This document was prepared in conjunction with work accomplished under Contract No. DE-AC09-96SR18500 with the U.S. Department of Energy.

A Disciplined Approach to Accident Analysis Development and Control Selection

Terry L. Ortner, PE
Mukesh K. Gupta

Abstract

The development and use of a Safety Input Review Committee (SIRC) process promotes consistent and disciplined Accident Analysis (AA) development to ensure that it accurately reflects facility design and operation; and that the credited controls are effective and implementable. Lessons learned from past efforts were reviewed and factored into the development of this new process. The implementation of the SIRC process has eliminated many of the problems previously encountered during Safety Basis (SB) document development. This process has been subsequently adopted for use by several Savannah River Site (SRS) facilities with similar results and expanded to support other analysis activities.

Introduction

In 2002 a new Documented Safety Analysis (DSA) and associated Technical Safety Requirements (TSRs) for the SRS Tank Farm facilities were developed in accordance with the requirements and guidance provided in DOE-STD-3009-94[1] to comply with 10CFR830 Subpart B[2]. In preparing for this substantial effort, a review of past experiences with Tank Farm SB development, implementation, and maintenance efforts was conducted to identify lessons learned that could be applied to the new DSA/TSR development effort. This review identified the following key issues:

- The facility engineering staff did not consistently display a strong ownership or understanding of the facility SB; instead they typically deferred to Regulatory Program personnel or to Washington Safety Management Solutions (WSMS) safety analysts that supported facility operations.
- During SB development there was a lack of a formal and clear communication mechanism between the facility engineering staff and the safety analysts with respect to accident scenario development and the specification of applicable inputs and assumptions.
- The control selection process was typically not performed in a collaborative manner with operations participation. This resulted in controls that were sometimes difficult or cumbersome to implement. Additionally there was a heavy reliance on the use of administrative versus engineered controls, even where engineered controls were sometimes available.
- Senior management was not typically involved in the SB development process until the final SB document approval stage. This resulted in significant rework and schedule

slippage when senior management directed an alternate analysis approach or control scheme.

An evaluation of these key issues concluded that there was a compelling need to devise a new and deliberate process for the development of the Tank Farm DSA and TSRs. The SIRC process was expressly developed to satisfy this need.

SIRC Process

The SIRC process was developed to provide a disciplined review and approval process for critical aspects of the Tank Farm DSA/TSR development effort. Figure 1 provides a depiction of the principal steps of the SIRC process. A key element of this process is the assignment of a facility Design Authority (DA) engineer as the "owner" for each accident. The assigned DA engineer is responsible for:

- developing accident progressions, facility inputs and assumptions, and analysis approach;
- identifying the need for Safety Class (SC)/Safety Significant (SS) controls based upon the results of the unmitigated analyses;
- leading the development of effective control sets and verifying the adequacy of the controls;
- identifying and initiating further control evaluations (e.g., backfit analyses, Natural Phenomena Hazard [NPH] qualification analyses, instrument uncertainty calculations);
- serving as the principal facility reviewer of the applicable DSA/TSR sections; and
- serving as the primary spokesperson for the assigned accident during SIRC reviews and subsequent reviews with the Department of Energy (DOE) and with Defense Nuclear Safety Facility Defense Board (DNFSB) staff members.

The assigned DA engineer is paired with an accident analyst to foster a team approach, augmented as needed with support from other organizations (e.g., Operations, Regulatory Programs).

Although much of the discussion in this paper is focused on AA, the SIRC process has also been used to provide a forum for the review and approval of selected key inputs and assumptions for Hazard Analyses. This has been particularly useful when the Hazard Analysis for a major modification concludes that there is no need to credit any controls for the facility/collocated workers.

