Final Abstract
ICONE-8347

A STUDY OF NUCLEAR POWER PLANT EVENTS THAT INVOLVE INSTRUMENTATION AND CONTROL SYSTEMS[1]

Terry W. Jackson
U. S. Nuclear Regulatory Commission
MS: T10-L1, Washington, DC 20555
Phone: (301) 415-6486
Fax: (301) 415-5074
Email: twj@nrc.gov

Robert W. Brill
U. S. Nuclear Regulatory Commission
MS: T10-L1, Washington, DC 20555
Phone: (301) 415-6760
Fax: (301) 415-5074
Email: rwb2@nrc.gov

The Office of Nuclear Regulatory Research at the NRC looked at two plant event databases to arrive at a snapshot of I&C impact on plant safety. These databases were the Accident Sequence Precursor(ASP) database and the Licensee Event Report(LER) database. The ASP database study considers events with a high conditional core damage probability. This study showed that (1) more than half of these events are affected by I&C failures, (2) many of the failed I&C components are found in pumps, valves, diesel generators, and power supply equipment, and (3) design/maintenance errors are as much of a cause of I&C failures as component failures. The LER database study was undertaken to determine if there is sufficient operational experience to uncover vulnerabilities of digital systems in nuclear power plants. This study considered those LERs involving digital-related failures over a five year period, beginning in 1994. The initial analysis placed the selected LERs in three categories, hardware, software, and human/system interface (HSI), and shows that the events are evenly disbursed in each of the categories. The analysis also shows that, during the time period, approximately 9% of all LERs contained digital-related failures, and approximately 9% of reactor trips are attributed to digital-related failures.

Both database studies show that I&C systems, particularly those that are digital, have a noticeable impact on nuclear power plant safety. As a result, nuclear safety research should conduct more in-depth studies on how I&C systems impact plant safety and how that impact can be quantified.

KEYWORDS: Instrumentation, Control, Digital, License Event Report, Accident Sequence Precursor

---

1 The views expressed in this paper are those of the authors and should not be construed to reflect the NRC position.

Proceedings of ICONE 8:
8th International Conference on Nuclear Engineering
April 2-6, 2000, Baltimore, MD USA

ICONE-8347

A STUDY OF NUCLEAR POWER PLANT EVENTS THAT INVOLVE INSTRUMENTATION AND CONTROL SYSTEMS[1]

Terry W. Jackson
U. S. Nuclear Regulatory Commission
MS: T10-L1, Washington, DC 20555
Phone: (301) 415-6486 Fax: (301) 415-5074
Email: twj@nrc.gov

Robert W. Brill
U. S. Nuclear Regulatory Commission
MS: T10-L1, Washington, DC 20555
Phone: (301) 415-6760 Fax: (301) 415-5074
Email: rwb2@nrc.gov

KEYWORDS: Instrumentation, Control, Digital, License Event Report, Accident Sequence Precursor

ABSTRACT

The Accident Sequence Precursor(ASP) database and the Licensee Event Report(LER) database provide a snapshot of instrumentation and control(I&C) impact on plant safety. The ASP database considers those events having a high conditional core damage probability. The ASP database study shows that (1) I&C failures impact more than half of the ASP events, (2) a large number of I&C failures occur in pumps, valves, diesel generators, and power supply equipment, and (3) design/maintenance errors cause as many I&C failures as component failures. The goal of LER database study is to identify operational experience that uncovers digital I&C vulnerabilities in nuclear power plants. This study considers digital-related LERs for a five year period; starting in 1994. The LER study placed LERs in three categories: hardware, software, and human/system interface(HSI). Analysis showed an even distribution of events in each of the categories. The analysis also showed that approximately 9% of all LERs, from 1994 to 1999, contain digital I&C failures, and 9% of reactor trips for those years are attributed to digital I&C failures. Both database studies show that I&C systems, particularly those that are digital, have noticeable impact on nuclear power plant safety.

INTRODUCTION

Instrumentation and control(I&C) systems are vital to nuclear power plant operation and safety. I&C systems provide operators with important plant information and send commands to plant components. Many balance-of-plant and safety systems are controlled automatically by I&C systems. With the introduction of digital technology, I&C systems are now embedded in plant components such as transformers, valves, and circuit breakers. As the U.S. Nuclear Regulatory Commission(NRC) moves toward a risk- informed, performance-based regulatory environment, two questions arise:

- What is the risk- significance of I&C systems? and
- What is the impact of digital technology on nuclear power plant safety?

