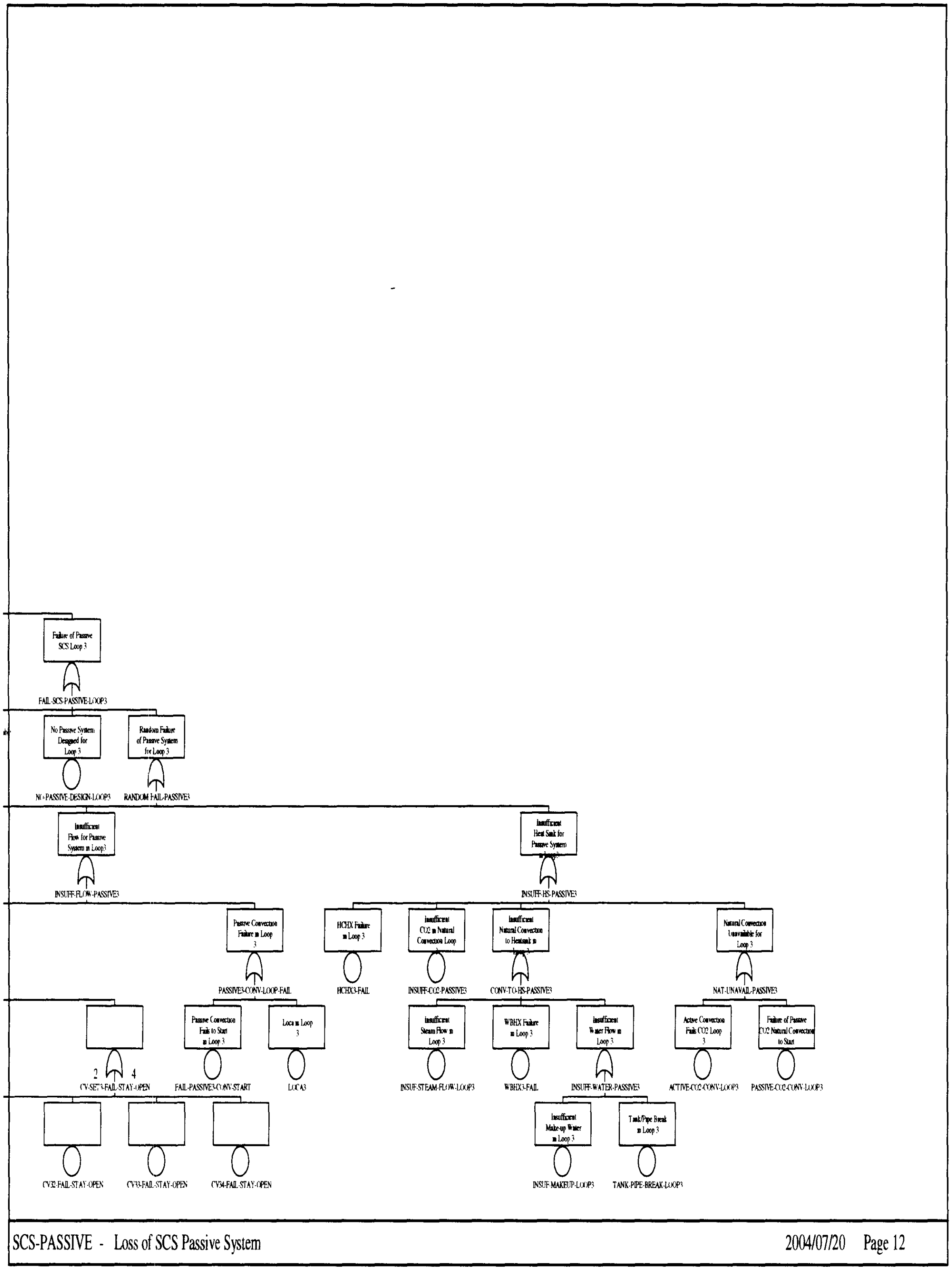

Failure of Passive SCS Loop 3
FAIL-SCS-PASSIVE-LOOP3
No Passive System Designed for Loop 3
NO-PASSIVE-DESIGN-LOOP3
Random Failure of Passive System for Loop 3
RANDOM FAIL-PASSIVE3
Insufficient Flow for Passive System in Loop3
INSUFF-FLOW-PASSIVE3
Insufficient Heat Sink for Passive System in Loop3
INSUFF-HS-PASSIVE3
Passive Convection Failure in Loop 3
PASSIVE3-CONV-LOOP-FAIL
HCHX Failure in Loop 3
HCHX3-FAIL
Insufficient CO2 in Natural Convection Loop 3
INSUFF-CO2-PASSIVE3
Insufficient Natural Convection to Heatsink in Loop 3
CONV-TO-HS-PASSIVE3
Natural Convection Unavailable for Loop 3
NAT-UNAVAIL-PASSIVE3
2
4
CV-SET3-FAIL-STAY-OPEN
Passive Convection Fails to Start in Loop 3
FAIL-PASSIVE3-CONV-START
Loca in Loop 3
LOCA3
Insufficient Steam Flow in Loop 3
INSUF-STEAM-FLOW-LOOP3
WBHX Failure in Loop 3
WBHX3-FAIL
Insufficient Water Flow in Loop 3
INSUFF-WATER-PASSIVE3
Active Convection Fails CO2 Loop 3
ACTIVE-CO2-CONV-LOOP3
Failure of Passive CO2 Natural Convection to Start
PASSIVE-CO2-CONV-LOOP3
CV32-FAIL-STAY-OPEN
CV33-FAIL-STAY-OPEN
CV34-FAIL-STAY-OPEN
Insufficient Make-up Water in Loop 3
INSUF-MAKEUP-LOOP3
Tank/Pipe Break in Loop 3
TANK-PIPE-BREAK-LOOP3
SCS-PASSIVE - Loss of SCS Passive System
2004/07/20
Page 12

Figure IV-59 Fault Tree for Passive SCS System in GFR: Zoom 7

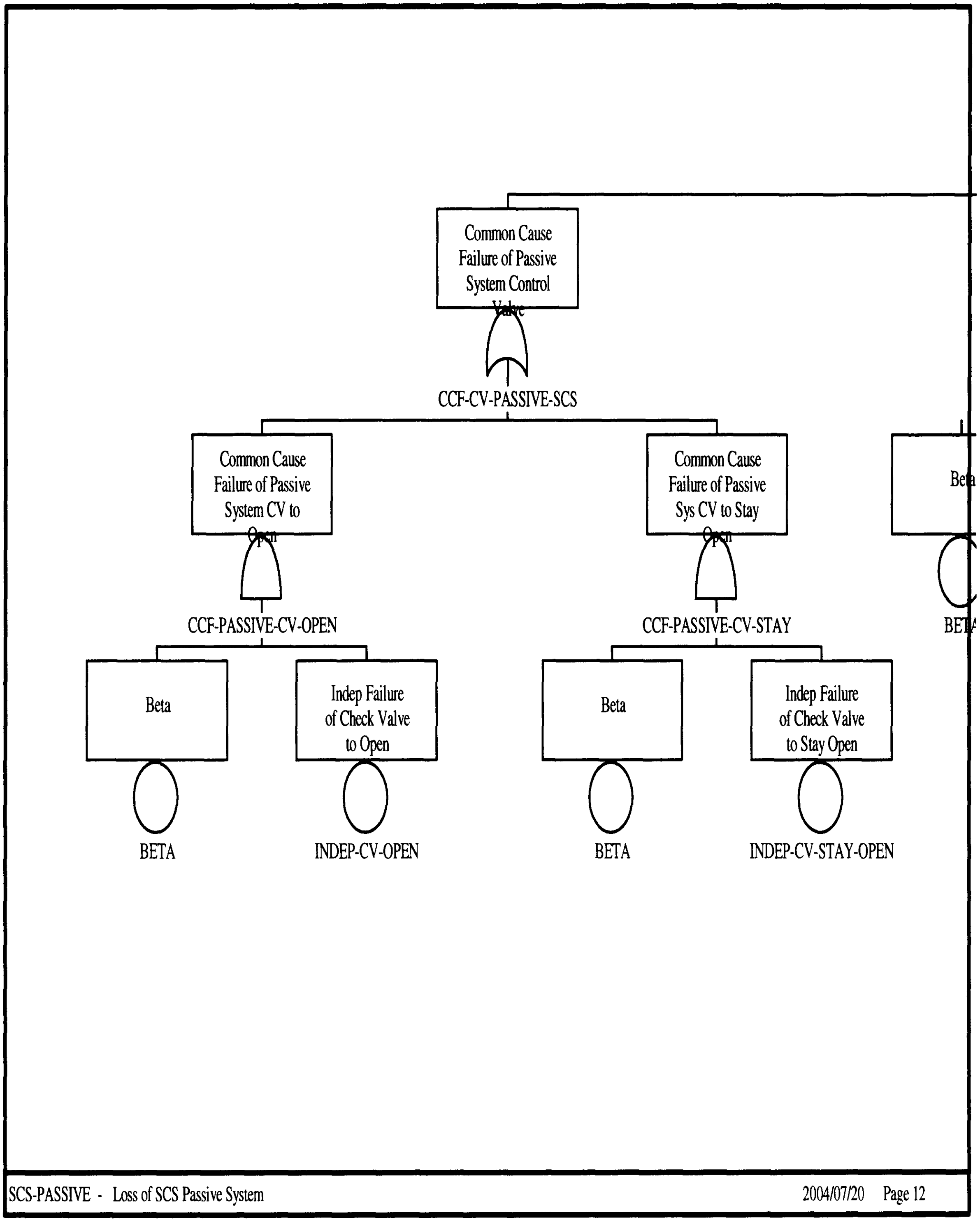


Figure IV-60 Fault Tree for Passive SCS System in GFR: Zoom 8

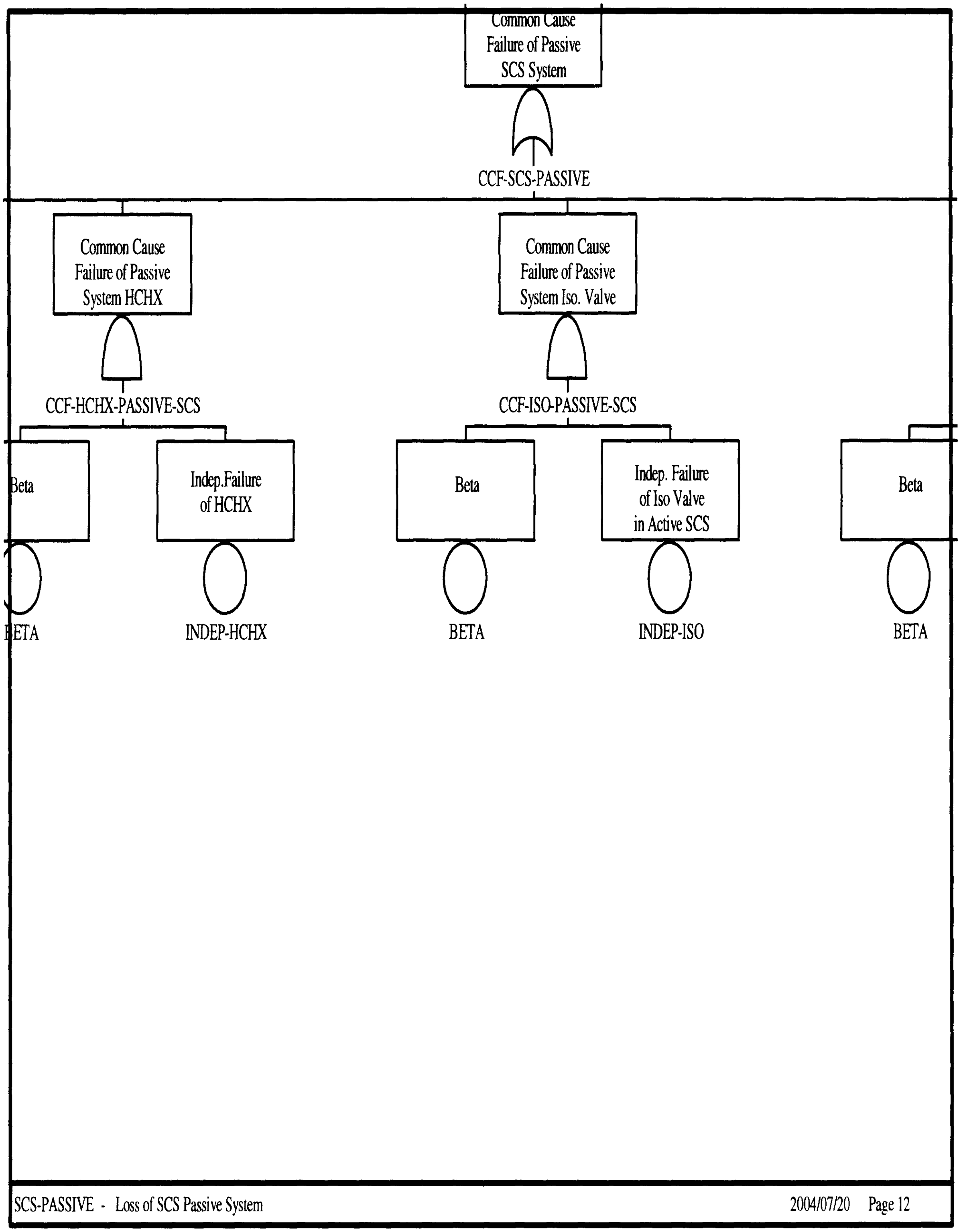


Figure IV-61 Fault Tree for Passive SCS System in GFR: Zoom 9

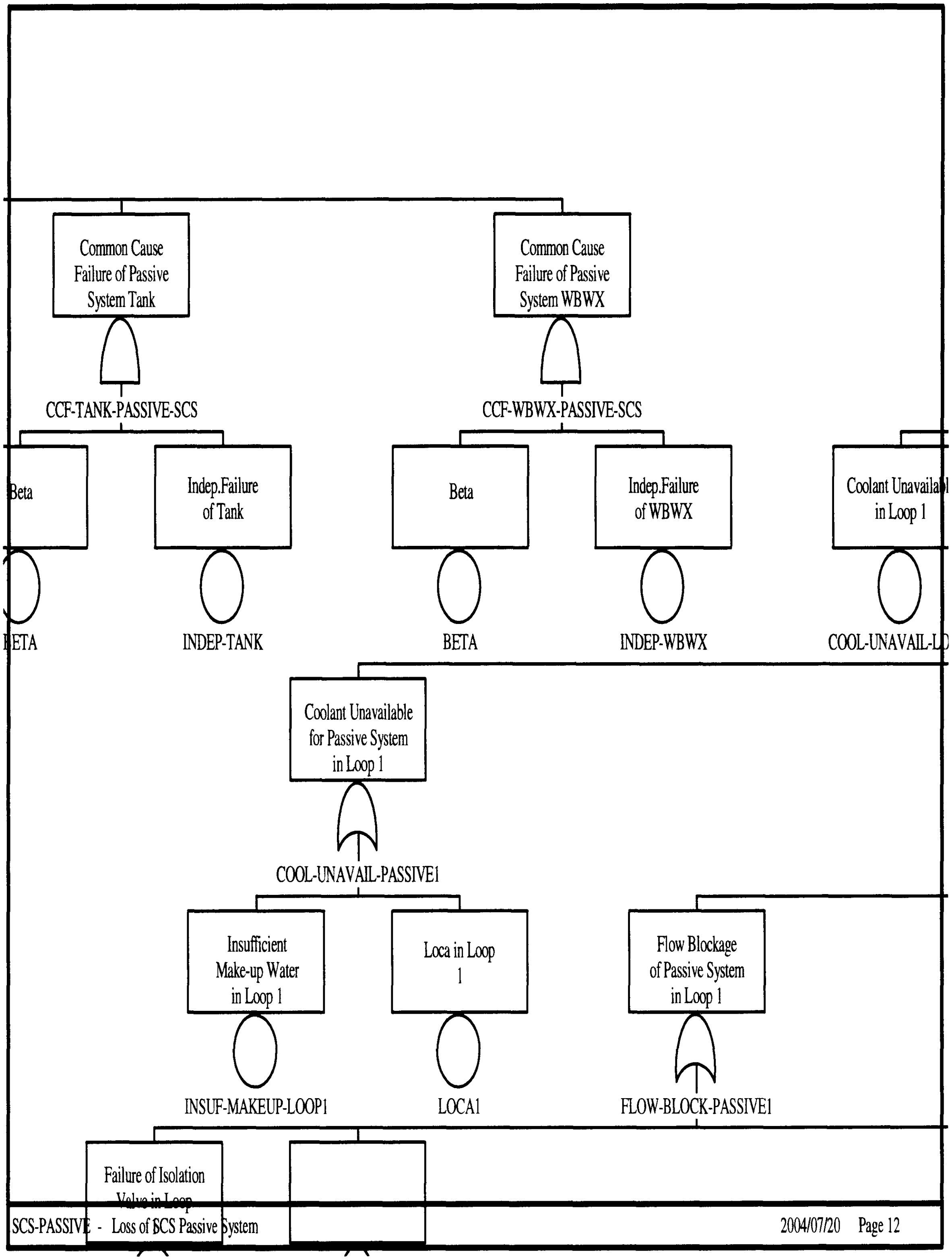

Common Cause Failure of Passive System Tank
CCF-TANK-PASSIVE-SCS
Common Cause Failure of Passive System WBWX
CCF-WBWX-PASSIVE-SCS
Beta
BETA
Indep.Failure of Tank
INDEP-TANK
Beta
BETA
Indep.Failure of WBWX
INDEP-WBWX
Coolant Unavaila l in Loop 1
COOL-UNAVAIL-L
Coolant Unavailable for Passive System in Loop 1
COOL-UNAVAIL-PASSIVE1
Insufficient Make-up Water in Loop 1
INSUF-MAKEUP-LOOP1
Loca in Loop 1
LOCA1
Flow Blockage of Passive System in Loop 1
FLOW-BLOCK-PASSIVE1
Failure of Isolation Valve in Loop
SCS-PASSIVE - Loss of SCS Passive System
2004/07/20 Page 12