SIRC Membership and Responsibilities

The SIRC Process provides for a two tiered approach to the review and approval of AA information, including a SIRC Subcommittee and a Senior SIRC. The SIRC Subcommittee is composed of experienced representatives from the DA Engineering, Regulatory Programs, Operations, Safety Analysis, and DOE Engineering organizations. This group is responsible for the review and approval of the unmitigated AA progression(s), analysis approach, key inputs and assumptions, unmitigated AA consequence results evaluation, control selection, and mitigated AA results. Additionally the SIRC Subcommittee can be used as working forum to develop facility positions on specific SB issues. Approval by the SIRC Subcommittee requires a

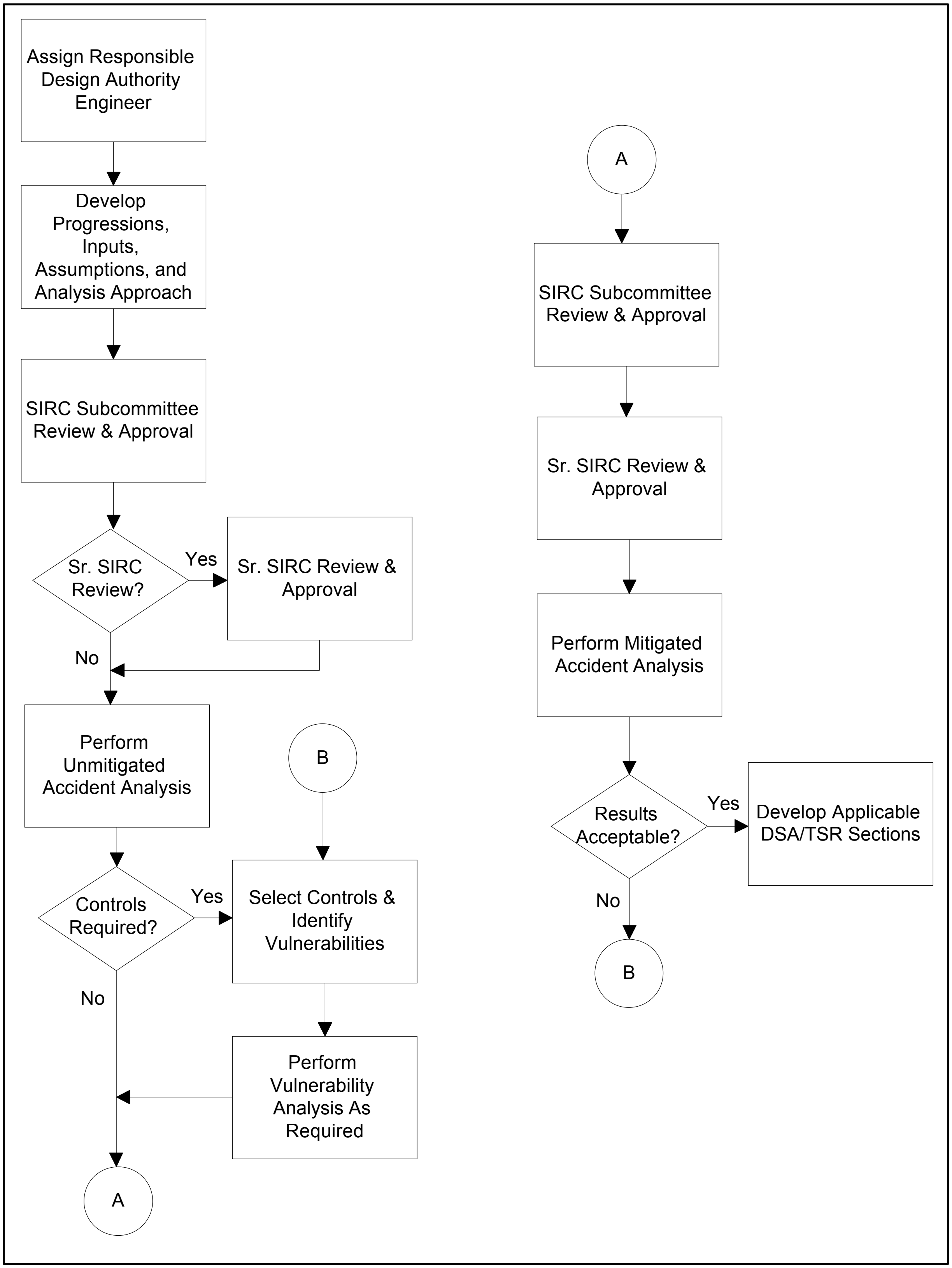

Figure 1 SIRC Process.