The Office of Nuclear Regulatory Research reviewed the Accident Sequence Precursor(ASP) and the Licensee Event Report(LER) databases to find answers to these questions. These studies, while limited in detail, provide insight into risk-significance of I&C systems. This paper presents these insights, as well as other interesting statistics regarding digital I&C vulnerabilities. The results of the ASP and LER studies help guide future research and regulatory developments regarding digital I&C systems.

1 ASP DATABASE STUDY

For some nuclear power plant events, the failure of I&C systems contribute to an increase in conditional core damage

[1] The views expressed in this paper are those of the authors and should not be construed to reflect the NRC position.

probability(CCDP). The CCDP is calculated as the probability of core damage given the fact that certain system failures have occurred. This study uses the ASP database, which provides the CCDP for selected LERs. Using the ASP database, those LERs involving I&C failures are collected and general conclusions are drawn concerning I&C failures and their effect on nuclear power plant safety. The following analysis is performed:

- the number of ASP events affected by I&C failures versus the total number of ASP events,
- the number of ASP events initiated by an I&C failure,
- location of I&C failures among plant systems,
- types of I&C failures (component failure, degraded performance, design error, maintenance error, and spurious operation)
- the frequency of I&C-related ASP events per year

The ASP database study does not differentiate between digital and analog technology since the distinction between the two technologies is not available in many of the ASP LERs. Furthermore, the type of I&C technology does not affect ASP calculations since it is based on the operability of the system and not the technology that carries out that operation.

1.1 ASP Characterization by Number of Events

The ASP study uses version 1.97 of the ASP database, which was developed by Idaho National Engineering Laboratory for the NRC(USNRC, 1997a). The following conditions govern the study:

- Only ASP LERs between 1984 and 1997 are observed since this time period captures events associated with a mature nuclear industry.
- Only those events having a CCDP of 1×10^{-5} or higher are considered due to their level of safety-significance.

I&C-related events are those events where the failure of an I&C component is part of the progression of events leading to a high CCDP. The following are statistics regarding the number of total ASP events and the number of I&C-related ASP events:

- 217 ASP events fall within the conditions stated above. I&C failures contribute to 86 of those events.
- 65 ASP events were initiated by I&C failures.

Table 1 provides a breakdown of I&C-related ASP events versus all ASP events by CCDP ranking.

1.2 ASP Characterization by I&C System

In the ASP study, four types of I&C systems are considered: safety, control, monitoring, and support. I&C safety systems are those structures, systems, and components that are relied upon to remain functional during and following design basis events(taken from the definition of safety-related structures, systems and components in 10 CFR 50.2). Control systems are those systems that manage normal balance-of-plant operation, and support systems are those systems that provide a function such as electric power, instrument air, HVAC, control power, and cooling water. Monitoring systems include alarm and display systems providing plant status to operators.

Table 2 provides the number and location of I&C failures contributing to a CCDP of $1\text{x}10^{-5}$ or greater. The number of I&C-related ASP events and I&C failures do not coincide since some ASP events contain multiple I&C failures among different plant systems. The following observations are made through the categorization of I&C failures by system type:

- Components in safety systems contribute the most to ASP events having CCDP of 1×10^{-5} or larger(46 failures).
- Support and control system I&C failures, when combined, contribute to more than half of the I&C failures(60 failures).

Table 1. I&C-related events vs. the total number of ASP events.

CCDP	Total ASP Events	I&C Related ASP Events	Percent I&C-related ASP Events
$1\times10^{-1} < x \leq 1$	0	0	—
$1\times10^{-2} < x \leq 1\times10^{-1}$	1	1	100%
$1\times10^{-3} < x \leq 1\times10^{-2}$	7	3	43%
$1\times10^{-4} < x \leq 1\times10^{-3}$	93	34	37%
$1\times10^{-5} < x \leq 1\times10^{-4}$	116	48	41%
Total:	**217**	**86**	**40%**

Table 2. ASP I&C failures categorized by system and subsystem type.