Figure IV-62 Fault Tree for Passive SCS System in GFR: Zoom 10

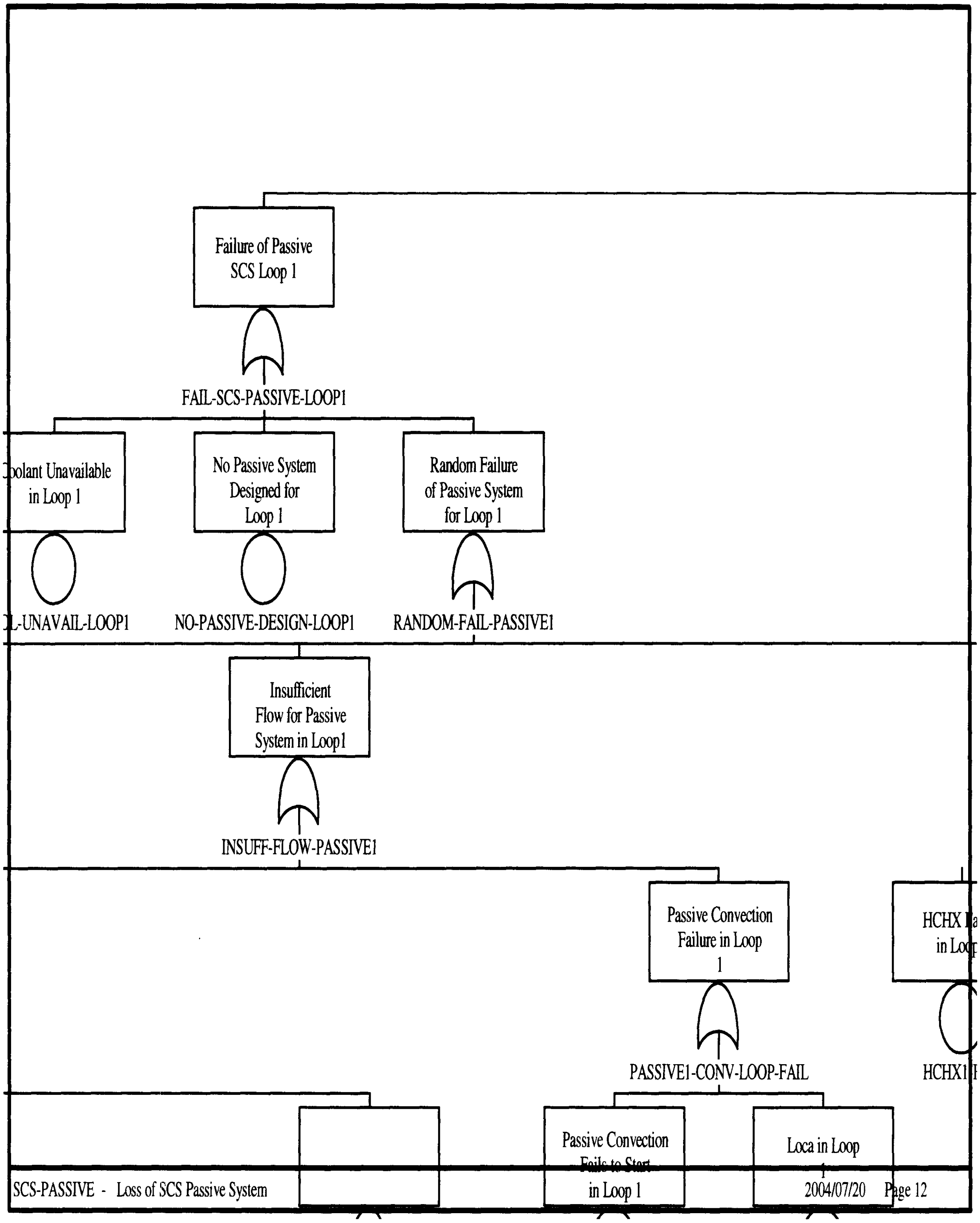

Failure of Passive SCS Loop 1
FAIL-SCS-PASSIVE-LOOP1
olant Unavailable in Loop 1
L-UNAVAIL-LOOP1
No Passive System Designed for Loop 1
NO-PASSIVE-DESIGN-LOOP1
Random Failure of Passive System for Loop 1
RANDOM-FAIL-PASSIVE1
Insufficient Flow for Passive System in Loop1
INSUFF-FLOW-PASSIVE1
Passive Convection Failure in Loop 1
PASSIVE1-CONV-LOOP-FAIL
HCHX Fa in Loop
HCHX1
Passive Convection Fails to Start in Loop 1
Loca in Loop 1
SCS-PASSIVE - Loss of SCS Passive System
2004/07/20
Page 12

Figure IV-63 Fault Tree for Passive SCS System in GFR: Zoom 11

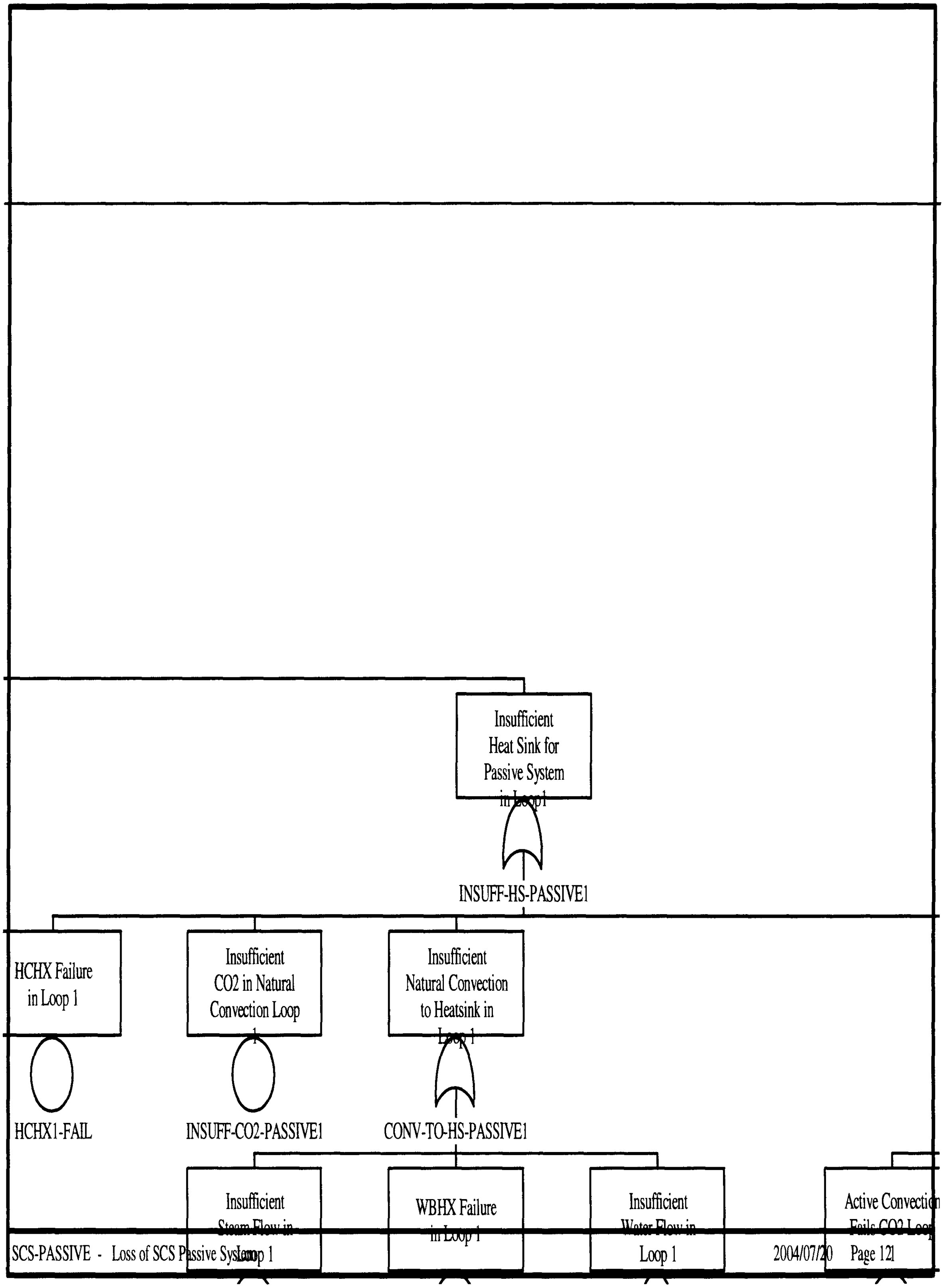

Insufficient Heat Sink for Passive System in Loop1
INSUFF-HS-PASSIVE1
HCHX Failure in Loop 1
HCHX1-FAIL
Insufficient CO2 in Natural Convection Loop 1
INSUFF-CO2-PASSIVE1
Insufficient Natural Convection to Heatsink in Loop 1
CONV-TO-HS-PASSIVE1
Insufficient Steam Flow in Loop 1
WBHX Failure in Loop 1
Insufficient Water Flow in Loop 1
Active Convection Fails CO2 Loop
SCS-PASSIVE - Loss of SCS Passive System
2004/07/20
Page 121

Figure IV-64 Fault Tree for Passive SCS System in GFR: Zoom 12

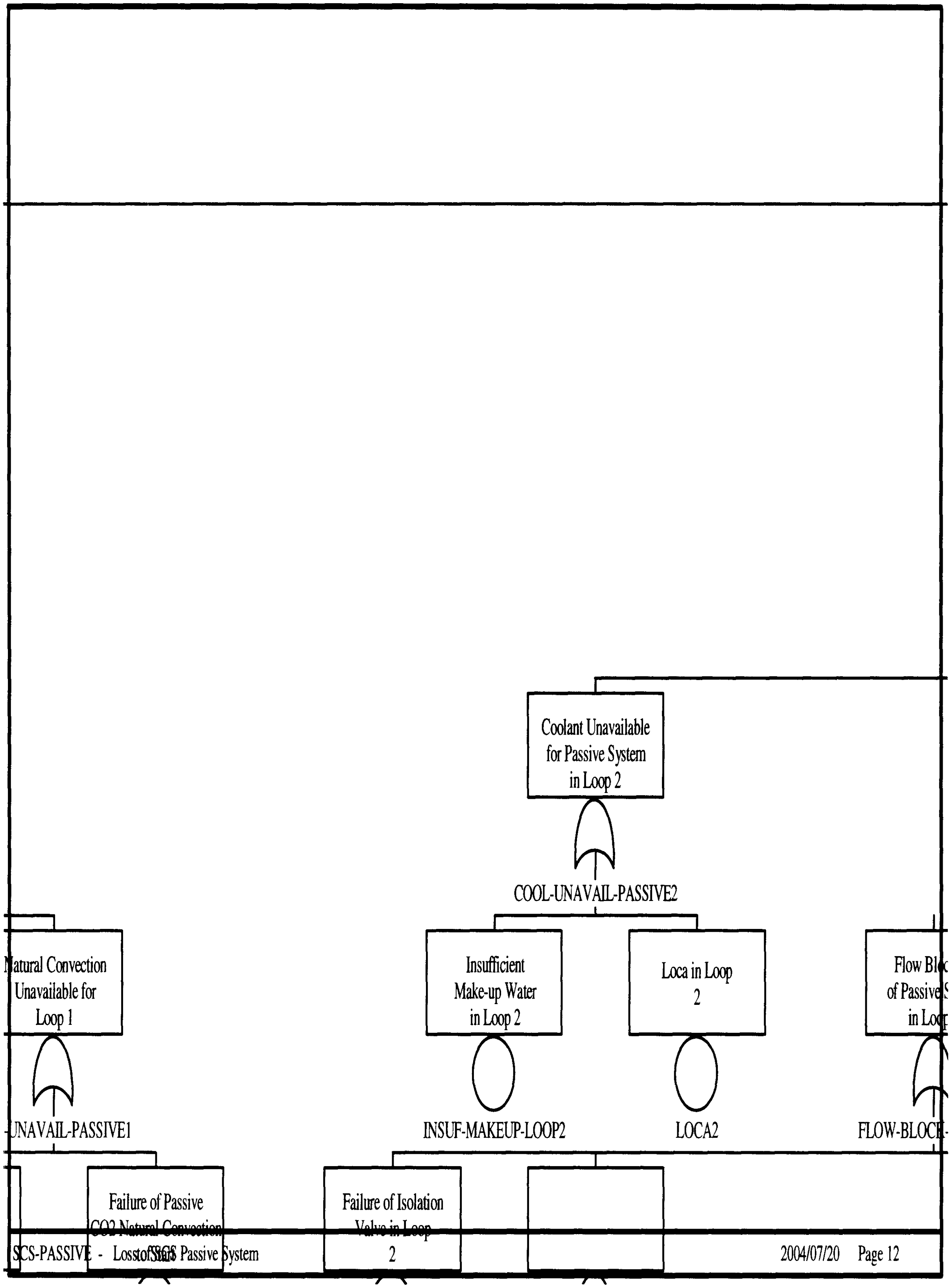

Coolant Unavailable for Passive System in Loop 2
COOL-UNAVAIL-PASSIVE2
Natural Convection Unavailable for Loop 1
-UNAVAIL-PASSIVE1
Insufficient Make-up Water in Loop 2
INSUF-MAKEUP-LOOP2
Loca in Loop 2
LOCA2
Flow Bl of Passive in Lo
FLOW-BLOC
Failure of Passive CO2 Natural Convection
Failure of Isolation Valve in Loop 2
SCS-PASSIVE - Loss of SCS Passive System
2004/07/20 Page 12

Figure IV-65 Fault Tree for Passive SCS System in GFR: Zoom 13

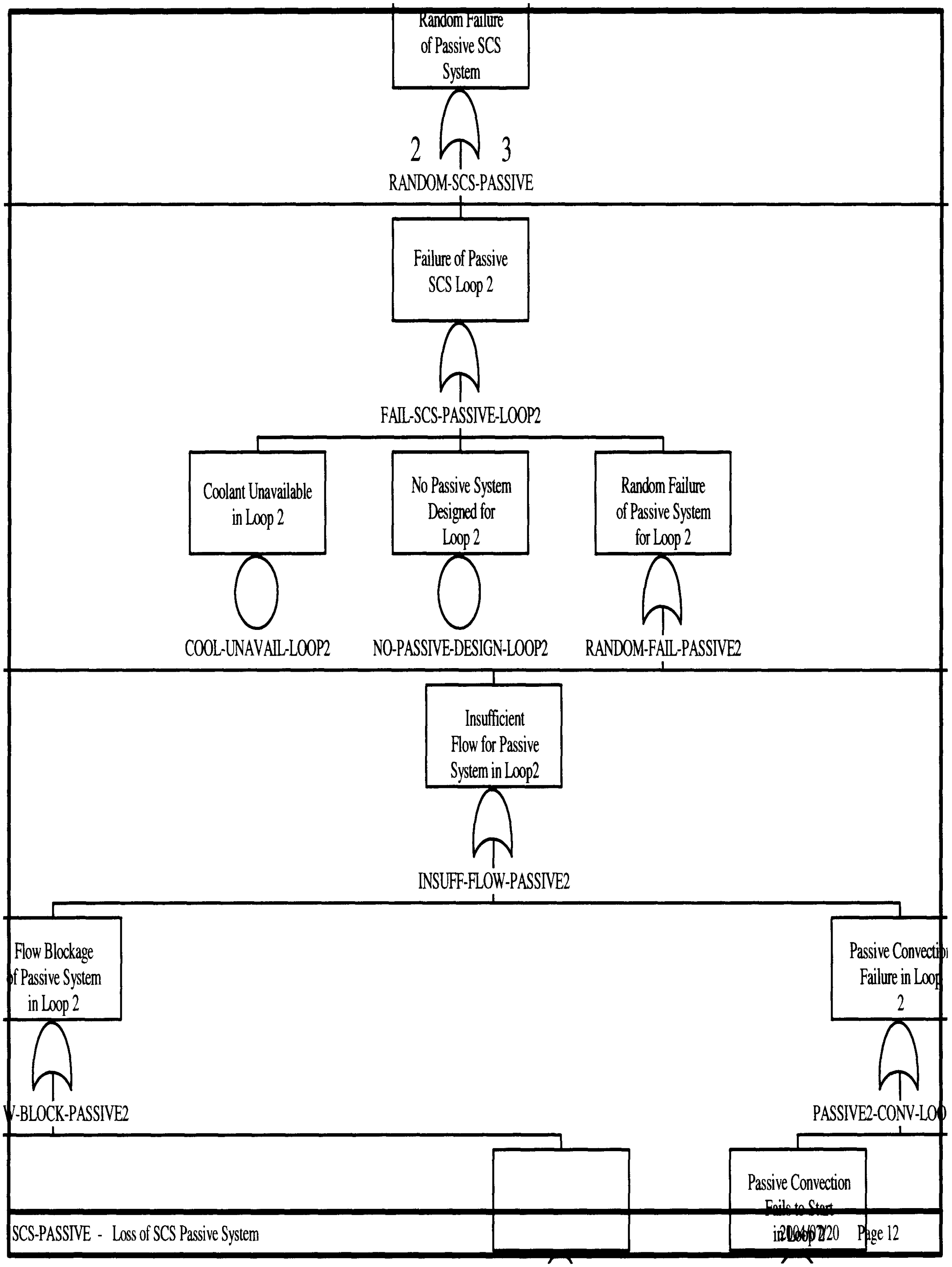

Random Failure of Passive SCS System
2
3
RANDOM-SCS-PASSIVE
Failure of Passive SCS Loop 2
FAIL-SCS-PASSIVE-LOOP2
Coolant Unavailable in Loop 2
COOL-UNAVAIL-LOOP2
No Passive System Designed for Loop 2
NO-PASSIVE-DESIGN-LOOP2
Random Failure of Passive System for Loop 2
RANDOM-FAIL-PASSIVE2
Insufficient Flow for Passive System in Loop2
INSUFF-FLOW-PASSIVE2
Flow Blockage of Passive System in Loop 2
-BLOCK-PASSIVE2
Passive Convecti Failure in Loop 2
PASSIVE2-CONV-LO
Passive Convection Fails to Start in Loop 2
SCS-PASSIVE - Loss of SCS Passive System
2004/07/20
Page 12