consensus of the members. The Senior SIRC is composed of senior managers from the same organizations represented on the Subcommittee. Approval by the Senior SIRC requires a unanimous decision by the voting membership. Although DOE management participates in the Senior SIRC, they are not voting members. DOE's membership is intended to promote communication of expectations between the DOE and the contractor and to lend their perspective on key issues/concerns. The Senior SIRC is responsible for reviewing selected key inputs and assumptions, and all unmitigated AA consequence results evaluations, control selections, and mitigated AA results. Additionally the Senior SIRC is responsible to disposition any vulnerabilities identified for the approved controls.

The participation of the DOE in the SIRC process has to be managed in a manner that balances its involvement in the process with its mandated oversight role. Approval via the SIRC process can not be construed by the Contractor as a guaranty of obtaining DOE approval when the associated SB documents are subsequently submitted. As non-voting members of the SIRC Subcommittee and the Senior SIRC, the DOE is under no obligation to pass judgment on the material presented in SIRC meetings. Our experience with the DOE's participation in the SIRC process to date has not been problematic in this respect. Additionally the DNFSB site representatives have been invited to observe Senior SIRC meetings as a means to ensure that they have the opportunity to be aware of significant SB development decisions and associated rationale on a real time basis.

Unmitigated Analysis

The responsible DA engineer, together with the accident analyst will review the supporting Hazard Analyses and identify those Hazard Events requiring further evaluation as Design Basis Accidents (DBAs) for the accident of interest. The review will identify the initiators for the assigned accidents so that the progression(s) can be accurately defined. The review will further identify those inputs and assumptions that are required for the analysis and that are within the purview of the facility (typically design, process, or operational in nature). Formal documentation of these inputs and assumptions via Safety Analysis Input Sheets is required to ensure that adequate technical rigor is embedded in the development process and to provide a review vehicle for the SIRC process. These input sheets are also used to document the Material at Risk to be used in the analysis (i.e., the material characteristics and volume/quantity/rate involved in the unmitigated scenario). To avoid duplication, the development of the input sheets is coordinated via the SIRC Subcommittee since some inputs and assumptions can be used in multiple AAs. The input sheets are not intended to take the place of formal calculations or technical reports. All calculationally-derived inputs must be based on an approved and confirmed (i.e., no open items) calculations/technical reports. Table 1 identifies and describes the information that must be addressed within the Safety Analysis Input Sheets.

The remaining source term parameters (Damage Ratio, Airborne Release Fraction, Leak Path Factor, and Respirable Fraction) are developed by the responsible DA engineer together with the analyst. Although these values are reviewed via the SIRC process, they are not required to be documented via Safety Analysis Input Sheets since these are typically well established for a given scenario based on the use of DOE-HDBK-3010[3] unless the use of a nonstandard source term parameter value is recommended (e.g., an ARF for a spray from a leaking jumper connector).