System Type	Subsystem Type	Number of I&C Failures	Percent Total I&C Failures
Monitoring	Generator/Turbine Protection Circuits	2	1.83%
	Hotwell Level Measurement	1	0.92%
	Subtotal:	**3**	**2.75%**
Safety	Engineered Safety Features Systems	25	22.94%
	MSIVs, PORVs, and SRVs	7	6.42%
	Reactor Protection System(RPS)	7	6.42%
	Emergency Diesel Generators	6	5.5%
	Radiation Monitoring	1	0.92%
	Subtotal:	**46**	**42.2%**
Support	Power Supply	31	28.44%
	Instrument Air	4	3.67%
	Service Water System	2	1.83%
	HVAC	1	0.92%
	Subtotal:	**38**	**34.86%**
Control	Feedwater Control	12	11.01%
	Generator/Turbine Control	6	5.5%
	Steam Dump Control	2	1.83%
	Reactor Pressure Control	1	0.92%
	Plant Multiplexer	1	0.92%
	Subtotal:	**22**	**20.18%**
	Total:	**109***	**100%**

* Of the 86 I&C-related ASP events, some contained multiple I&C failures.

- I&C failures associated with pumps, valves, or diesel generators contribute the most to the safety system category(38 out of 46 failures).
- Power supply failures contribute the most to the support system category(31 out of 38 failures). Power supply failures are associated with control circuitry within breakers/inverters, or with instrument power supplies.

1.3 ASP Characterization by I&C Failure

I&C failures are catalogued into five categories: component failure, degraded performance, design error, maintenance error, and spurious operation. In component failure, the I&C equipment does not function. Degraded performance refers to the incomplete accomplishment of the I&C system's designated function. Spurious operation includes those instances where the I&C system actuates when it is not necessary. Finally, design and maintenance errors involve those incorrect actions performed by technicians, developers, and operators that prevent the I&C system from accomplishing its full task.

Table 3 lists the types of I&C failures found in the ASP database study and how many occurred. Component failures comprise the majority of I&C failures with 37 out of the 109 total I&C failures. There are various types of component failures, but it is interesting to note that 10 of the 36 component failures are power supply failures, and another 6 are attributed to relay failures. Another point of interest is that out of the 19 degraded performance incidents, 18 are associated with safety and control systems.

1.4 ASP Characterization By Year

Figure 1 correlates the number of I&C-related ASP events by year for 1984 through 1997. To draw conclusions from this data, it is better to consider the percentage of I&C-related events versus all events, as shown in Fig. 2. Also shown in Fig. 2 is a regression plot of percent I&C-related ASP events for all ASP events within a year. While the percentage is decreasing (-0.96 percent/year), the average number of I&C-related events is approximately 40% of the total ASP events.

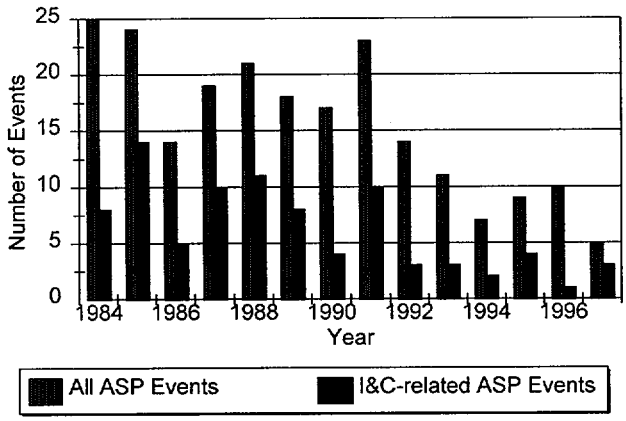

Figure 1. Number of I&C-related ASP events by year.

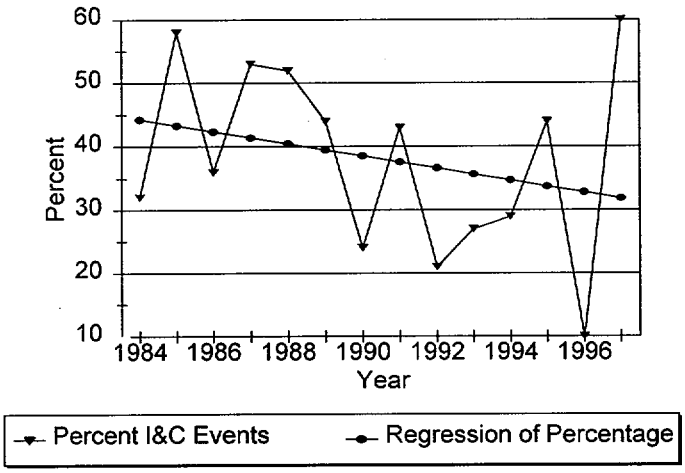

Figure 2. I&C-related ASP events versus all ASP events for the conditions of this study.