Figure IV-66 Fault Tree for Passive SCS System in GFR: Zoom 14

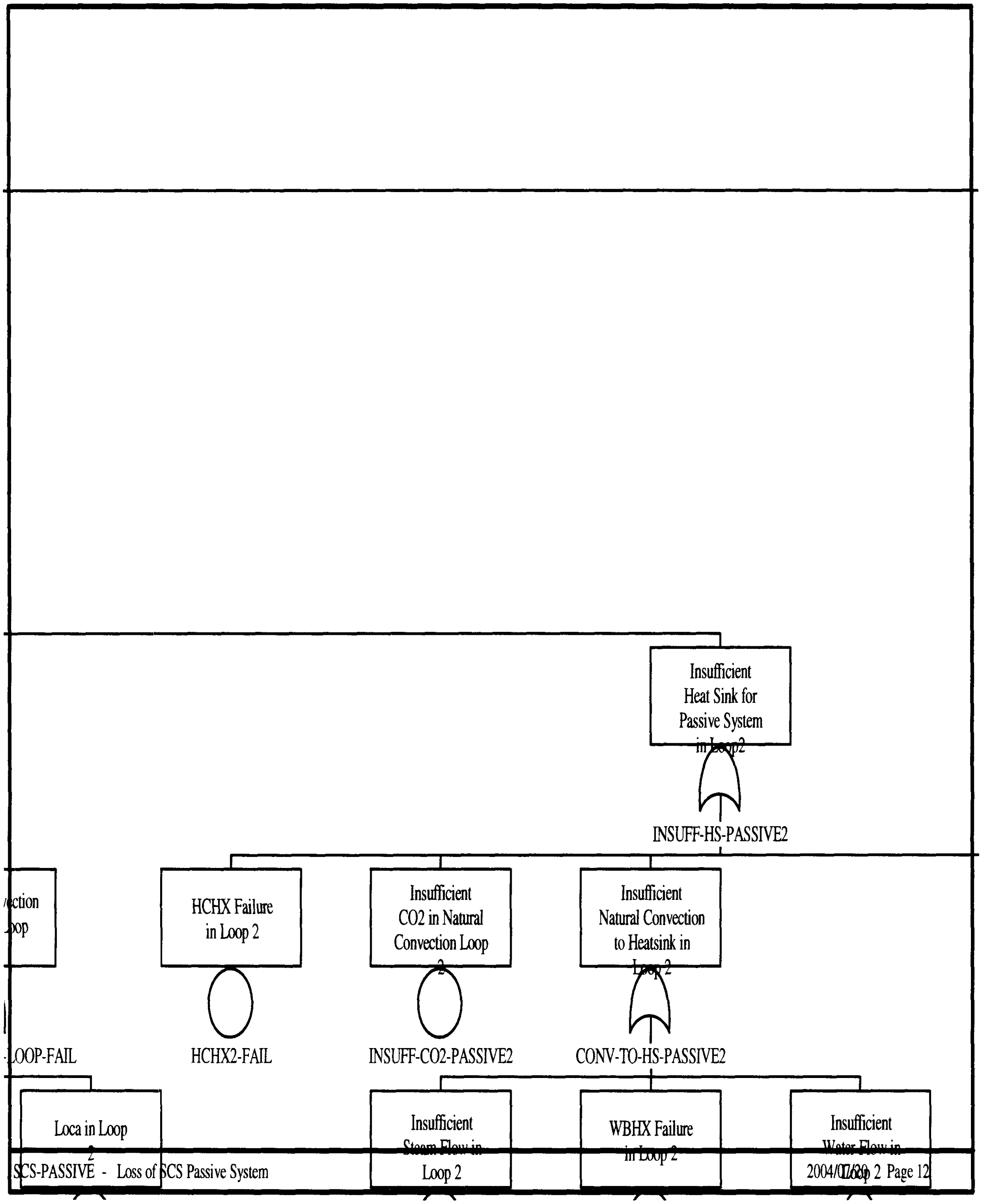


Figure IV-67 Fault Tree for Passive SCS System in GFR: Zoom 15

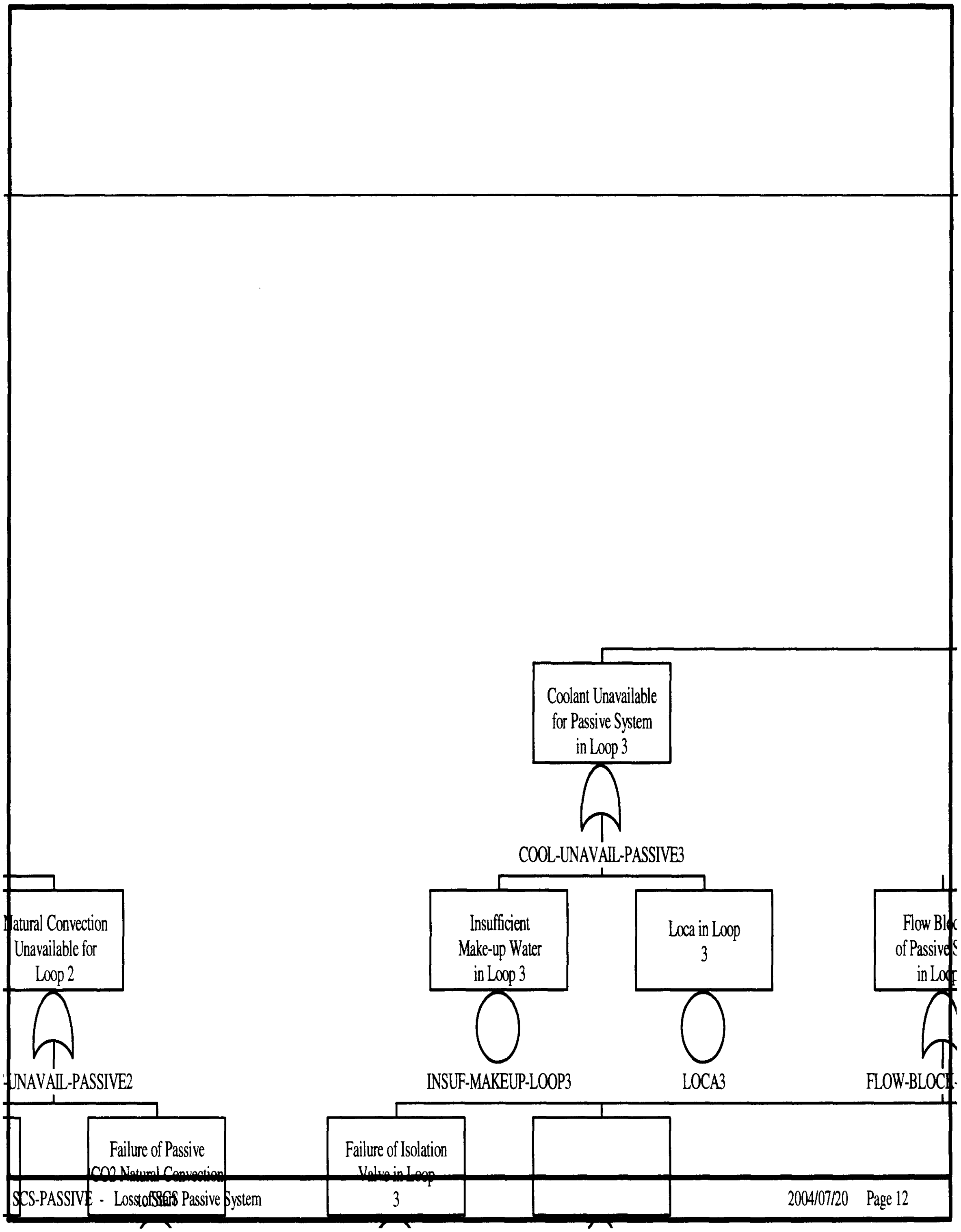

Coolant Unavailable for Passive System in Loop 3
COOL-UNAVAIL-PASSIVE3
atural Convection Unavailable for Loop 2
-UNAVAIL-PASSIVE2
Insufficient Make-up Water in Loop 3
INSUF-MAKEUP-LOOP3
Loca in Loop 3
LOCA3
Flow Bl of Passive in Lo
FLOW-BLOCK-
Failure of Passive CO2 Natural Convection
Failure of Isolation Valve in Loop 3
SCS-PASSIVE - Loss of SCS Passive System
2004/07/20 Page 12

Figure IV-68 Fault Tree for Passive SCS System in GFR: Zoom 16

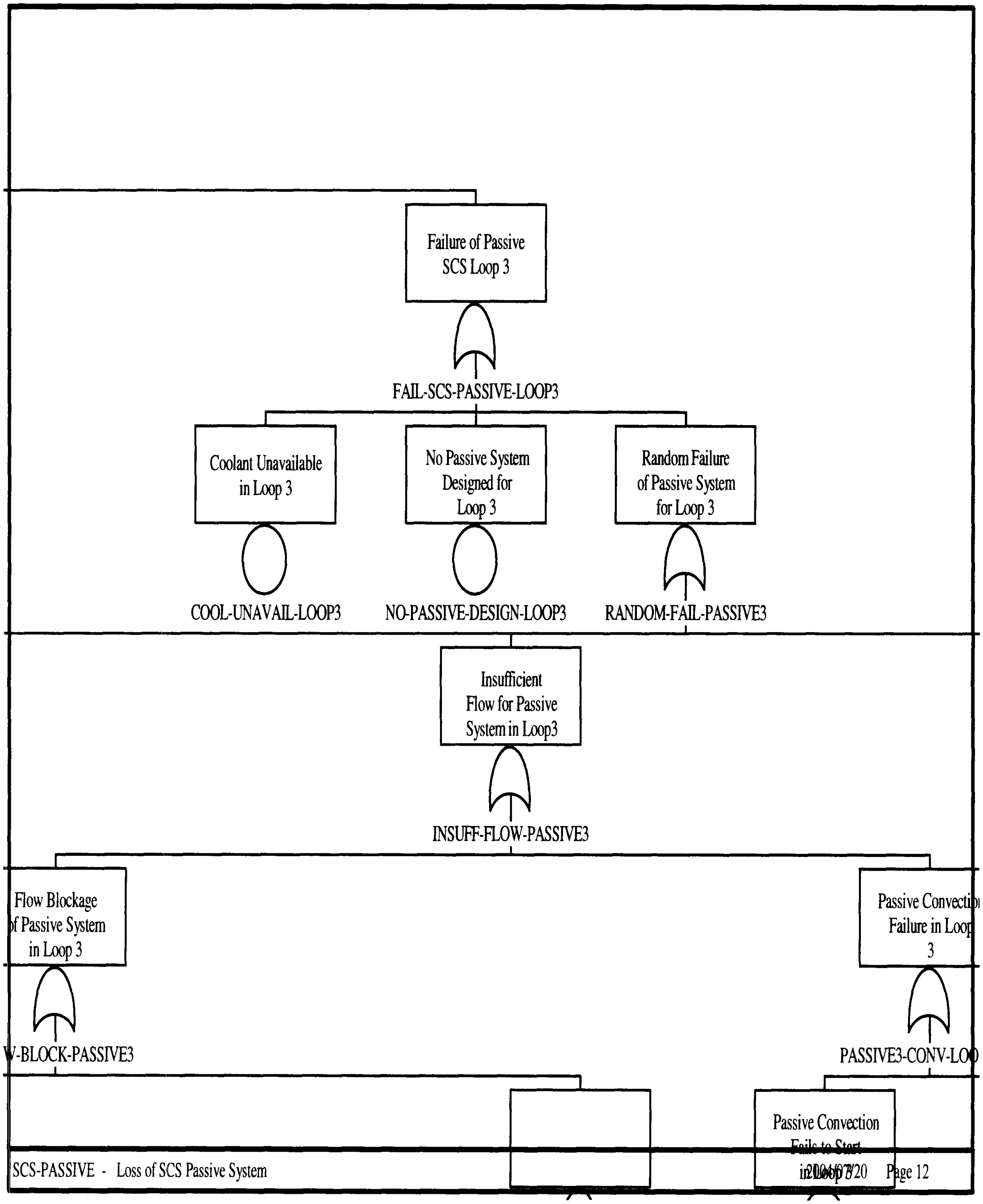

Failure of Passive SCS Loop 3
FAIL-SCS-PASSIVE-LOOP3
Coolant Unavailable in Loop 3
COOL-UNAVAIL-LOOP3
No Passive System Designed for Loop 3
NO-PASSIVE-DESIGN-LOOP3
Random Failure of Passive System for Loop 3
RANDOM-FAIL-PASSIVE3
Insufficient Flow for Passive System in Loop3
INSUFF-FLOW-PASSIVE3
Flow Blockage of Passive System in Loop 3
-BLOCK-PASSIVE3
Passive Convecti Failure in Loo 3
PASSIVE3-CONV-LO
Passive Convection Fails to Start in Loop 3
SCS-PASSIVE - Loss of SCS Passive System
2004/07/20
Page 12

Figure IV-69 Fault Tree for Passive SCS System in GFR: Zoom 17

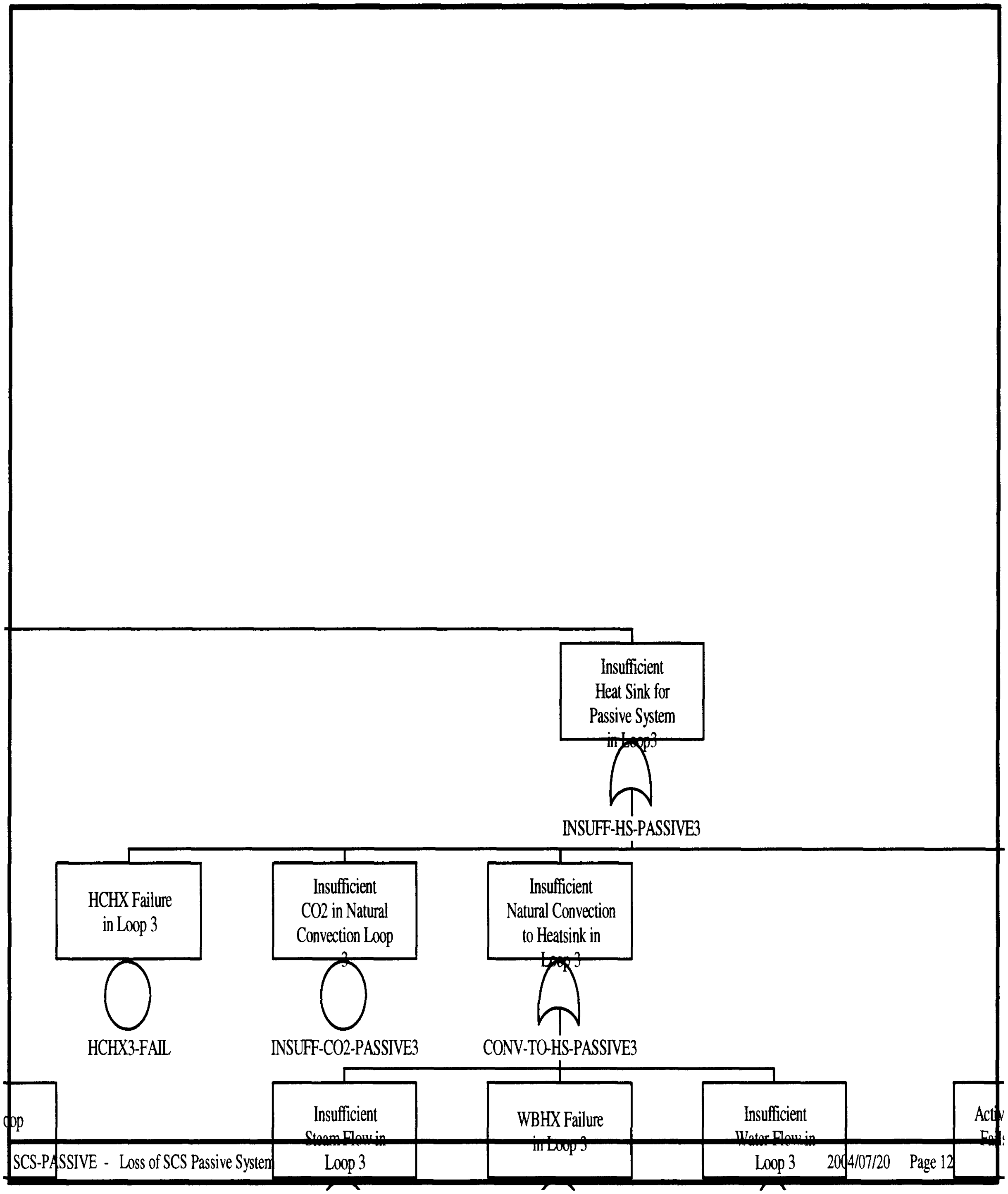

Insufficient Heat Sink for Passive System in Loop3
INSUFF-HS-PASSIVE3
HCHX Failure in Loop 3
HCHX3-FAIL
Insufficient CO2 in Natural Convection Loop 3
INSUFF-CO2-PASSIVE3
Insufficient Natural Convection to Heatsink in Loop 3
CONV-TO-HS-PASSIVE3
Insufficient Steam Flow in Loop 3
WBHX Failure in Loop 3
Insufficient Water Flow in Loop 3
SCS-PASSIVE - Loss of SCS Passive System
2004/07/20
Page 12