Table 1 Safety Analysis Input Sheet

Input Name	Provide descriptive noun name (e.g., Pump Tank Volume)
Conservative Direction	Identify direction of input value that results in a higher consequence
Safety Analysis Use	Briefly describe intended analysis use(s)
Normal Range	Identify normal operating range of input parameter
Inherent Controls	Identify any controls that are inherent in the input/assumption and that must be protected to preserve the adequacy of the analysis
References	Identify supporting references (e.g., calculations, technical reports, handbooks, drawings, specifications)
Historical Events	Briefly summarize actual operating experience that may be useful to support the recommended input/assumption
Physical Limitations	Describe any applicable physical limitations inherent in the input/assumption
Safety Analysis Value	Specify value to be used in accident analysis
Justification	Provide technical justification for the recommended Safety Analysis Value addressing both its adequacy and appropriateness with references as needed
Assumptions	Identify and justify any assumptions made in arriving at the recommended Safety Analysis Value

The responsible DA engineer and analyst will mutually establish a recommended analysis methodology approach. In the past, many Tank Farm AAs were performed as single point analyses (i.e., the analysis calculated a consequence based upon a single input value). Any subsequent changes in input values required revised analyses to be performed. This inefficient use of limited analysis resources often resulted in undesirable cost and schedule impacts. In recognition of this, a concerted effort is made to encourage the use of alternate approaches, as appropriate. Such approaches include the use of "Victory" analyses (backwards calculation of what value a key input parameter would have to be for the resulting consequence to reach an Evaluation Guideline [EG]) and "Ruler" analyses (parametric type calculation of consequence as a function of a key input parameter). These types of calculations are sometimes useful in assessing the relative sensitivity of the analysis results to a given input/assumption.

The responsible DA engineer presents the accident progression(s) (including source term information as described above), Safety Analysis Input Sheets, and recommended analysis approach to the SIRC Subcommittee. The SIRC Subcommittee reviews are typically very detailed in nature and often take the form of an "oral board" in which the engineer is expected to vigorously defend the proposed AA information. Aside from ensuring the technical adequacy of the information presented, the SIRC Subcommittee also verifies that the information is consistent, as applicable, with information previously approved for other AAs. The SIRC Subcommittee can approve the information as presented, approve the information with comments (requires subsequent SIRC Subcommittee Chair review to verify satisfactory completion of assigned open items), or reject all or part of the information (requires subsequent SIRC Subcommittee review of all rejected items). Once SIRC Subcommittee approval is obtained, the Chair is responsible to determine which, if any, of the unmitigated AA information requires further review by the Senior SIRC. This determination is typically based upon: the relative complexity of an input or assumption (especially where the input/assumption is primarily based upon a qualitative argument such as a maximum postulated spill size); the use of non-standard inputs/assumptions (Leak Path Factor < 1.0) or analysis approaches; and whether a similar input/assumption has previously been reviewed by the Senior SIRC. Those progressions, Safety Analysis Input Sheets, and analysis approaches requiring further review will be presented to the Senior SIRC by the responsible DA engineer. This review is typically not as detailed as the SIRC Subcommittee review and tends to focus on the larger implications of the information presented. Unmitigated AA can be completed once the required SIRC Subcommittee and Senior SIRC approvals have been obtained.

Control Selection/Mitigated Analysis

The responsible DA engineer will evaluate the results of the unmitigated AA with the analyst to assess whether the consequence results challenge the Offsite EG defined in DOE-STD-3009-94[1] or the Onsite Facility Worker and Collocated Worker consequence limits defined in Washington Savannah River Company (WSRC) Manual E7 Procedure 2.25[4], thus determining the need for Safety Class (SC)/Safety Significant (SS) controls. For the purposes of this paper, the Facility Worker and Collocated Worker consequence limits will hereafter be referred to as the Onsite EGs. Controls are selected in accordance with the requirements of the governing SRS functional classification procedure[4] using a team approach, led by the responsible DA engineer, which as a minimum includes the analyst and representatives from Operations and Regulatory Programs. The control selection hierarchy guidance (preventive versus mitigative, engineered versus administrative, active versus passive, control barrier selected closest to the hazard) is factored into the selection process as well as the need for controls that provide significant defense in depth. The team approach is used as a means to counteract the subjective nature of the control selection process and to provide a collaborative evaluation of the effectiveness of the controls as well as the facility's ability to implement the proposed controls. Where existing structures, systems, and components (SSCs) are selected, the DA Engineer will initiate the required evaluation activities (formal backfit analyses, NPH qualification analyses, uncertainty analyses, etc.). Additionally, if an administrative control is selected, the team will evaluate whether the proposed control rises to the level of a Specific Administrative Control (SAC) in accordance with DOE-STD-1186[5].