Table 3. Types of I&C failures for the I&C-related ASP events.

Types of Systems	Component Failure	Degraded Performance	Design Error	Maintenance Error	Spurious Operation
Control	9	6	1	5	1
Monitoring	1	0	0	1	1
Safety	12	12	4	12	6
Support	15	1	6	11	5
Total:	**37**	**19**	**11**	**29**	**13**

The actual I&C safety performance trend is difficult to determine from the ASP database for two reasons. First, there are not many data points in the latter years (1993 - 1997), which results in a large variance between those data points. Second, most ASP events are composed of multiple failures involving I&C, mechanical, and electrical components. Due to CCDP contribution from multiple types of system failures, it is difficult to determine the trend of one type of system, such as I&C.

2 LER DATABASE STUDY

The LER database consists of reports from the licensees for types of reactor events and problems that are believed to be significant and useful to the NRC in its effort to identify and resolve threats to public safety. It is designed to provide the information necessary for engineering studies of operational anomalies and trends and patterns analysis of operational occurrences. This database is stored in the Sequence Coding and Search System (SCSS) web site(USNRC,1999).

A study of these LERs was undertaken to determine if there was sufficient operational experience which could be used to uncover digital I&C system vulnerabilities in nuclear power plants. This examination covered all LERs during the years 1994-1998 and includes both digital failures and external events causing digital I&C systems to malfunction. An example of an external event affecting a digital I&C system is a case in which the control room operators received annunciations indicating that nonessential loads from the 600-volt bus had been de-energized. This event was caused by an arcing ground on a freight elevator brake solenoid, which resulted in a trip of the nonessential load lockout logic on the 600-volt bus. The ground also caused a trip of the RPS motor-generator feeder breaker(The affected breaker is equipped with a microprocessor-based trip unit.). The ground affected the trip unit such that its microprocessor actuated the breaker, which in turn tripped the reactor.

Our initial analysis placed the selected LERs in three categories: hardware, software, and human/system interface (HSI)(A significant number of the LERs include personnel errors which did not result in inappropriate operator actions. These are included in the category HSI.). In a number of LERs, the reported problem fell into multiple categories. For example, in one LER, a sudden trip of the main turbine generator resulted in a reactor trip. The causes of the turbine trip include:

- a hardware failure in a digital feedwater control card,
- a software error in the main turbine trip logic allowing a single failure to trip the turbine, and
- an HSI (personnel) design error where the redundant turbine trip relays were connected in parallel rather than in series.

2.1 LER ANALYSIS SUMMARY

There are 5681 LERS between 1994 -1998, with 446 of those LERs involving digital anomalies. Figure 3 shows the percent of LERs involving digital anomalies on a per year basis. With the exception of 1994, the number of LERs is relatively constant. A possible explanation of the high number of digital-related LERs in 1994 is that it was a year in which utilities performed a number of digital upgrades and startup and learning problems occurred.

There were 484 reactor trips from 1994 - 1998, with digital anomalies contributing to 60 of these. As shown in Fig. 4, the

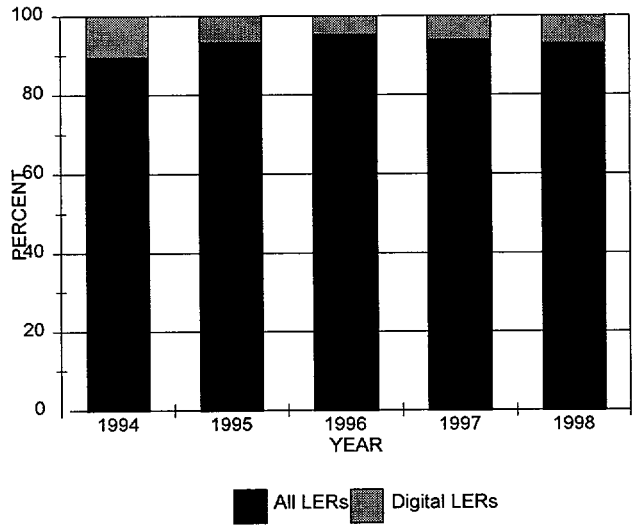

Figure 3. LER percentages.