Figure IV-70 Fault Tree for Passive SCS System in GFR: Zoom 18

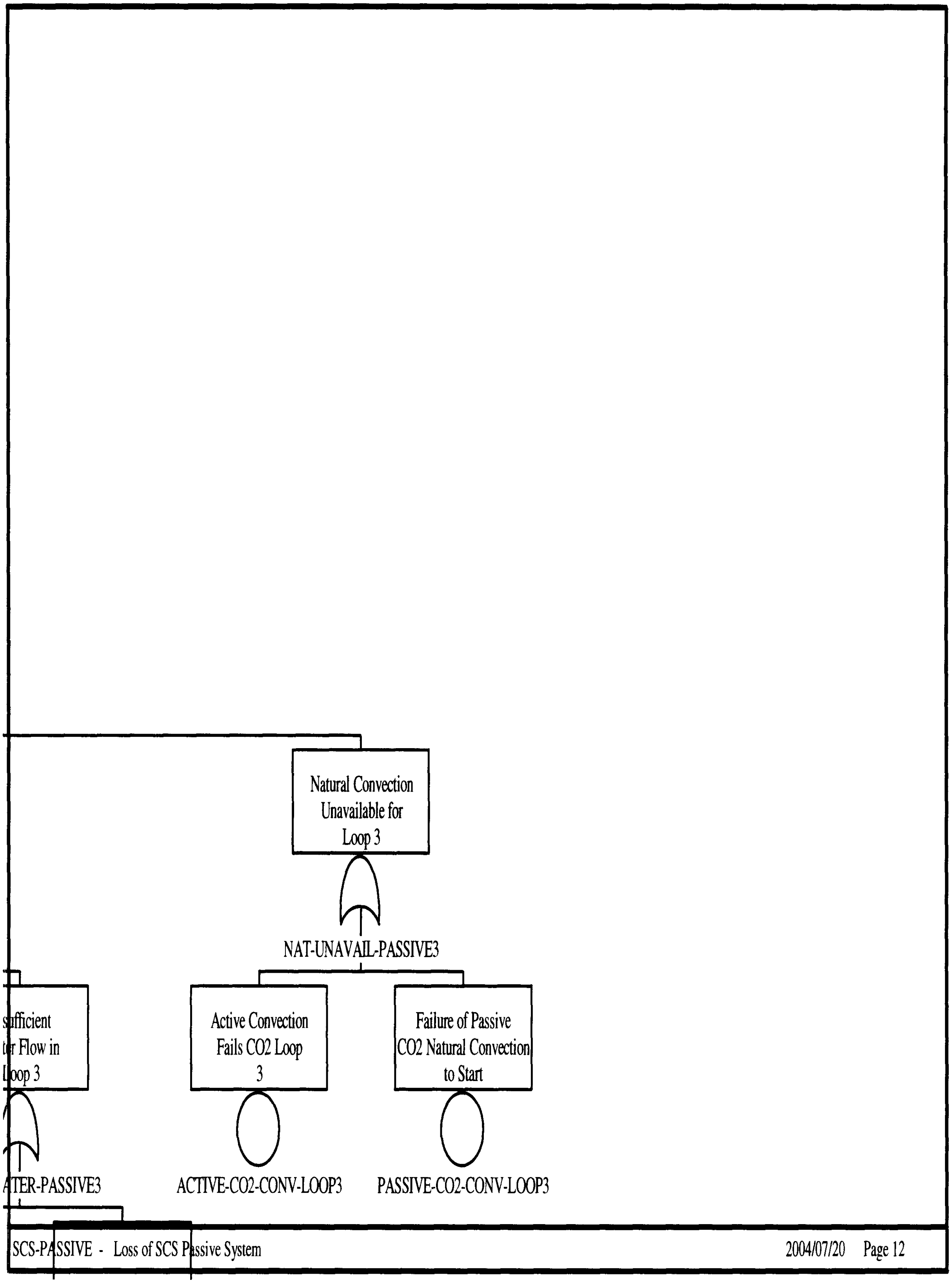

Natural Convection Unavailable for Loop 3
NAT-UNAVAIL-PASSIVE3
sufficient
ter Flow in
Loop 3
ATER-PASSIVE3
Active Convection Fails CO2 Loop 3
ACTIVE-CO2-CONV-LOOP3
Failure of Passive CO2 Natural Convection to Start
PASSIVE-CO2-CONV-LOOP3
SCS-PASSIVE - Loss of SCS Passive System
2004/07/20 Page 12

Figure IV-71 Fault Tree for Passive SCS System in GFR: Zoom 19

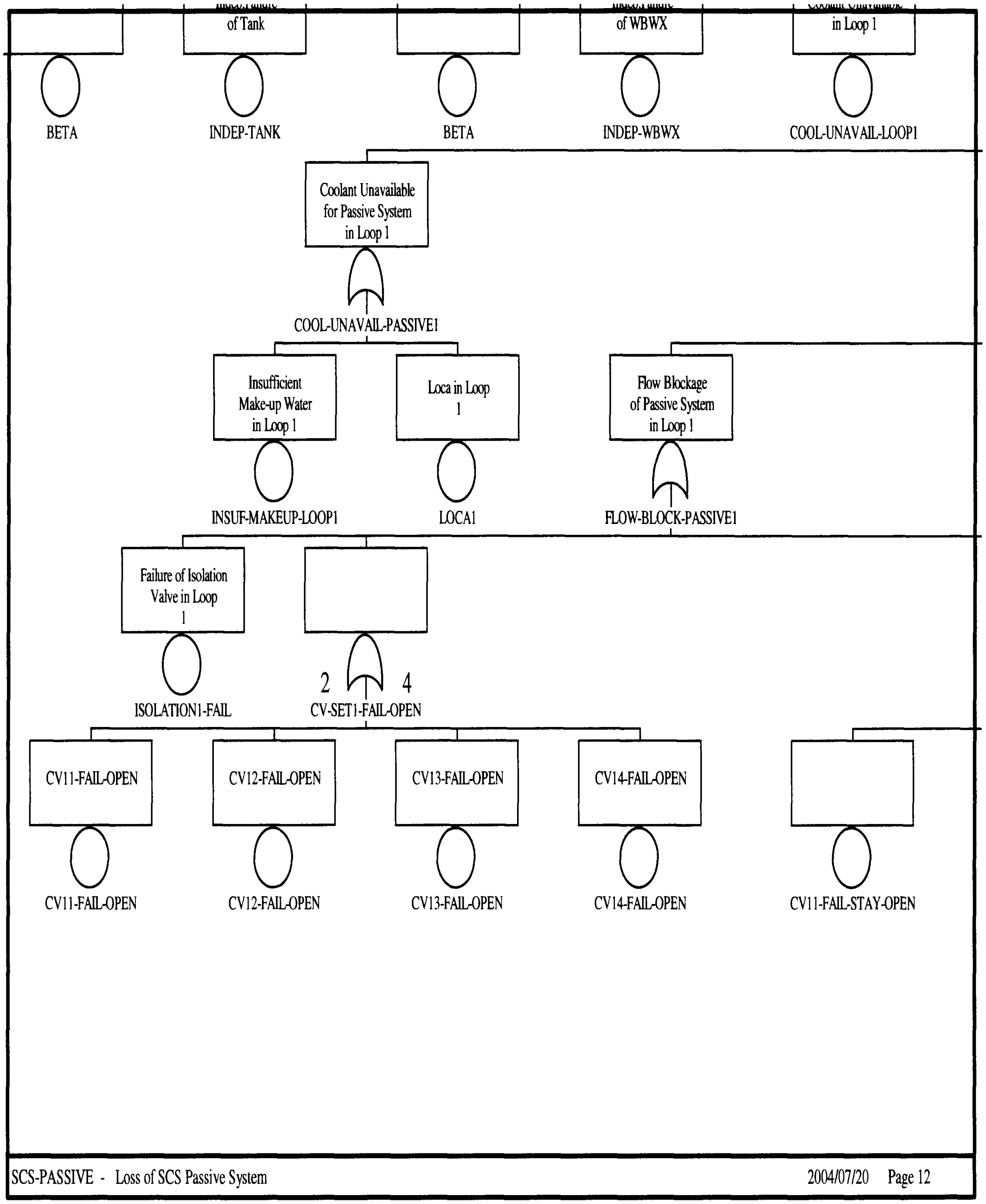


Figure IV-72 Fault Tree for Passive SCS System in GFR: Zoom 20

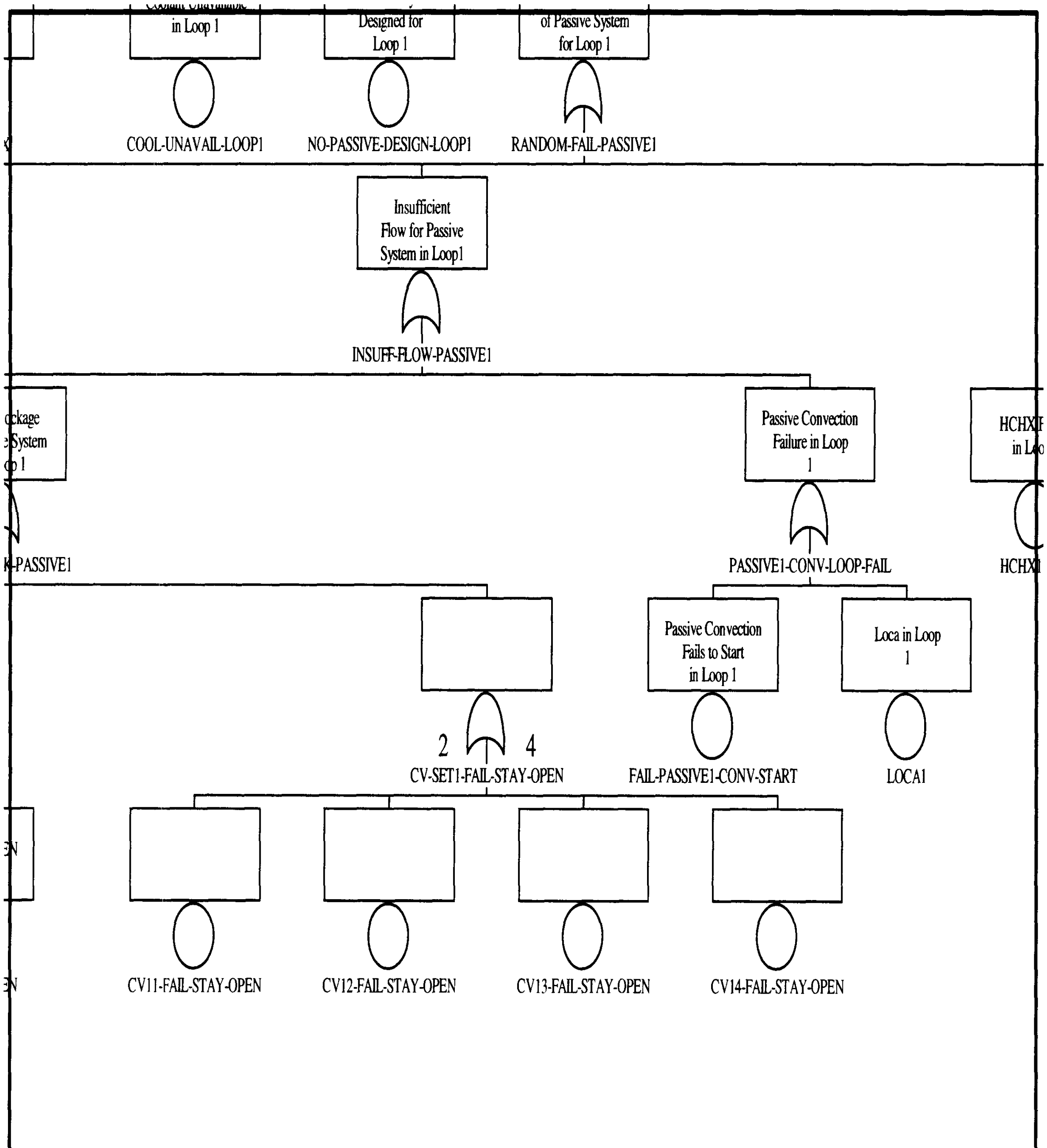


Figure IV-73 Fault Tree for Passive SCS System in GFR: Zoom 21

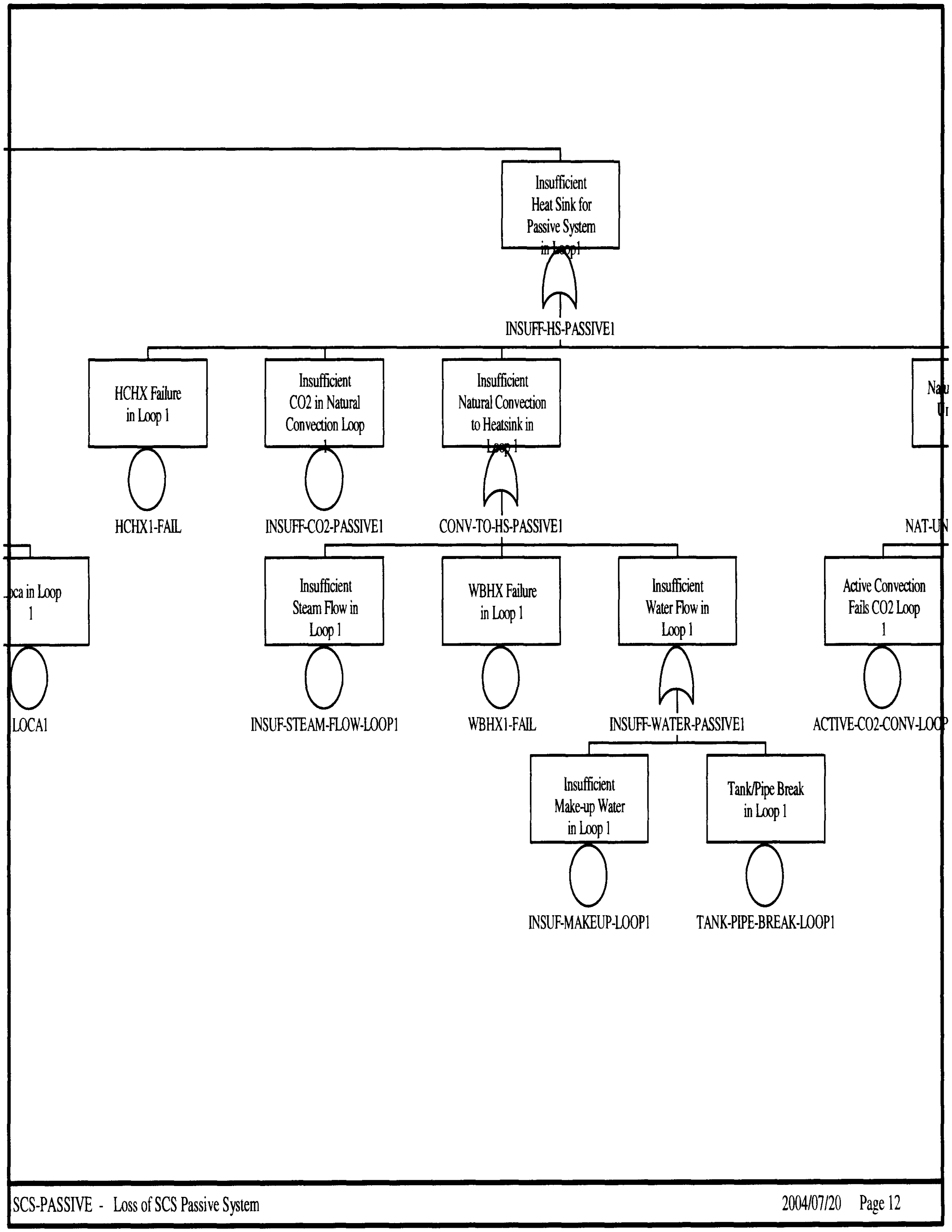

Insufficient Heat Sink for Passive System in Loop1
INSUFF-HS-PASSIVE1
HCHX Failure in Loop 1
HCHX1-FAIL
Insufficient CO2 in Natural Convection Loop 1
INSUFF-CO2-PASSIVE1
Insufficient Natural Convection to Heatsink in Loop 1
CONV-TO-HS-PASSIVE1
Natu
Ur
NAT-U
ca in Loop 1
LOCA1
Insufficient Steam Flow in Loop 1
INSUF-STEAM-FLOW-LOOP1
WBHX Failure in Loop 1
WBHX1-FAIL
Insufficient Water Flow in Loop 1
INSUFF-WATER-PASSIVE1
Active Convection Fails CO2 Loop 1
ACTIVE-CO2-CONV-LOOP
Insufficient Make-up Water in Loop 1
INSUF-MAKEUP-LOOP1
Tank/Pipe Break in Loop 1
TANK-PIPE-BREAK-LOOP1
SCS-PASSIVE - Loss of SCS Passive System
2004/07/20 Page 12