In some situations vulnerabilities may be identified during the control selection process or the subsequent evaluation of newly credited existing SSCs (e.g., no available means to prevent a flammable mixture from forming in the vapor space of a process vessel during or following a seismic event). Such vulnerabilities must be evaluated and dispositioned.

The responsible DA engineer will present the results of the unmitigated AA and the proposed control selections to the SIRC Subcommittee for review and approval. This detailed review verifies whether the:

- consequence results challenge the Offsite or Onsite EGs (i.e., Are controls required?);
- control selection is consistent with the hierarchy guidance and, if not, whether such deviations are appropriate;
- controls represent a complete set (including consideration of support systems and all identified initiators for each progression);
- controls are independent if multiple levels of control are proposed (i.e., primary controls and defense in depth controls can achieve their intended safety function without reliance on one another);
- controls are the most effective controls possible, to the degree practical;
- administrative controls (if any) should be designated as SACs; and
- controls are implementable

This review is highly subjective in nature and relies heavily on the collective knowledge and experience of the SIRC Subcommittee members. A technically inquisitive and thorough review is essential to ensure that a complete, effective, and defendable set of controls is selected. DOE participation at this level can provide the DOE with valuable insight into the overall selection process and affords the SIRC Subcommittee an opportunity to understand any concerns that the DOE representative may identify. This review may identify the need to revise previously approved progressions, inputs, assumptions, or analysis approaches and result in the need to reperform the unmitigated AA and control selection process.

Once all SIRC Subcommittee action items have been resolved and approval obtained, the responsible DA Engineer presents the unmitigated consequences and control selection to the Senior SIRC. As previously discussed, this review is typically performed at a higher level than that of the SIRC Subcommittee and tends to focus on the “big picture” implications of the consequence results and the control selection. The Senior SIRC will review any vulnerability analyses performed for the selected controls. One of three potential vulnerability disposition options (or some combination thereof) is approved by the Senior SIRC: (1) elimination of vulnerability via facility modification; (2) mitigation of vulnerability via compensatory measure; or (3) acceptance of the vulnerability as is. Cost/benefit analysis results are typically used as guidance during this disposition process. The result of the vulnerability disposition is factored into the development of the associated SB document text. Mitigated AA and the development of the associated SB document sections can be completed once the required SIRC Subcommittee and Senior SIRC approvals have been obtained. If the mitigated AA fails to confirm the effectiveness of an approved control, additional control selection, review, and approval activities are required.

Use of SIRC Subcommittee as a Working Group

In addition to the review and approval responsibilities described above, the SIRC Subcommittee can be used as a working forum to develop facility positions on specific SB issues. For example, during the implementation of DOE-STD-1186[5], the WSMS Regulatory Program group developed a preliminary assessment of which Administrative Controls should be designated as SACs. This assessment was reviewed in detail by the SIRC Subcommittee with a focus on defining the basis for why an Administrative Control was or was not designated as a SAC. The results of this review were subsequently documented in a formal technical report that was included as a reference in the DSA/TSR change package submittal to the DOE. Following the completion of the SAC designation reviews, the SIRC Subcommittee held a series of meetings during which each SAC was evaluated against the SAC considerations/attributes described in DOE-STD-1186[5] (e.g., LCO versus Administrative Control format, functional classification and reliability of SSCs used to implement the SAC, need for Human Reliability Analysis, need for additional operator training/drills). A detailed checklist, based on DOE-STD-1186 was developed and used to guide these evaluations. A great deal of effort was expended to define each SAC as clearly as possible and to identify any potential response actions, if a SAC requirement could not be met. The results of the SIRC Subcommittee evaluations were directly used as input into the SAC bases section development (author participated in the meetings). A brief overview of the SAC selection and evaluation results was presented to the Senior SIRC for concurrence. This review primarily focused on the implementation aspects of the SACs. The use of the SIRC process in the SAC development effort demonstrated the effectiveness of using a dedicated group of senior experienced personnel to resolve complex issues requiring consideration of a broad range of issues in a timely manner.