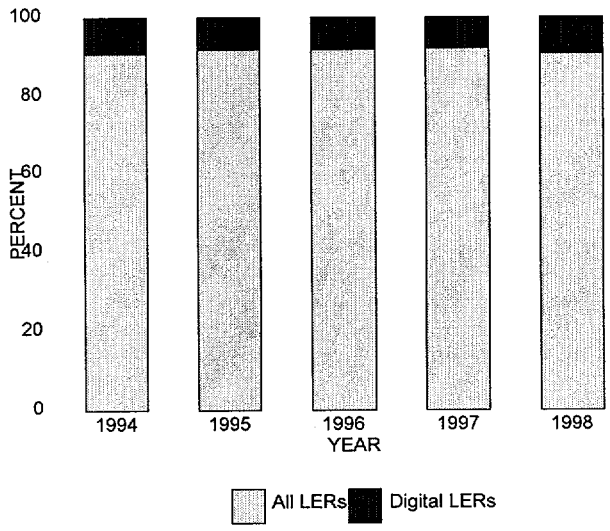

Figure 4. Trip percentages.

percent of all trips caused by digital anomalies is relatively constant over the time period. Approximately 13% of all digital-related LERs involved a reactor trip.

The number of digital LERs per category(hardware, software, and HSI) is evenly distributed, as shown in Fig. 5. Fig. 6 presents an analysis by system type. Digital anomalies in three safety/risk-significant systems(reactor protection, feedwater, and reactor coolant system) contributed to nearly 28% of the LERs. The largest single contributor to the LERs was the plant computer at 26%.

Table 4 presents data on the number of digital anomalies for each reactor vendor. The table indicates the number of incidents for each reactor manufacturer is relatively the same for the number of units produced by that manufacturer.

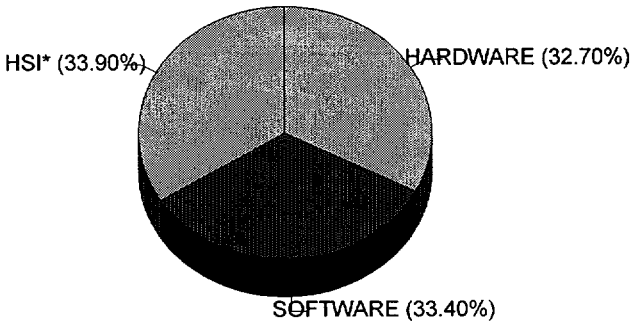

Figure 5. Digital anomaly categories.

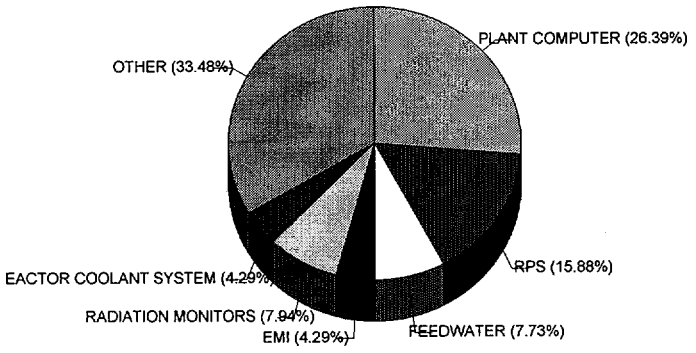

Figure 6. Digital LERs by system

CONCLUSION

To support the NRC's mission, the Office of Nuclear Regulatory Research engages in safety research related to I&C systems. It is important for this research activity to remain abreast of safety-related needs in the nuclear industry, particularly as the agency moves toward a risk-informed regulatory environment. To support this notion, this report looks at I&C safety performance and its impact on nuclear power plant safety using the ASP and LER databases. This section observations made from the database studies.

Although the ASP database does not provide the detailed information necessary to determine the exact risk-importance of I&C systems, it does provide many indicators showing that some I&C systems are risk-significant. The following observations support this statement:

- Only ASP events with a CCDP of $1x10^{-5}$ or greater are considered in this study. Of these events, 40% have at least one I&C failure contributing to the progression of events leading to a high CCDP and 30% of these events were initiated by an I&C failure.
- I&C failures in safety systems make up 42% of all I&C failures in ASP events having a CCDP of $1x10^{-5}$ or greater.