Figure IV-74 Fault Tree for Passive SCS System in GFR: Zoom 22

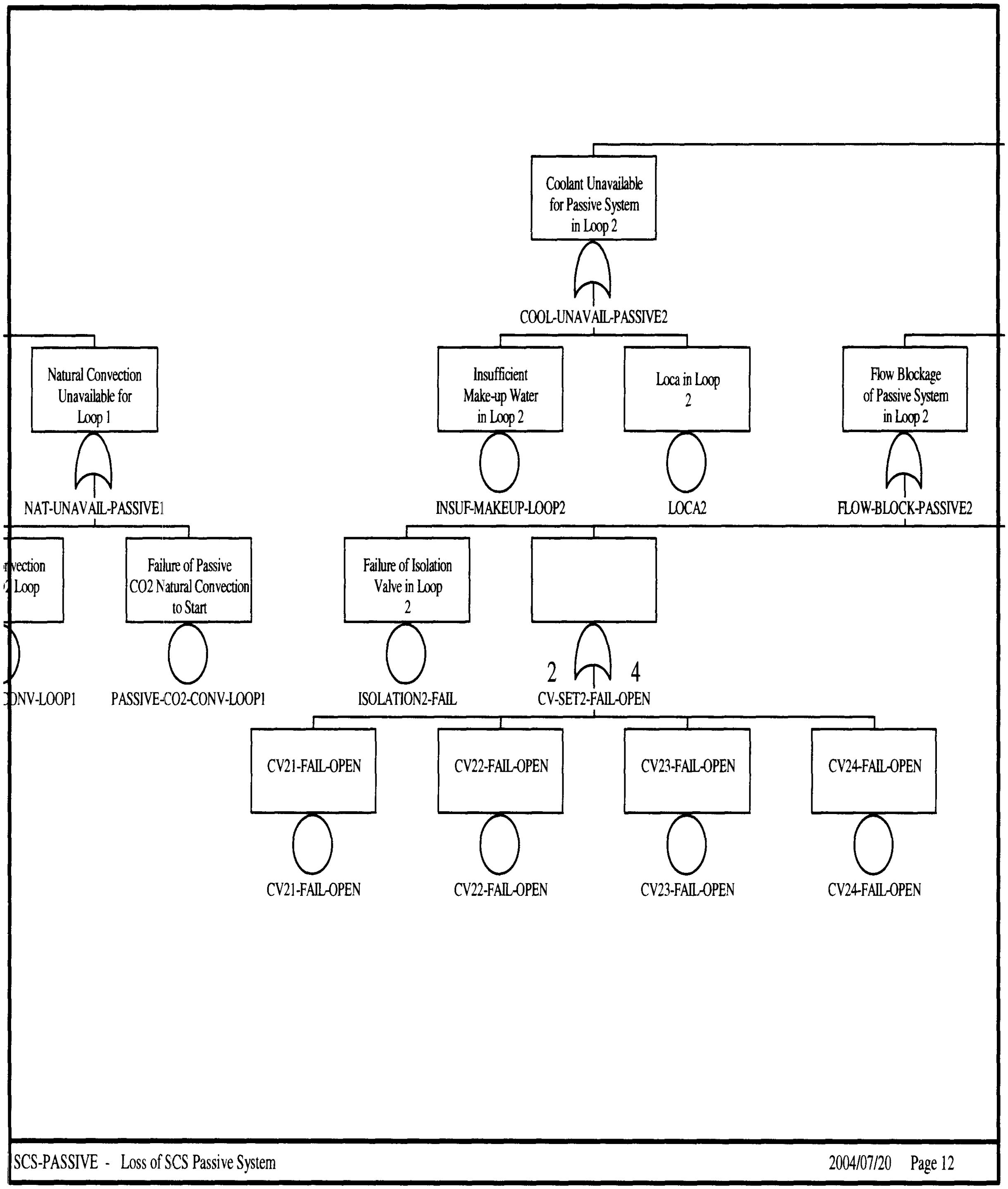


Figure IV-75 Fault Tree for Passive SCS System in GFR: Zoom 23

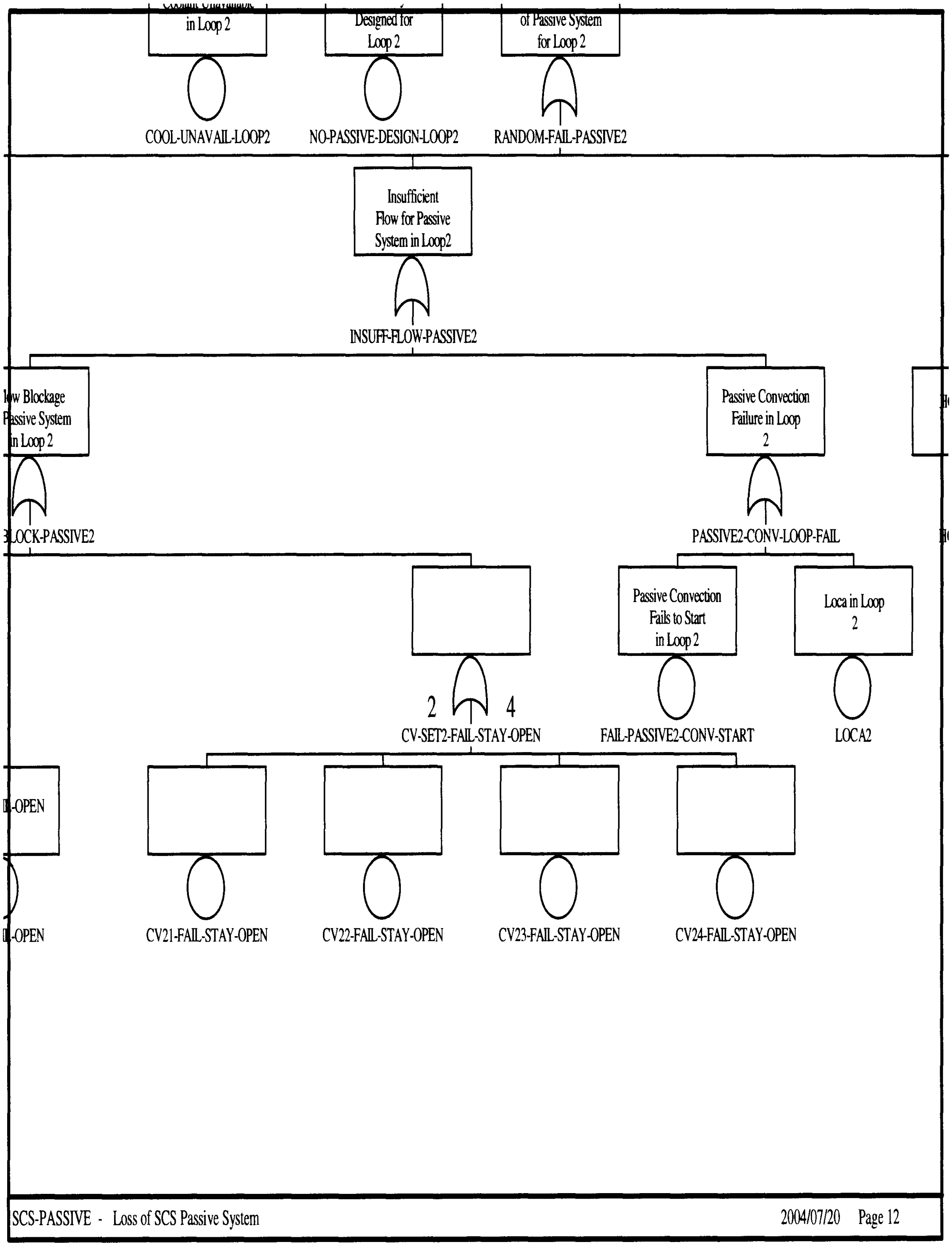


Figure IV-76 Fault Tree for Passive SCS System in GFR: Zoom 24

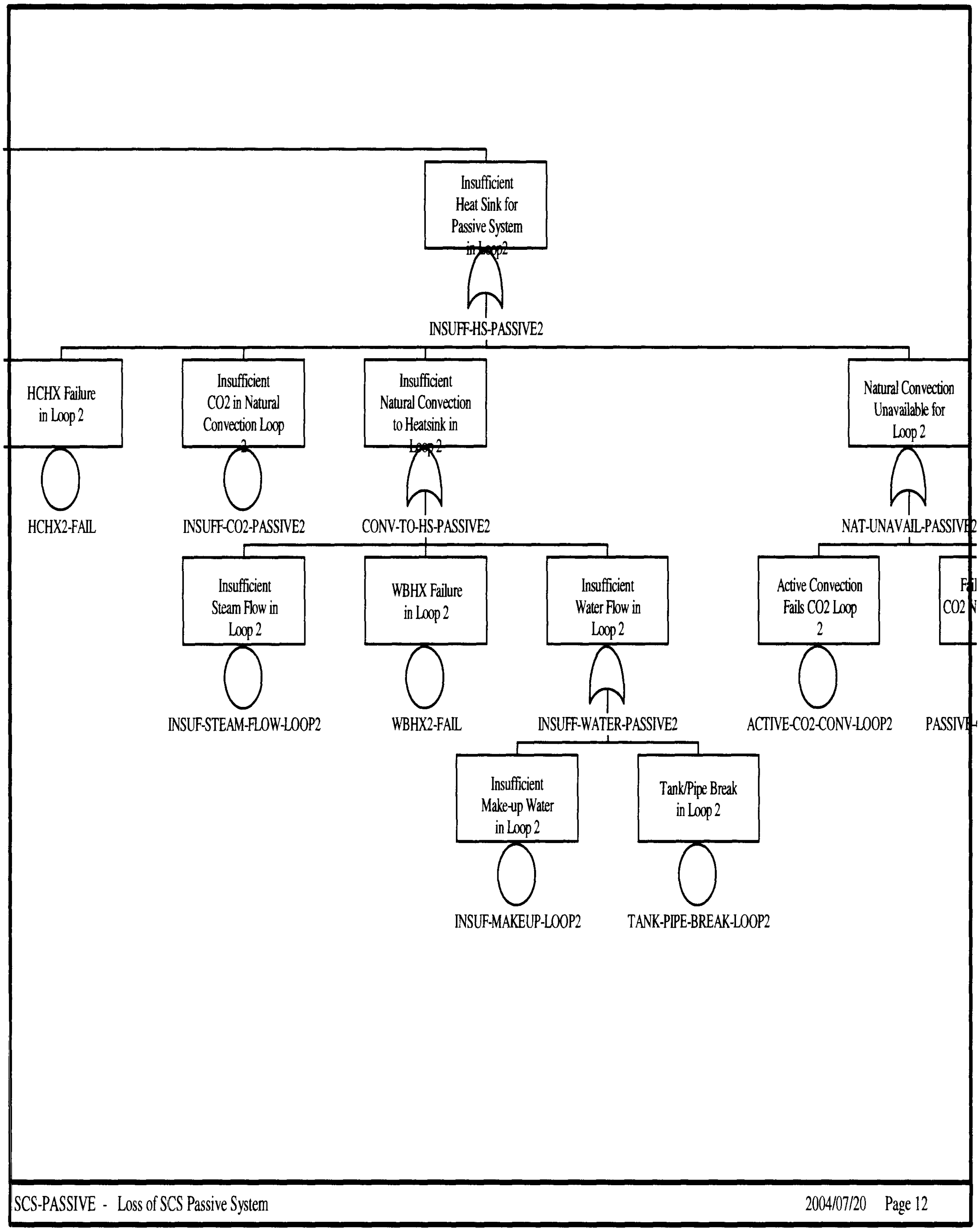

Insufficient Heat Sink for Passive System in Loop2
INSUFF-HS-PASSIVE2
HCHX Failure in Loop 2
HCHX2-FAIL
Insufficient CO2 in Natural Convection Loop 2
INSUFF-CO2-PASSIVE2
Insufficient Natural Convection to Heatsink in Loop 2
CONV-TO-HS-PASSIVE2
Natural Convection Unavailable for Loop 2
NAT-UNAVAIL-PASSIVE2
Insufficient Steam Flow in Loop 2
INSUF-STEAM-FLOW-LOOP2
WBHX Failure in Loop 2
WBHX2-FAIL
Insufficient Water Flow in Loop 2
INSUFF-WATER-PASSIVE2
Active Convection Fails CO2 Loop 2
ACTIVE-CO2-CONV-LOOP2
Fail
CO2 N
PASSIVE-
Insufficient Make-up Water in Loop 2
INSUF-MAKEUP-LOOP2
Tank/Pipe Break in Loop 2
TANK-PIPE-BREAK-LOOP2
SCS-PASSIVE - Loss of SCS Passive System
2004/07/20 Page 12