Experience with the SIRC Process

The SIRC process as described above was used in the development of the new DSA/TSR for the SRS Tank Farm facilities in 2002. The responsible DA engineers were subsequently able to effectively present the results of their effort to DOE and DNFSB staff personnel and resolve comments during the DOE review and approval process. These engineers returned back to their assigned facility positions and continue to serve as Subject Matter Experts for their accidents. Their participation in the development process, including the SIRC reviews, resulted in these engineers having an unusually comprehensive and valuable understanding of the DSA and TSRs. As part of the facility Technical Staff continuing training program, these engineers conduct in depth presentations on "their" accidents on a periodic basis.

The new Tank Farm DSA and TSRs were approved by DOE and implemented in April 2003. Although technical comments/questions were generated during the DOE review process, the bulk of these had to do with the level of bases detail provided in these documents rather than on the accident analysis inputs, assumptions, consequence results, and control selection. The SIRC process was judged to be successful by all involved and was institutionalized and used by the Tank Farm for all subsequent SB document revision efforts. The end result has been SB amendments that are routinely approved by the DOE without significant review issues. The general level of ownership and understanding of the SB within the Tank Farm engineering staff continues to increase as additional engineers go through SB document development/revision efforts via the SIRC process.

The most common problem encountered in the SIRC process subsequent to the initial DSA/TSR development effort is the lack of preparation on the part of the responsible DA engineers and the lack of involvement of their managers in ensuring their readiness. This lack of preparation has resulted in having to conduct multiple SIRC Subcommittee meetings before approval is obtained, negatively impacting project schedules. A typical problem is a lack of technical rigor in developing and defining proposed inputs/assumptions (including a lack of documentation for calculationally-derived values). To address such difficulties, a SIRC process overview briefing was developed and is now presented to each project team (including project management personnel) preparing to go through the SIRC process. This overview includes examples of actual problems encountered in past SIRC reviews.

The success of the SIRC process as used by the Tank Farms has resulted in the process being adopted by all other SRS Liquid Waste Operations facilities (Defense Waste Processing Facility and the Saltstone Facility) as well as by the Solid Waste facilities. Recently, the process has been endorsed for as a good practice for adoption by all SRS Hazard Category 2 nuclear facilities.

Conclusions

Experience with the SIRC process has demonstrated that the process provides an effective means to develop a technically sound SB and implementable controls. It has measurably improved ownership and understanding of the SB by the facility engineering staff; fostered a true partnership between the DA, Operations, Regulatory Programs, Safety Analysts, Senior Management, and the DOE in the development of accurate and implementable SB documents; and minimized the need to reperform AA and control selection work.

References

1. DOE STD-3009-94, Preparation Guide for US Department of Energy Nonreactor Nuclear Facility Safety Analysis Reports, Change Notice 3, March 2006
2. Title 10, Code of Federal Regulations, Part 830, Subpart B, Safety Basis Requirements
3. DOE-HDBK-3010-94, Airborne Release Fractions/Rates and Respirable Fractions for NonReactor Nuclear Facilities, Change Notice 1, March 2000
4. Washington Savannah River Company, Manual E7, Procedure 2.25, Functional Classifications, Rev. 14, November 30, 2004
5. DOE-STD-1186-2004, Specific Administrative Controls, August 2004