The first observation shows considerable I&C failure contribution to risk-significant, nuclear power plant events, and the second observation links I&C failures to risk-important plant systems(e.g., diesel generator, engineered safety features, and reactor protection system). Therefore, based on the findings of this report, it appears that I&C systems have a considerable impact on plant safety and steps should be taken to better identify their contribution.

Besides pointing to the risk-significance of I&C systems, the ASP database also brings to light certain issues, warranting future safety research. The following lists some observations made in the report:

- I&C components in support and control systems contribute to 55% of I&C failures in ASP events having a CCDP of $1x10^{-5}$ or greater.
- Of the safety-related I&C failures in this study, 83% involve pumps, valves, or diesel generators.
- Of the support system I&C failures in this study, 80% involve power supplies.
- Together, design and maintenance errors comprise 37% of the total I&C failures found in this study. Component failures alone comprise 34% of the total I&C failures.

The first observation indicates that some I&C components in non-safety systems have risk-significance. This same point was also noted in the Individual Plant Examinations(USNRC, 1997b). The second observation suggests a closer look at I&C components embedded in safety systems. Often, the scope of safety-related

Table 4. Digital anomalies extracted from license event reports by plant type.

Plant Type	Anomaly Type	1994	1995	1996	1997	1998	Total	% Total by Plant and Anomaly Type
Babcok & Wilcox	Hardware	2	2	2	2	2	10	37.0%
	Software	-	2	1	3	4	10	37.0%
	HSI*	2	3	-	2	-	7	26.0%
	Total:	**4**	**7**	**3**	**7**	**6**	**27**	
Combustion Engineering	Hardware	14	3	1	1	7	26	32.1%
	Software	8	4	10	3	10	35	43.2%
	HSI*	6	3	2	3	6	20	24.7%
	Total:	**28**	**10**	**13**	**7**	**23**	**81**	
Westinghouse	Hardware	26	13	12	14	15	86	37.0%
	Software	9	12	9	11	12	56	24.6%
	HSI*	19	14	8	30	12	82	38.4%
	Total:	**54**	**39**	**29**	**55**	**39**	**216**	
General Electric	Hardware	19	4	2	4	1	30	24.6%
	Software	13	10	14	6	8	51	41.8%
	HSI*	15	6	6	9	5	41	33.6%
	Total:	**47**	**20**	**22**	**19**	**14**	**122**	
All Plants	Hardware	61	22	17	21	25	146	32.7%
	Software	30	28	34	23	34	149	33.4%
	HSI*	42	26	16	44	23	151	33.9%
	Total:	**133**	**76**	**67**	**88**	**82**	**446**	

* Human System Interface

I&C components is limited to reactor protection systems and engineered safety features actuation systems. However, many safety systems and components, such as pumps, valves, and diesel generators, depend upon I&C components to function correctly. The third observation points to the risk-significance of embedded I&C components in breakers, inverters, and other required power supply components for both safety and non-safety systems. The final observation show design and maintenance errors having as much impact on I&C reliability as component failure.

Based upon the analysis of the LER database, the presence of digital systems affect plant performance and safety. The analysis has shown that digital systems are involved with approximately 9% of the events reported in LER's and contribute approximately 9% of the trips. Analysis of the LER database reveals the types of problems occurring with digital I&C system installation and usage. However, it is of insufficient depth to perform a definitive risk analysis. Perhaps one of the most significant observations is that with the use of computers, the problems encountered are caused by poor and/or incomplete implementation of the system requirements and the human tendency to believe what the computer shows them. A significant number of the LERs were attributed to missed surveillances. In many of these LERs, the surveillance scheduling computer programs were written in such a way that they did not alert the user to the critical dates.

REFERENCES

USNRC, 1997a, *Accident Sequence Precursor Database*, Ver. 1.97, U. S. Nuclear Regulatory Commission, Washington, D.C.

USNRC, 1997b, *Individual Plant Examination Program: Perspectives on Reactor Safety and Plant Performance*, NUREG-1560, Vol. 1, U. S. Nuclear Regulatory Commission, Washington, D.C.

USNRC, 1999, *Sequence Coding and Search System Database*, http://scss.ornl.gov/scss/default.htm