Figure IV-77 Fault Tree for Passive SCS System in GFR: Zoom 25

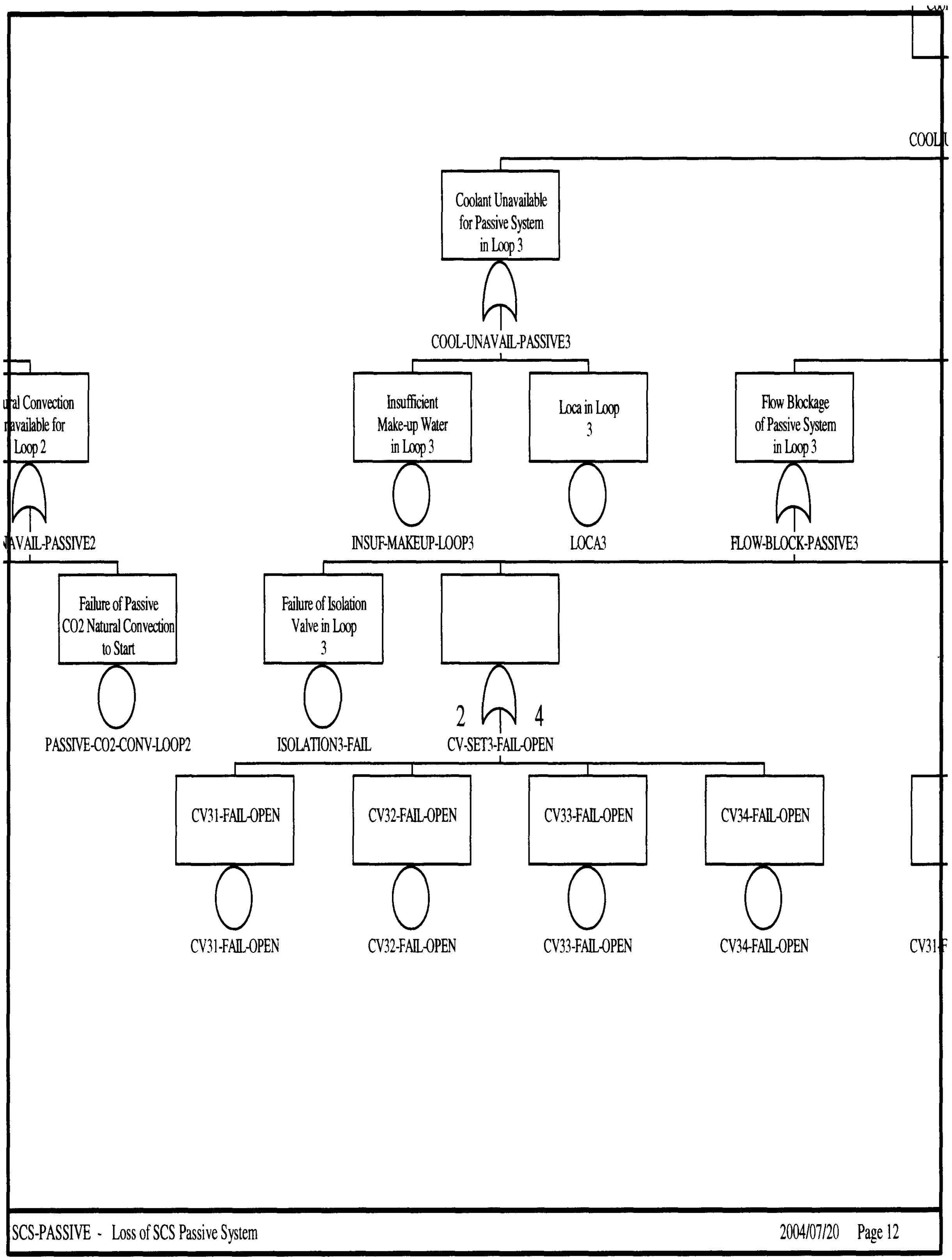


Figure IV-78 Fault Tree for Passive SCS System in GFR: Zoom 26

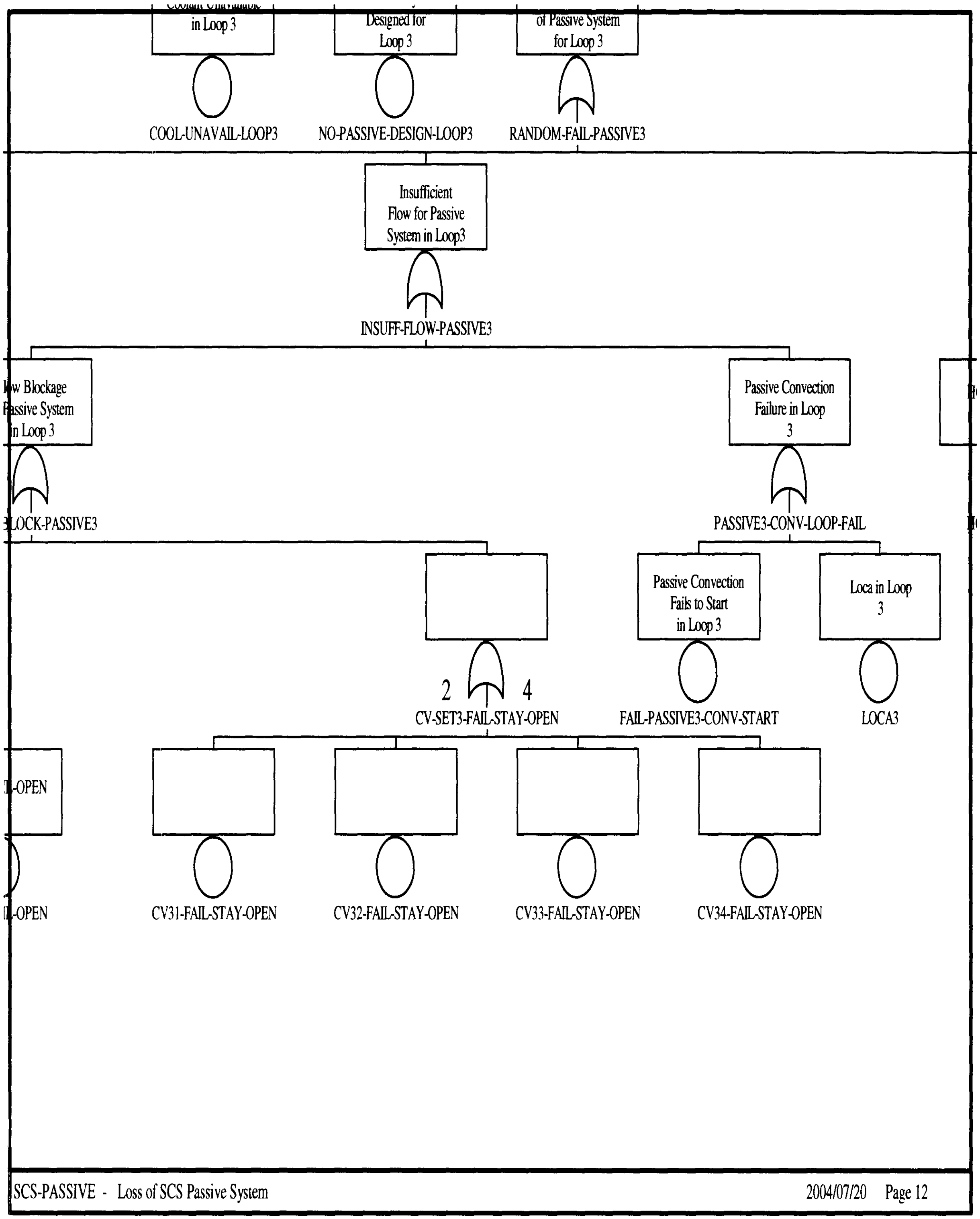


Figure IV-79 Fault Tree for Passive SCS System in GFR: Zoom 27

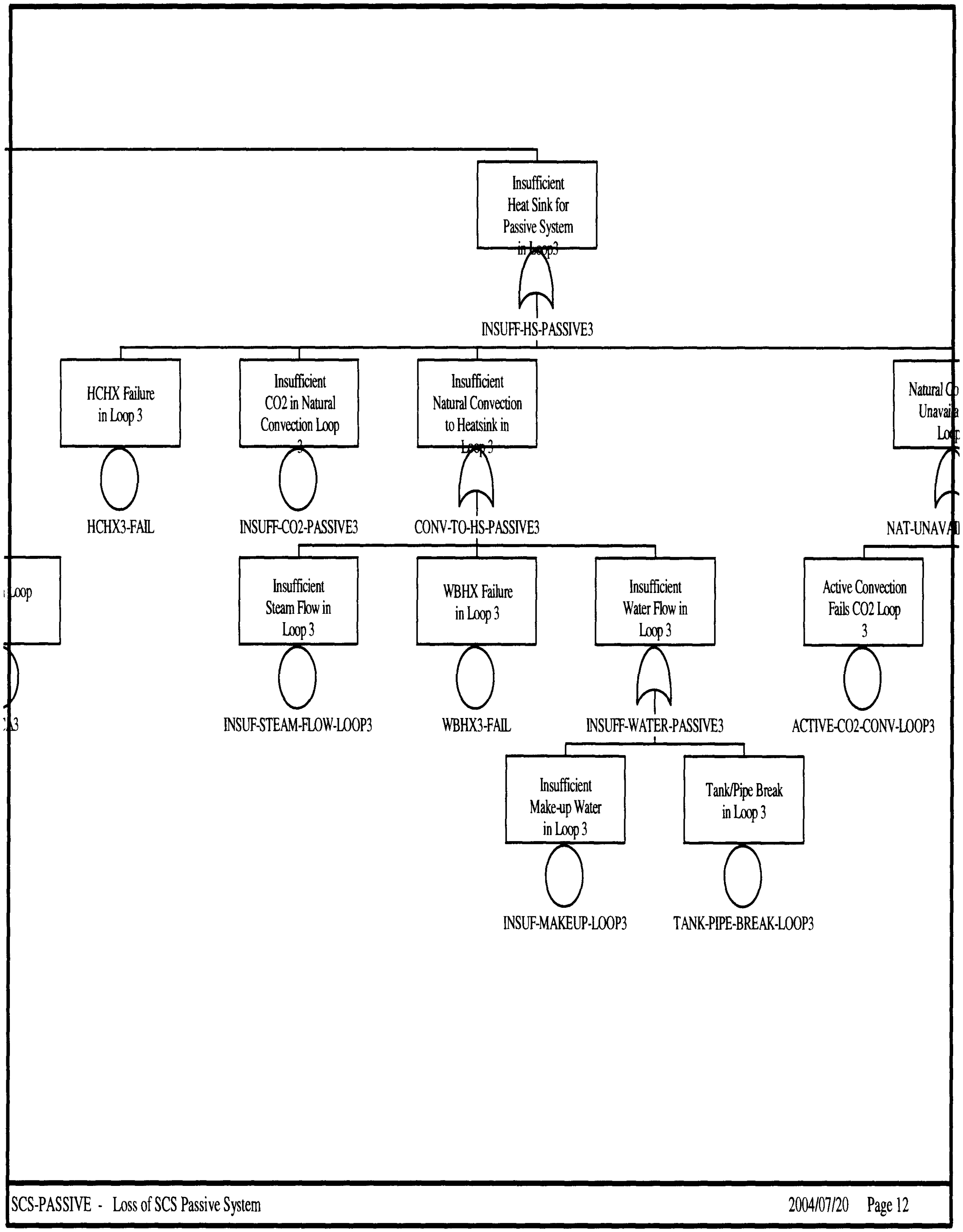
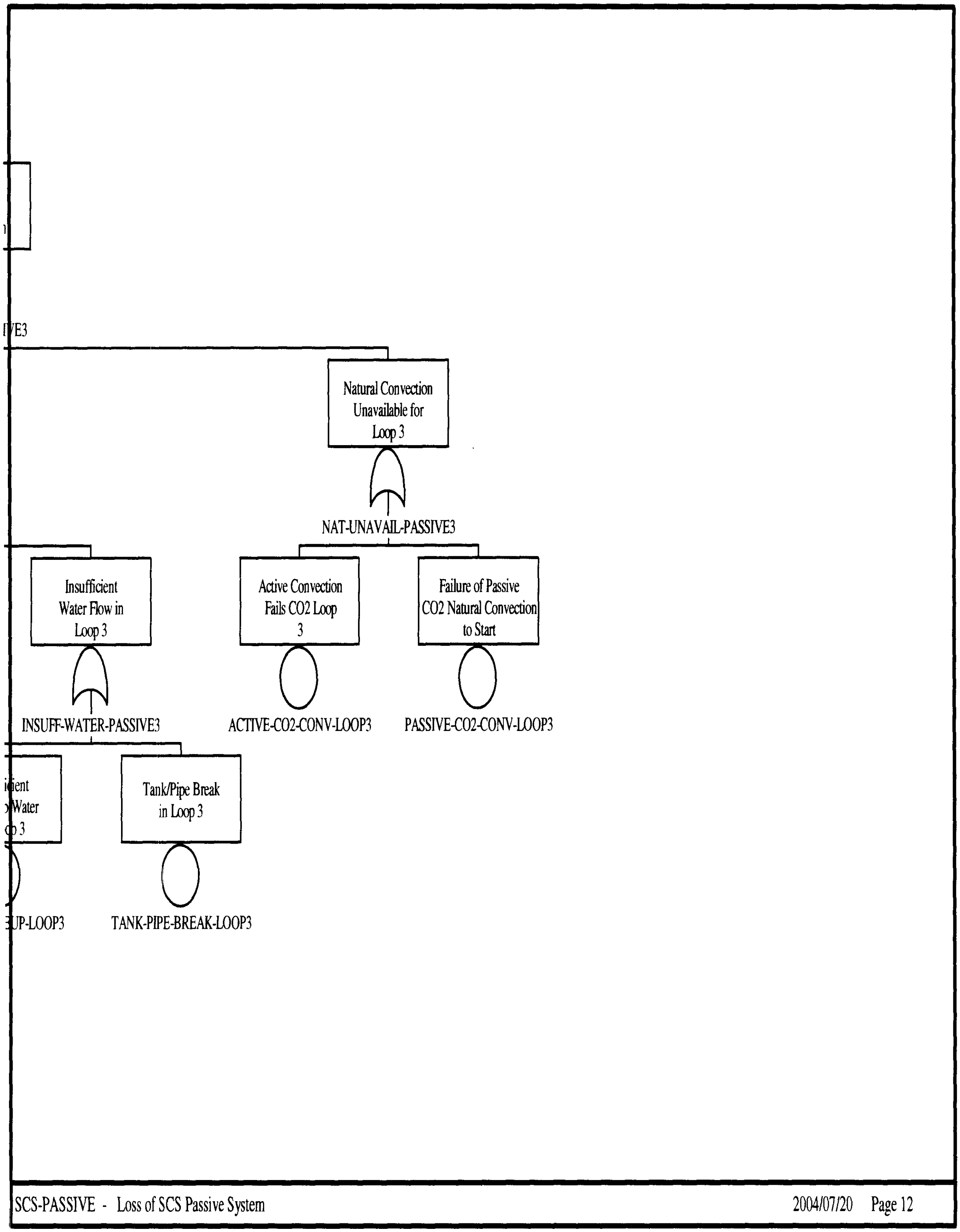

Insufficient Heat Sink for Passive System in Loop3
INSUFF-HS-PASSIVE3
HCHX Failure in Loop 3
HCHX3-FAIL
Insufficient CO2 in Natural Convection Loop 3
INSUFF-CO2-PASSIVE3
Insufficient Natural Convection to Heatsink in Loop 3
CONV-TO-HS-PASSIVE3
Natural C
Unavai
Loo
NAT-UNAVA
Loop
3
Insufficient Steam Flow in Loop 3
INSUF-STEAM-FLOW-LOOP3
WBHX Failure in Loop 3
WBHX3-FAIL
Insufficient Water Flow in Loop 3
INSUFF-WATER-PASSIVE3
Active Convection Fails CO2 Loop 3
ACTIVE-CO2-CONV-LOOP3
Insufficient Make-up Water in Loop 3
INSUF-MAKEUP-LOOP3
Tank/Pipe Break in Loop 3
TANK-PIPE-BREAK-LOOP3
SCS-PASSIVE - Loss of SCS Passive System
2004/07/20 Page 12

Figure IV-80 Fault Tree for Passive SCS System in GFR: Zoom 28



E3
Natural Convection Unavailable for Loop 3
NAT-UNAVAIL-PASSIVE3
Insufficient Water Flow in Loop 3
INSUFF-WATER-PASSIVE3
Active Convection Fails CO2 Loop 3
ACTIVE-CO2-CONV-LOOP3
Failure of Passive CO2 Natural Convection to Start
PASSIVE-CO2-CONV-LOOP3
ient
Water
p 3
UP-LOOP3
Tank/Pipe Break in Loop 3
TANK-PIPE-BREAK-LOOP3
SCS-PASSIVE - Loss of SCS Passive System
2004/07/20 Page 12

Figure IV-81 Fault Tree for Passive SCS System in GFR: Zoom 29

After analyzing this system for the DBA based on the turbine trip initiating event, it was found that the Conditional Core Damage Probability (CCDP) for the system had a mean value of 2.3E-5 per reactor-year. Given the frequency of a turbine trip of 3E-1 per year, the CDF would be 7.0E-6. The turbine trip case was used to analyze the impact of the current turbine trip DBA for LWRs on the CDF of the plant. From a regulatory standpoint, when analyzing a plant one wishes to form an envelope of safety with its DBAs. This envelope deals with the consequences of the accidents, where the thinking is that if a plant can handle the accidents that can cause the greatest harm to the plant and still cool the plant safely, then the plant and its systems will be able to handle any accident that arises (in that accident class). This is why when one creates the DBAs as a set of assumptions for a postulated accident, the plant owners must show that they can safely cool the plant due to these given conditions (usually ones that involve multiple points of damage to plant systems). The conditions given are ones that are rather infrequent, so it is thought that if the plant systems are able to effectively deal with the more damaging and infrequent failures, then they should then be able to deal with the more frequent and less damaging plant accidents. These less damaging accidents would fall within the envelope of the more damaging and infrequent accidents. In the analysis to follow we see the impact that the DBAs truly have on the CDF for a given initiator (i.e. the impact to the initiator's CDF if failures given by the DBAs assumptions could never occur and the systems in which these failures would occur would always function properly).

Given the assumptions listed in the turbine trip DBA were always held true (i.e., there is a reactor SCRAM along with onsite power given a loss of offsite power (or vice-versa)), the new mean value CCDP is lowered to 2.2E-5 per reactor-year (with CDF of 6.6E-6). So we see there is little change in the sequence's overall CDF given current LWR DBA regulations. The small amount of change from the current DBAs again shows that these assumptions that are given in the DBAs occur fairly infrequently. The purpose is to build the safety envelope, talked of earlier, with these infrequent initiators. The current DBAs seem to capture this well, yet only have a low impact on the CDF, which may suggest that more risk-informed DBA regulations could be used to have a higher impact on reactor safety goals and surrogate risk guidelines. If DBAs were chosen based on their impact on the overall CDF for an initiator, rather than the current deterministic method, a better safety envelope could be built. This could ensure that all lesser accidents can be protected against (or mitigated) properly, because they would fall under the envelope of the more damaging (impact on CDF) accidents.

What we have seen from examining this system is that, based on the current Surrogate Risk Guidelines (SRG) for the sum of all individual event sequences which have the same initiator (CDF of 1E-5 per reactor year) (USNRC, 2004), currently this turbine trip initiated accident and its set of sequences would fall below the required value. This, from the designer's standpoint would show that the system's safety was adequate. The design team could now move on to the third stage of the MIT framework and use a metric (like MAUT) to determine what decision options are best for the plant. It was also learned that by doing analysis such as this, a designer could see where safety can be improved even further if so desired by seeing how changing various systems or components could impact the CDF (or other risk guideline) of not only an individual initiator, but also the overall plant.

This exercise was also used to show a regulators point of view. Through the development of fault and event trees, the PRA group learned that when PRA is done correctly, a regulator or designer, even one not as familiar with the design, could easily follow through the logic of a reactor system. This shows the straightforwardness of risk-informed regulation, where a regulator would more easily check a risk-informed plants design against surrogate risk guidelines set forth by the NRC and determine, at least from a preliminary safety standpoint, if the plant met the safety guidelines set forth by the regulator. By using the turbine trip test case, the PRA group saw how a process like this would work and how easily it could be checked.

(This page intentionally left blank)

V Other Initiators for the GFR

Along with the Turbine Trip initiator, the GFR group examined two other initiators. As we said earlier, to develop a set of regulatory requirements one will need to look at the current DBAs in a risk-informed mind-set. Thus members of the GFR group look at, for both design and regulatory purposes, for reasons discussed earlier, these other GFR initiators.

The first was the Loss-of-Coolant Accident (LOCA) initiator as looked at by Delaney, Apostolakis and Driscoll, in "Risk-Informed Design Guidance for a Generation-IV Gas-Cooled Fast Reactor Emergency Core Cooling System" (Delaney et al, 2004). The second was the Loss of Offsite Power initiator as examined by Grégoire Jourdan in his thesis "Using Risk-Based Regulations for Licensing Nuclear Power Plants: Case Study of the Gas-Cooled Fast Reactor" (Jourdan, 2004). Both of these will be examined in detail in the following section as was done in chapter 4 for the Turbine Trip Initiator.

V A Loss-of-Coolant Accident (LOCA)

Delaney et al examined the LOCA initiator for the emergency core cooling system (ECCS) in the GFR as shown in figure III-13. Delaney quotes Criterion 35 of 10CFR50, Appendix A. This says:

"A system to provide abundant emergency core cooling shall be provided. The system safety function shall be to transfer heat from the reactor core following any loss of reactor coolant at a rate such that (1) fuel and clad damage that could interfere with continued effective core cooling is prevented and (2) clad metal-water reaction is limited to negligible amounts.

Suitable redundancy in components and features, and suitable interconnections, leak detection, isolation, and containment capabilities shall be provided to assure that for onsite electric power system operation (assuming offsite power is not available) and for offsite electric power system operation (assuming onsite power is not available) the system safety function can be accomplished, assuming a single failure" (Delaney et al, 2004).

This becomes the basic definition for design basis accident for the LOCA initiator which, as said in Delaney et al's paper "treats the double-ended break of the largest pipe in the reactor coolant system in addition to offsite power being unavailable and a single failure in the most critical place as the DBA for the ECCS" (Delaney et al, 2004).

The overall system is viewed, and Delaney et al develop an event tree for the LOCA as was done for the Turbine Trip initiator. This is shown in figure 5-1, for the bare bones reactor.

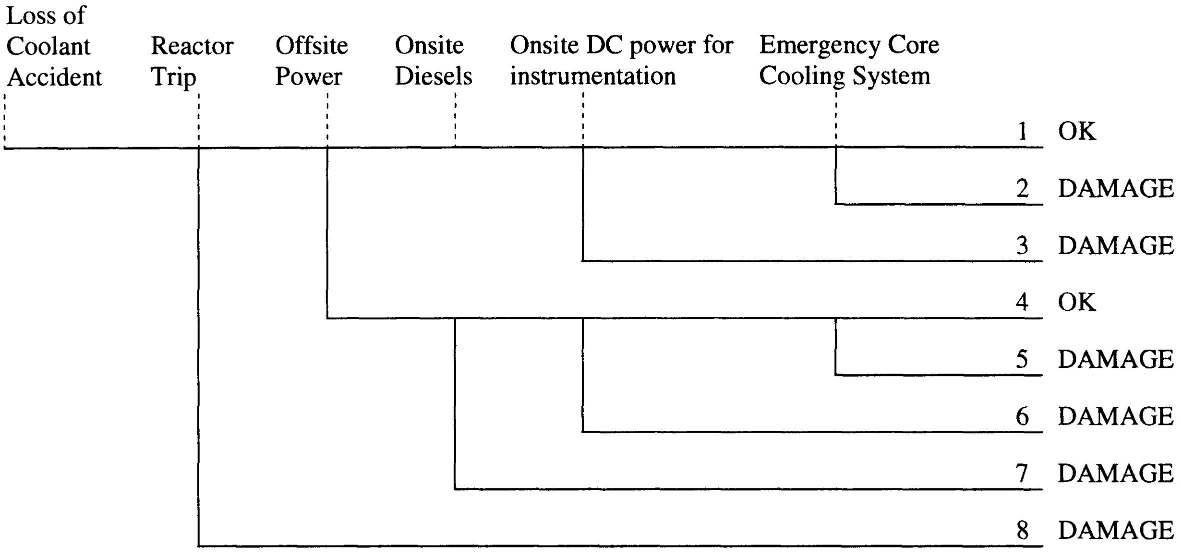


Figure V-1 Bare-Bones ECCS Event Tree from Delaney et al's LOCA initiator for the GFR (Delaney et al, 2004)

As was done with the Turbine Trip initiator, Delaney et al model the system in SAPHIRE building fault trees for each of the GFR systems. The component failure data was the same that was used in the turbine trip case as shown in appendix A, Table A-1. These models were then used to find the CCDP.

Since Delaney et al's work investigated many variations in the GFR design, the design that was settled on at the time of the Turbine Trip initiator investigation will be the one shown here (as to be consistent with what was done in chapter IV). When looking at this design of the GFR system systems (with 3x50% active and passive SCS loops along with 2x100% Diesels and 2x100% batteries), we found from Delaney et al's work that the CCDP was 7.7E-4 per reactor year. Also knowing that the probability of a LOCA is approximately 5.5E-4, we get an overall CDF for a LOCA in this case to be 4.2E-7 per reactor year. This would fall into the acceptable region for the Surrogate Risk Guidelines (SRG) for individual event sequences (CDF of 1E-5 per reactor year) as defined by the NRC; currently this loss of coolant initiated accident sequence would fall below the required value (Delaney et al, 2004).

As was done with the turbine trip case, this case was used to analyze the impact of the current LOCA DBA for LWRs on the CDF of the plant. Again, an analysis of a plant from a regulatory standpoint seeks to develop an envelope of safety with DBAs. The consequences of the accidents are bounded by this envelope (with the thinking being that if one can protect against the more damaging accidents, then the less damaging accidents will be covered as well). As said previously, the conditions given for each DBA are ones that are rather infrequent; it is thought that if the plant can deal with infrequent failures, they should be able to deal with the frequent accidents. The DBA assumptions for LOCA were again examined to see their impact on the plant's CDF due to a given initiator. Given the assumptions listed in the LOCA DBA were always held true (i.e., having onsite power function properly given a loss of offsite power (or vice-versa) along with the adhering to the single failure criterion), the new resulting CCDF would be 1.4E-4. With these assumptions held true, a new CDF of 7.6E-8 is found (Delaney et al, 2004). This is a larger change than in the turbine trip case. It suggests the importance of this DBA to the regulator, and would be an area that the design team might want to focus some of their efforts, to make sure that these DBA assumptions do hold true for this reactor. However, as expressed in the turbine trip initiator section, it is felt that a DBA framework that is more risk-informed and develops a safety envelope based on the contribution of each accident sequence to the overall CDF for a particular initiator may be a more effective methodology.

V B Loss of Offsite Power (LOOP)

Jourdan examined another initiator for the GFR. This initiator was the LOOP initiator for the reactor system of the GFR, again shown in figure 5-2. The Loss of Offsite Power DBA is currently defined in LWR plants as:

"A major plant load loss can result from the loss of external electrical load due to some electrical system disturbance. Offsite alternating current power remains available to operate plant components such as the reactor coolant pumps; as a result, the onsite emergency diesel generators are not required to function for this event. Following the loss of generator load, an immediate fast closure of the turbine control valves will occur. This will cause a sudden reduction in steam flow, resulting in an increase in pressure and temperature in the steam generator shell. As a result, the heat transfer rate in the steam generator is reduced, causing the reactor coolant temperature to rise, which in turn causes coolant expansion, pressurizer insurge, and RCS pressure rise.

For a loss of external electrical load without subsequent turbine trip, no direct reactor trip signal would be generated. The plant would be expected to trip from the Reactor Protection System if a safety limit were approached. A continued steam load of approximately 5 percent would exist after total loss of external electrical load because of the steam demand of plant auxiliaries" (U.S. Code of Federal Regulations, 2004).

Essentially, if we assume a loss of offsite power, we also assume that onsite power is functioning for this DBA. We also assume immediate closure of the Turbine Control Valves (TCV) and a Reactor SCRAM. Finally there is again the Single Failure Criteria (SFC).

In Jourdan's work he again looks at the overall system. He is also able to develop an event tree for LOOP as was done with the other two initiators. This is shown in figure 5-2, for the bare bones reactor.

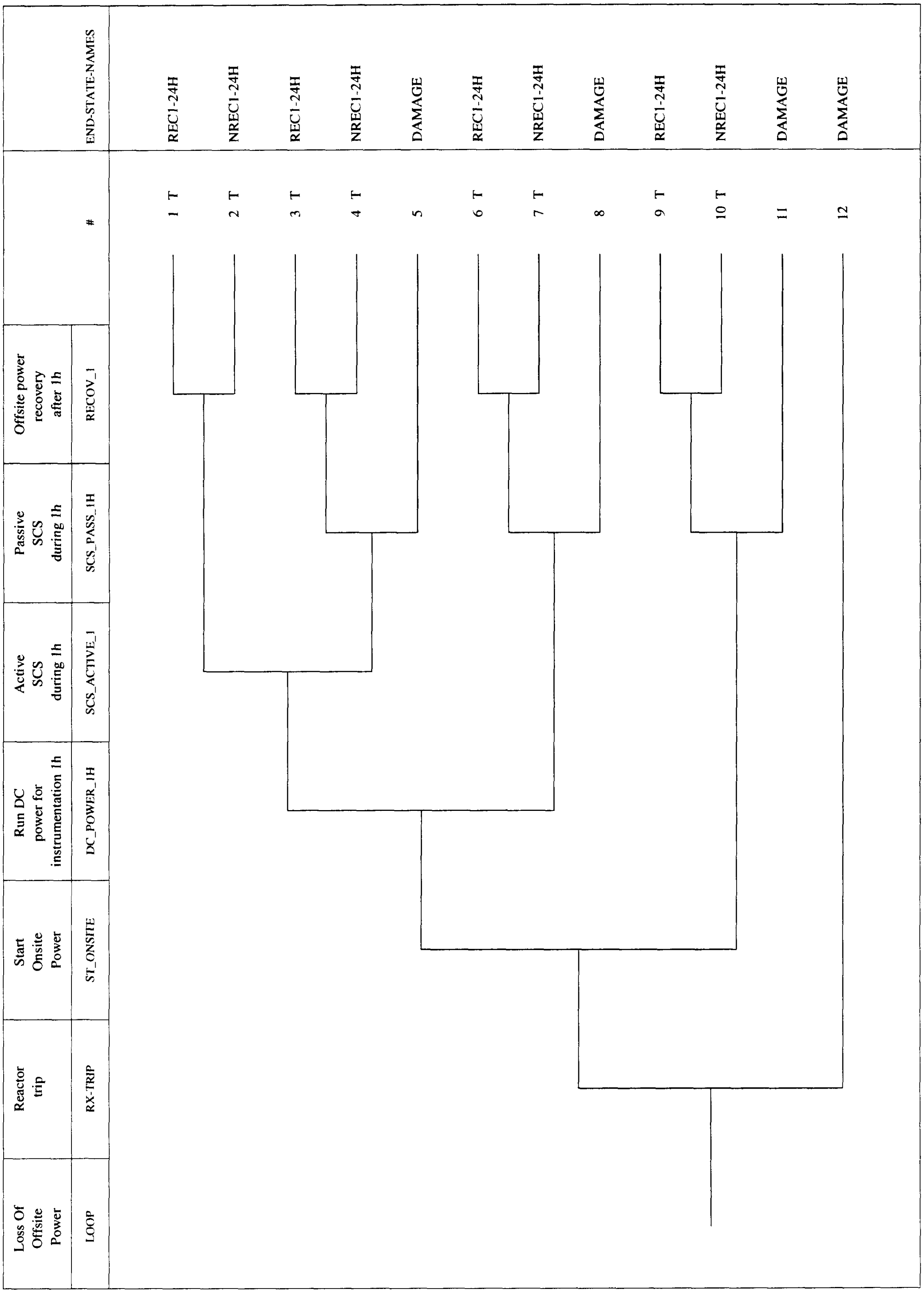


Figure V-2 Event Tree from Jourdan's LOOP initiator for GFR (2004)

We again look at the same GFR system set-up that had been used for the LOCA and turbine trip cases (3x50% active and passive SCS loops, along with 2x100% Diesels and 2x100% batteries), and find from Jourdan's work that the CCDP for LOOP was 4.3E-6 per reactor year. Also knowing that the probability of a LOCA is approximately 2.1E-2 (Office of Nuclear Regulatory Research, 2001), we get an overall CDF for a LOOP in this case to be 8.9E-8 per reactor year (Jourdan, 2004). This would fall into the acceptable region for the Surrogate Risk Guidelines (SRG) for individual event sequences (CDF of 1E-5 per reactor year) as defined by the NRC; currently this loss of offsite power initiated accident sequence would fall below the required value. Again this is something that we saw with LOCA but we did not see with the turbine trip initiator.

Again, as with the two other cases, the current LWR DBA assumptions for LOOP were all put in place (i.e., we also assume that onsite power is functioning, immediate closure of the Turbine Control Valves (TCV) and a Reactor SCRAM along with adhering to the Single Failure Criteria (SFC)). The new resulting CCDP would be 4.1E-6 (Jourdan, 2004). This gives a new CDF of 8.7E-8. This is not a large change for adding the DBA assumptions, yet still passes the SRG per sequence requirement. This again shows designers and regulators, that due to the current LWR DBAs only decreasing the initiators CDF by a small amount, there may need to be a change in DBAs for next generation reactors, that would help to reduce the core damage frequency of the plant by a greater amount, thus focusing the DBAs in more safety significant areas.

VI Proposed Risk-Informed Methodology

VI A Methodology

After reviewing the system and various LWR DBAs, the next step was to draw some insights from the current regulations and the GFR design to propose a method for constructing risk-informed design basis accidents. Based on the knowledge we obtain through risk-analysis of the plants, we should then be able to find out where protective measures are needed and tailor the design basis accidents for each plant design to protect against any lapses in safety culture. DBAs are needed as a protective safety-net against these lapses. DBAs provide a barrier against unknowns that could jeopardize the safety of the plant, workers, public, and environment. In this section, a methodology is proposed for developing risk-informed DBAs for new and innovative reactors.

The first step in this methodology is that success criteria must be selected for the new plant design. This deals with thermal-hydraulic and other calculations that ensure no damage to the plant, environment or the public. One would look at failure data for similar systems and then through risk-informed analysis be able to propose a failure limit through a deliberated policy decision.

An example of how criteria can be developed is found in the paper "A methodology for Developing a Probability Distribution for the Failure Enthalpy of High-Burnup Fuels via Simulation" written by Pagani and Apostolakis (2004). In this paper, the authors are able to develop success criteria through the probabilistic analysis of failure data for nuclear plants.

The authors state that to find the failure probability, we must find the probability that the capacity exceeds the load. In this case the probability density functions (pdf) of the capacity and load are $f_C(c)$ and $f_L(\ell)$, respectively. So, to develop the failure probability, equation 5-1 is used:

$$P(L > C) = \int_{-\infty}^{\infty} [\int_{x}^{\infty} f_L(y)dy]f_C(x)dx \qquad (5\text{-}1)$$

The authors were able to use data from the plants along with various computer codes and conceptual models to simulate accidents in the plant that may occur. Through these simulations, the full failure probability for the system was developed. This gave a distribution of failure limits for the enthalpy at a given burnup level (Pagani et al, 2004). This work is an excellent example of how one can use plant data and simulations, along with probabilistic analysis, to select success criteria for a given reactor type. A method such as this one would need to be repeated for various plant factors to ensure a comprehensive set of risk-informed success criteria for the plant.

After success criteria have been established for the plant, one must then find all the possible sequences that could occur in the plant (not knowing yet if these sequences pass or fail the selected criteria). Thus event and fault trees for the plant design will need to be constructed. There would be many possible sequences for a given plant design, S_1 through S_n. Each of these sequences would have a frequency of occurrence, i.e., f_1 through $f_{n.}$ These sequences along with the defined success criteria would be the basis for developing new design basis accidents for the given reactor type.

For the next step we go back to the Surrogate Risk Guidelines defined in the USNRC's technology neutral framework. The overall sum of the frequencies for various sequences from a given initiating event must be 10^{-5} / RY (which comes from the statement that no single initiating event can contribute more than 10% of the total plant CDF defined as 10^{-4} /RY) (USNRC, 2004). This still holds true, but we must now find out how to pick the various individual sequences to analyze for a given initiating event. This methodology proposes that the best way to do this, after of course making sure the sum of all the frequencies is below the required SRG, is to find which individual sequences contribute the most to the overall sum. Since a value must be set to determine which sequences are examined, it is proposed that sequences be ranked by their frequencies. Then to exploit the rankings of the sequences, the highest frequency sequences will be added together until they reach a value greater than 95% of that initiator's CDF (i.e., the sum of CDF of all sequences with the same initiator). Once those sequences are found that add to a value greater than the threshold of 95% of the initiator's CDF, those are determined to be the dominant sequences for the initiator to later be analyzed and checked against the plant's success criteria.

Thusly for given sequences S_1 through S_n (with frequencies f_1 through f_n) first one checks that:

$$\sum_{1}^{n} f_x < 10^{-5} /RY \qquad (5\text{-}2)$$

All initiators must pass this first criterion. Then, for the second criterion, the question for those sequences associated with the initiator, S_1 through S_n, is which of these sequences, when ranked in order of contribution to CDF, when summed together (starting at the most contributing sequences and adding down, add to a value greater than 95% the sum of all the sequences associated with the same initiator.

Once we do this analysis, any sequences which meet this second criterion and are determined to be dominant must then be examined by the designer to prove that these sequences do in fact meet the success criteria that was defined for the given plant design in the first step of this methodology.

The most important sequences based on risk-informed methodologies have now been found for the given initiator. These are ones that contribute the most to the CDF of the plant and serve, as the original DBAs, as an envelope for all other sequences to be encompassed by. The designer would then develop through analyzing these sequences along with the plant's success criteria, what assumptions would need to be made to ensure the 95% confidence level, as shown with the second criterion, that these highly contributing sequences met the success criteria of the plant. The current DBAs, through their assumptions, require failures of certain systems. To include these types of assumptions, this framework will use ideas. Since the important sequences have already been found, the regulations would ask the designer to show what system(s) are important to that sequence (i.e., contribute the most to the risk from that system). The assumption made would be for the designer to assume that system(s) was down and make sure the success criteria developed in the initial steps for the reactor type could be passed. This would help to ensure that these assumptions truly gave the designer and regulator extra confidence about the system. The assumptions that are develop through this deliberation process between the design team and the regulators will now be the design basis accidents for this plant. This would hold with the original purpose of the plant assessment framework, which would be a set of stylized accidents, based on assumptions, that serve to bound all other accidents, except now instead of using purely deterministic methods, we have used plant experience, data, models and simulations along with our risk-informed methodology to define the design basis accidents for the new plant design.

However, since this method will be risk-informed rather than purely risk-based, there must be a level of conservatism placed into the DBAs. There are always various unknowns that the designer and regulator may not be able to catch. This is why some form of safety-net must be put in place to protect against any threats to safety that are unaccounted for in a purely risk-based methodology. These protective measures add structuralist elements to provide a last line of defense which catches safety concerns which may occur, but may not be as apparent.

These conservative elements will be implemented directly into the success criteria that are defined for the plant. As said before, plant data and simulations, along with probabilistic analysis, to select success criteria for a given reactor type. These criteria, many of which are mechanistic, would use various calculations to show that if met, the reactor would maintain safe operation. Conservatism can be added into these calculations in one of two proposed ways. One way is to use purely conservative codes, data, and calculation methods to develop the safety criteria for the reactor design. The conservatism would be there from the start, allowing a level of confidence to be added to the initial safety criteria. The sequences using the second criterion, as having the greatest impact on the CDF, would eventually be checked against these more conservative criteria adding confidence against possible unknowns.

However, there is also another option that could be used to add conservatism to the success criteria. The second option still uses best estimate calculations when developing the distributions for the success criteria. Yet, now the regulator picks a certain percentage (for example 5%) of which they would allow probability for exceeding the success criteria. As with the first option, this option places a level of conservatism directly into the success criteria. Again, the sequences selected (using the second criterion), due to their impact on CDF, will be checked against these more conservative success criteria. These are two options for the regulator to choose which would be better for generation IV reactor regulations.

In the second part of this section, an example of how the beginning part of this methodology is used will be shown for the example of the turbine trip case, discussed earlier, for the MIT-GFR design.

VI B Case Study

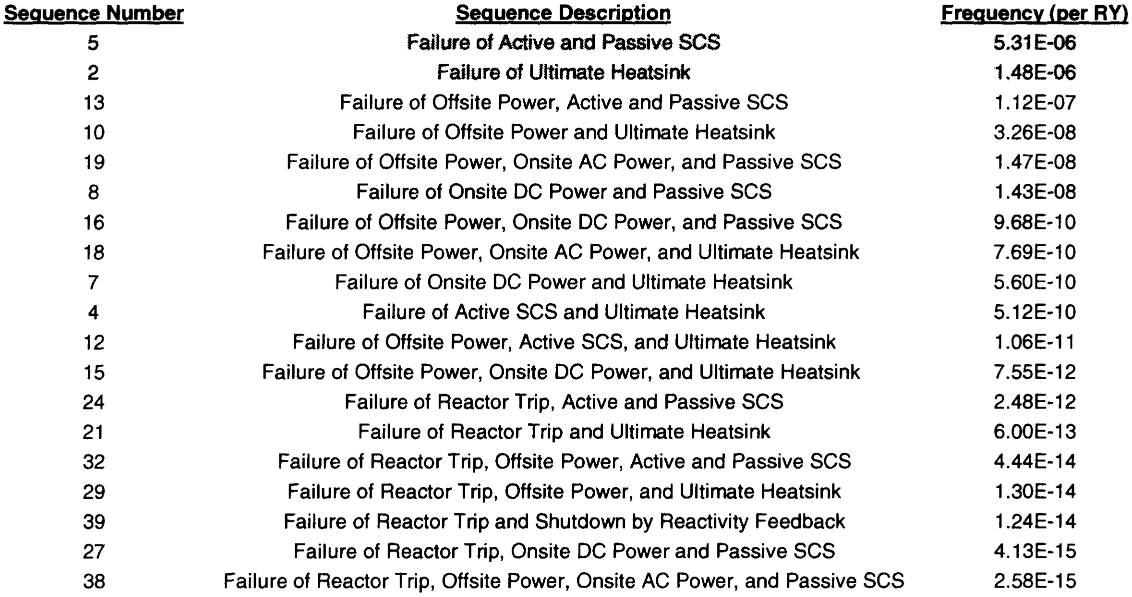
Earlier in this paper the work done on the turbine trip initiator was examined. In this section we will use this to show how steps two and three of the methodology (the development of sequences and selecting of contributing sequences would occur).

For the first check from equation (1), we already found that the Conditional Core Damage Probability (CCDP) for the system had a mean value of 2.4E-5 per Reactor-Year. Again, with the frequency of a turbine trip being 3E-1 per year, the CDF would be 7.0E-6 /RY. This would be an initial check that if failed the regulator would tell the designer to go back and make sure this initiator sequence did in fact pass the surrogate risk guidelines set up in the NRC's technology neutral framework. For the turbine trip case for the GFR, this initial test passed the SRG of 1E-5/RY.

Next we will continue to show how the bounding sequences are selected for the next step of the methodology. First all the sequences are ranked by their frequencies for the turbine trip initiator. Then the highest frequency sequences were added together until they reached a value greater than 95% of that initiator's CDF (i.e., the sum of CDF of all sequences with the same initiator). The 95% CDF value was found to be 6.6E-6. Looking at the sequences in table VI-1, it was shown that sequences 2 and 5 added up to 6.8E-6 (a value greater than the 95% threshold value). These dominant sequences deal with the Ultimate Heatsink and Active/Passive SCS systems, respectively, will later be analyzed and checked against the plant's success criteria.

In analyzing the system, the frequencies of various sequences were found; the most prominent ones are shown in table VI-1, with the highlighted sequences being the ones found to be most dominant:

Table VI-1 Dominating Sequences and their Frequencies for Turbine Trip Initiator in GFR



Sequence Number	Sequence Description	Frequency (per RY)
5	**Failure of Active and Passive SCS**	**5.31E-06**
2	**Failure of Ultimate Heatsink**	**1.48E-06**
13	Failure of Offsite Power, Active and Passive SCS	1.12E-07
10	Failure of Offsite Power and Ultimate Heatsink	3.26E-08
19	Failure of Offsite Power, Onsite AC Power, and Passive SCS	1.47E-08
8	Failure of Onsite DC Power and Passive SCS	1.43E-08
16	Failure of Offsite Power, Onsite DC Power, and Passive SCS	9.68E-10
18	Failure of Offsite Power, Onsite AC Power, and Ultimate Heatsink	7.69E-10
7	Failure of Onsite DC Power and Ultimate Heatsink	5.60E-10
4	Failure of Active SCS and Ultimate Heatsink	5.12E-10
12	Failure of Offsite Power, Active SCS, and Ultimate Heatsink	1.06E-11
15	Failure of Offsite Power, Onsite DC Power, and Ultimate Heatsink	7.55E-12
24	Failure of Reactor Trip, Active and Passive SCS	2.48E-12
21	Failure of Reactor Trip and Ultimate Heatsink	6.00E-13
32	Failure of Reactor Trip, Offsite Power, Active and Passive SCS	4.44E-14
29	Failure of Reactor Trip, Offsite Power, and Ultimate Heatsink	1.30E-14
39	Failure of Reactor Trip and Shutdown by Reactivity Feedback	1.24E-14
27	Failure of Reactor Trip, Onsite DC Power and Passive SCS	4.13E-15
38	Failure of Reactor Trip, Offsite Power, Onsite AC Power, and Passive SCS	2.58E-15

From this table we can see that sequence 2 and 5 (Failure of the Ultimate Heatsink and Failure of Active and Passive SCS), with frequencies of 1.48E-6 and 5.31E-6 / RY, as said earlier, add up to a value greater than the 95% threshold value. Thus the regulator would inform the designer that these are sequences which would need to be checked for all success criteria that were developed in step one (through models and computer codes) and would have to be verified through calculations by the design team to show that a sequence this important and which has such an impact on the system, would be able to meet all success criteria for the plant. The regulator would also ask the designer to show that given that either the ultimate heatsink or both the active and passive SCS systems were down, the reactor can still meet its success criteria. As said earlier these success criteria would have a structuralist element to them as a way of placing conservatism into the proposed risk-informed DBA regulations. Conservatism can be added into these calculations in one of two proposed ways. This would be in one of two ways: using purely conservative codes, data, and calculation methods to develop the safety criteria or using best estimate calculations when developing the distributions for the success criteria along with the regulator picking a certain percentage of which they would allow probability for exceeding the success criteria. A suggestion for this is 5%. It would still be the regulators decision of which of these two options to use. Either way, conservatism would be implemented directly into the success criteria and thus be there from the beginning. Sequences selected (using the second criterion) as having the greatest impact on the CDF would eventually be checked against these more conservative criteria. These structuralist elements would add confidence against possible unknowns.

In carrying out the next step in the method, it was found that sequence 5 occurs when the passive shutdown-cooling-system does not function properly. The design team would need to show through calculations and computer simulations what assumptions could be made to assure that the passive SCS would function with a high frequency (shown through fault tree analysis as well). These assumptions would take into account the failure limits obtained when developing the success criteria in step one. Through a deliberation process with the regulator, the design team would prove that given these assumptions, the passive SCS would function and thus the dominating sequence 5 would be a success (and pass the prescribed success criteria developed earlier). This would show the regulator that we have accounted for the most dominant accidents which would serve as an envelope to account for all other possible sequences. Thus, the design team and regulators will be creating new DBAs, in a risk-informed manner, for the newly proposed reactor design. This is risk-informed, because it has a basis in PRA, yet still contains deterministic elements as a safeguard against unknowns (set-up in the initial success criteria). The assumptions developed from the calculations, models and checks against success criteria, along with confirmation through the deliberation process between designer and regulator, will serve as the basis for the DBAs for each initiator. This method will be repeated for all possible sequences and initiators (based on plant data, simulation codes, and experience from plant histories). In each case, as discussed earlier, a set of assumptions would be developed by finding which sequences dominate, and then which system dominate those dominating sequences. The assumptions would assume those dominant systems were down and make sure the sequences could still pass the success criteria developed for the given reactor. This would ensure a safety envelope for the plant, treating the most damaging accidents to ensure that if these accidents could be defended against, so could less damaging ones. These would include the LOOP and LOCA work discussed earlier (as analyzed by Jourdan and Delaney et al respectively).

VII Conclusions

With the need for new and innovative designs, as stressed in the "Technology Roadmap for Generation IV Nuclear Energy Systems", there also needs to be new and innovative regulations (U.S. Department of Energy, 2002a). Due to a lack of knowledge and industry experience with these designs, as opposed to the breadth and depth of knowledge the industry has on LWRs, we must now use risk-information to make up for this lack of confidence.

In this paper current LWR regulations were explored. It was shown that originally design basis accidents were deterministically determined by a panel of experts. These were deemed "reasonable" accidents by the panel, in that they could reasonably occur in the lifetime of a reactor; however they were also a set of stylized accidents, based on certain assumptions, whose consequences were the most damaging and thusly served as an envelope to encompass all other less serious accidents. However, this deterministic methodology was shown to miss a few key initiators and accident sequences. Through the reactor safety study done in WASH-1400, these accidents were learned of and turned into DBAs, including system interfacing LOCAs, Anticipated Transients without Scram, and Station Blackout (U.S. Nuclear Regulatory Commission, 1975). This was one of the first examples of how probabilistic risk analysis could be used in regulating reactors and adjusting where safety was either needed, or where regulators may have been overly conservative.

Currently, with new reactor concepts being looked at in industry and university settings, the regulatory agencies are looking to develop a new technology neutral framework for regulations. Currently this is being done by the USNRC, which seeks to risk-inform their regulations. This paper attempted to show this could be done and that risk-informed design basis accidents would be a proper direction to go in, when forming a new regulatory framework for the next generation of nuclear reactors.

To show the feasibility of risk-informing design basis accidents, a methodology was developed and used. First, given a new plant design, success criteria are developed. These would be developed through various calculations by the designer to show that no damage would come to the plant, workers or public if these success criteria held true. It was shown in the work by Pagani et al how this would be done through plant data, uncertainty models, and computer code simulations. The example that Pagani et al gave, was the distribution of where there are enthalpy failures at certain burn-up stages for a reactor (Pagani et al, 2004). Again it is stressed that this method will be risk-informed rather than purely risk-based, and so one needs to add a level of conservatism placed into the DBAs. Due to the unknowns that the designer and regulator may not discover, there needs to be a safety-net to protect against safety threats to the reactor. The structuralist elements proposed, will be implemented directly into the success criteria for the plant. Plant data and simulations, along with probabilistic analysis, will be used to select success criteria for a given reactor type. The criteria would use various calculations to show that if met, the reactor would maintain safe operation. Conservatism would be added into these calculations. This would be done through two proposed options. The first would be to use purely conservative codes, data, and calculation methods when developing the safety criteria for the reactor design. The second option uses best estimate calculations when developing the distributions for the success criteria. It was proposed for this option that the regulator pick 5% of the distribution of which they would allow probability for exceeding the success criteria. For both options conservatism would be there from the start. This allows a level of confidence to be added to the initial safety criteria. The regulator would be able to choose which of the two options they think are more appropriate for adding a deterministic level of conservatism to the design basis accidents. Once the calculations are done and models run, there would be a policy decision made, after deliberation, what the exact success criteria would be for a new reactor design.

Once this is done, it is shown how all sequences would be found for a plant by developing event and fault trees for the new design. These sequences for each initiator would be what are examined when developing the design basis accidents. For each initiator sequence, it was shown that the Surrogate Risk Guidelines defined by the NRC would be used, where the overall sum of the frequencies for various sequences from a given initiating event must be 10^{-5} / RY (which comes for the statement that no single initiating event can contribute more than 10% of the total plant CDF defined as 10^{-4} /RY) (USNRC, 2004).

This is the first requirement that each initiator must pass as shown in equation (5-2). When investigating the GFR test case, it was found that all three of the initiators that were investigated, met the surrogate risk guidelines. The LOOP initiator, as shown in the work of Jourdan, had a mean value CDF of 8.9E-8 per reactor year (Jourdan, 2004) while the LOCA initiator, as developed by Delaney et al, had a mean value CDF of 4.2E-7 per reactor year (Delaney et al, 2004). Both were shown to be well below the requirement of 1E-5 / RY. The Turbine Trip test case also met methodologies first requirement, with a mean value CDF of 7.1E-6/ RY.

The Turbine Trip was the initiator that was investigated most extensively, so the later stages of the methodology were used on it as a test case. The next methodology step was to select the dominant sequences for the next step of the methodology. First all the sequences were ranked by their frequencies for the turbine trip initiator. Then the highest frequency sequences were added together until they reached a value greater than 95% of that initiator's CDF (i.e., the sum of CDF of all sequences with the same initiator). It was found that sequences 2 and 5 added up to 6.8E-6 (a value greater than the 95% threshold value of 6.6E-6). These dominant sequences deal with the Ultimate Heatsink and Active/Passive SCS systems, respectively, will later be analyzed and checked against the plant's success criteria.

It was discussed how current DBAs contain assumptions which require certain systems to fail. Including these assumptions into this framework will be done by finding the system(s) which are most important (contribute the most to that sequences risk) to the most dominant sequences (in earlier steps as shown). The designer would assume that system(s) was down and make sure the success criteria developed in the initial steps for the reactor type could be passed. This would ensure that these assumptions gave the regulator extra confidence about the system. In this case, the design team for this reactor would be able to prove that given either the ultimate heatsink or the active and passive SCS systems were set as failed, the sequences dominant to the turbine trip initiator (determined to be sequences 2 and 5) passed the success criteria. This would be the way that the DBA for this initiator would be developed after some designer and regulator deliberation.

It is felt that a methodology like this would hold true to all the original DBA intentions. Based on their frequency of occurrence, these stylized accidents that would be developed would not be outlandish, but rather be "credible". Also, due to the fact that they contribute to over 95% of an initiators overall CDF, they would be a set of bounding cases, which serve as an envelope to account for all other accidents. The use of success criteria, as designed for each plant would also help to bring the technology neutral framework to technology specific designs, ensuring that all aspects of safety were accounted for, even taking into account original design features to that reactor type. This would also allow for designers to be more creative in their designs.

It is recommended that this methodology be tried out on a much larger scale, where a separate part of the design team would have the time to create success criteria from various simulations and plant data. Once a complete set of success criteria is developed (along with conservative codes for them), and with knowledge of the system, one would be able, through the use of probabilistic techniques, to find the bounding sequences and develop design basis accidents as shown in our test case. A full scale test of the deliberation process to finalize the DBAs is another facet that must be fully explored to ensure that this method can truly work.

From what has been seen in this paper, it is felt that risk-informed regulations are feasible and should be used for the next generation of nuclear reactors. Due to the lack of plant knowledge for innovative designs, risk-informed methodologies may be a way for the regulators and designers to gain a level of confidence about the safety of new technologies. Overall, it is felt that risk-informing regulations allows designers to be more creative and effective with their designs, while still assuring the regulatory body that all safety concerns are being met. It allows a wide variety of plant designs to be commissioned while still protecting the health and safety and well-being of all stakeholders, including the plant, its workers, the public and the environment.

(This page intentionally left blank)

References

Apostolakis, G.E., Golay, M.W., Camp, A.L., Durán, A.L., Finnicum, D.J. and Ritterbusch, S.E., 2001. *A New Risk-Informed Design and Regulatory Process.* Proceedings of the Advisory Committee on Reactor Safeguards Workshop on Future Reactors, June 4-5, 2001, Report NUREG/CP-0175, pp. 237-248, US Nuclear Regulatory Commission, Washington, DC.

Apostolakis, G.E., Koser, J.P. and Sato, G., 2004. Decision Analysis and its Application to the Frequency of Containment Integrated Leakage Rate Tests. *Nuclear Technology*, 146, 181-198.

Beckjord, E.S., Cunningham, M.A., and Murphy, J.A, 1993. Probabilistic Safety Assessment development in the United States 1972-1990, *Reliability Engineering and System Safety,* 39, 159-170.

Broadhurst, R.H., Scarborough, J.C., 1980. Assessment of Gas Turbine Failure Modes from Historical Steam Turbine Experience, *American Nuclear Society Transactions*, 35, 391-393.

Bush, S.H., 1978. A Reassessment of Turbine Generator Failure Probability, *Nuclear Safety*, 19, 681-698.

Delaney, M.J., Apostolakis, G.E., and Driscoll, M.J, 2004. *Risk-Informed Guidance for Future Reactor Systems.* Accepted for publication in *Nuclear Engineering and Design.*

Ingersoll Rand Energy Systems, 2004. Manufacturer Data, Available: http://www.irpowerworks.com.

Jourdan, Grégoire, 2004. *Using Risk-Based Regulations for Licensing Nuclear Power Plants: Case Study of the Gas-Cooled Fast Reactor*, MS Thesis, MIT, Cambridge, MA.

Kress, T.S., 2002. *Impediments to the Certification of New Technology Reactor Designs.* PSA '02, International Topical Meeting on Probabilistic Safety Assessment. American Nuclear Society. LaGrange Park, IL.

Nuclear Energy Institute, 2002. *A Risk-Informed, Performance-Based Regulatory Framework for Power Reactors.* NEI-02-02, Washington, DC.

Office of Nuclear Regulatory Research, 2000. *Framework for Risk-Informing the Technical Requirements of 10CFR50.* U.S. Nuclear Regulatory Commission, SECY-00-0198, Washington, DC.

Office of Nuclear Regulatory Research, 2001. *Feasibility Study of a Risk-Informed Alternative to 10CFR50.46, Appendix K and GDC 35.* U.S. Nuclear Regulatory Commission, SECY-01-0133, Washington, DC.

Okrent, David, 1981. *Nuclear Reactor Safety: On the History of the Regulatory Process.* University of Wisconsin Press, Madison, WI.

Pagani, L.P. and Apostolakis, G.E., 2004. *A Methodology for Developing a Probability Distribution for the Failure Enthalpy of High-Burnup Fuels via Simulation.* Accepted for Publication in *Nuclear Technology.*

Saito, T. and M. Gasparini, 2004. *Safety of Evolutionary and Innovative Nuclear Reactors: IAEA Activities and World Efforts.* ICAPP '04 Proceedings, Pittsburgh, PA.

Sorensen, J.N., Apostolakis, G.E., Kress, T.S., and Powers, D.A., 1999. *On the Role of Defense in Depth in Risk-Informed Regulation.* PSA '99. International Topical Meeting on Probabilistic Safety Assessment. Washington, D.C.

Sorensen, J.N., 2002. *Some Observations on Risk-Informing Appendices A & B to 10 CFR Part 50,* Report prepared for the Advisory Committee on Reactor Safeguards, NUREG-1755, U.S. Nuclear Regulatory Commission, Washington, DC.

U.S. Code of Federal Regulations, 2004. Title 10, Part 50, Appendix A. *General Design Criteria for Nuclear Power Plants,* US Government Printing Office, Washington, DC.

U.S. Department of Energy, 2002a. *A Technology Roadmap for Generation IV Nuclear Energy Systems,* Washington, DC. Available at: http://ne.doe.gov/geniv/roadmap.html.

US Department of Energy, 2002b. *Moving Forward: Generation-IV Nuclear Energy Systems.* Available at: http://gen-iv.ne.doe.gov/

U.S. Nuclear Regulatory Commission, 1975. *Reactor Safety Study: An Assessment of Accident Risks In U.S. Commercial Nuclear Power Plants. WASH-1400 (NUREG-75/014).*

U.S. Nuclear Regulatory Commission, 2003. *Application of the Single-Failure Criterion to Safety Systems,* Regulatory Guide 1.53, Washington, DC.

U.S. Nuclear Regulatory Commission, 2004. *Regulatory Structure for New Plant Licensing, Part 1: Technology Neutral Framework.* Washington, D.C.

Westinghouse Electric Company, 2003. *AP-1000 Probabilistic Risk Assessment, Revision 1.* Pittsburgh, PA.

(This page intentionally left blank)

APPENDIX

Table A-1 Case Study Component Failure Data (Delaney et al, 2004)

Device	Failure mode	Mean Failure Probability*	Error Factor	Source
Accumulator	All failure mode	2.40E-06	30	(Westinghouse Electric Company, 2003)
Check Valve	Failure to open	1.00E-04	3	(Westinghouse Electric Company, 2003)
Diesel	Failure to Start	1.40E-02	3	(Westinghouse Electric Company, 2003)
Diesel	Failure to run	5.76E-02	10	(Westinghouse Electric Company, 2003)
Electric motor	Failure to Start	3.75E-04	3	(U.S. Nuclear Regulatory Commission, 1975)
Electric motor	Failure to run	3.00E-04	3	(U.S. Nuclear Regulatory Commission, 1975)
Electrical Buswork	Failure during operation	4.80E-06	5	(Westinghouse Electric Company, 2003)
Heatric Heat Exchangers	Failure while operating	2.40E-05	10	(Westinghouse Electric Company, 2003)
Microturbine	Failure to run	6.00E-04	5	(Ingersoll Rand Energy Systems, 2004)
Offsite Power	Loss of Offsite Power	2.10E-02	3	(Office of Nuclear Regulatory Research, 2001)
Turbine	Failure to Start	2.00E-02	10	(Westinghouse Electric Company, 2003)

Turbine	Failure while running	1.44E-02	10	(Westinghouse Electric Company, 2003)
Blower	Physical failure while running	1.37E-06	5	(Bush, 1978, Broadhurst et al, 1978)
Electric Valve	To denergized position	1.00E-03	3	(Westinghouse Electric Company, 2003)
Pressure Valve	To denergized position	1.00E-03	3	(Westinghouse Electric Company, 2003)
Electric Switch	Failure on demand	1.00E-03	3	(Westinghouse Electric Company, 2003)
Generator	Failure during operation	4.80E-06	5	(Westinghouse Electric Company, 2003)
Reactor Trip	Failure on demand	1.00E-07	5	(Delaney et al, 2004)
DC Transmission	Failure during operation	2.40E-03	10	(Delaney et al, 2004)
Battery Power System	Failure during operation	4.80E-05	3	(Delaney et al, 2004)
Inverter	Failure during operation	4.80E-04	3	(Delaney et al, 2004)
Battery Charger	Failure during operation	1.68E-04	3	(Delaney et al, 2004)
CO2 Loop	Failure during operation	5.45E-04	10	(Westinghouse Electric Company, 2003)
Steam loop	Failure during operation	5.45E-04	10	(Westinghouse Electric Company, 2003)
WBHX	Failure while operating	2.40E-05	10	(Westinghouse Electric Company, 2003)
Automatic Activation	Failure on demand	1.00E-04	10	(Delaney et al, 2004)
Indication	Failure on demand	1.00E-06	10	(Delaney et al, 2004)
Manual Hardware Activation	Failure on demand	1.00E-04	10	(Delaney et al, 2004)

Operator Failure to Act	Failure on demand	1.00E-03	10	(Delaney et al, 2004)

*A run time of 24 hours per demand was used to obtain failure probabilities per demand for data given in failure rate per hour