Proceedings of the 15th International System Safety Conference
Washington, DC August 13-17, 1997 page 393

SYSTEM SAFETY ANALYSIS PITFALLS

by Ludwig Benner, Jr., PE; Ludwig Benner & Associates; Oakton, VA

Keywords: hazard analysis; system definition; analysis technique deficiencies

Abstract

Unacknowledged deficiencies in system safety techniques create pitfalls for system safety analysts. The deficiencies are the absence of (1) a generally accepted specifications for defining a system for system safety analysis purposes, (2) a generally accepted method for defining systems, and task requirement to apply the specifications or method, and (3) a system safety analysis feedback method and requirement that would disclose these deficiencies.

System safety analysts typically use system or subsystem descriptions supplied by others. Published system safety hazard discovery techniques provide no specifications for what constitutes an acceptable system definition. This deficiency creates unsuspected problems for system safety analysts. Consequences include inadequately understood system interactions, and undiscovered or overlooked hazards that lead to unnecessary mishaps. Remedial action is suggested.

Introduction

My awareness of the deficiencies described in this paper was stimulated by a system safety analysis project. The project was undertaken to discover and define previously unidentified risks posed by existing equipment to be operated in a new environment. To perform the analysis, the potential interactions of the system with its environment had to be identified and documented. To discover new hazards and risks in the new situation, we needed to understand how the system worked. What could happen during system start up, operation, shut down or maintenance that could affect its new environment?

The system was described in engineering drawings and operating and maintenance manuals. We were advised of known hazards from previous analyses. Our attempt to understand how the system worked was guided by a principle I taught in MORT training courses (Ref 4):

"If you can't flow chart it, you don't understand it."

No flow charts of the system operations were provided. Therefore our first step was to recast the information furnished into flow charts of the system start-up, operation, shut-down and maintenance processes.

The system to be analyzed had been operating several years. Nevertheless, it took five revisions to get system personnel to clarify the processes, and develop a flow chart of component interactions that everyone could agree accurately defined the system. Some new hazards were observed as this was done. Because the system had been in service for several years, an obvious question arose:

How could an adequate system safety analysis have been performed on the existing system if its operation was defined so ambiguously?

That question prompted me to search the system safety literature to determine if system definition ambiguities resulted from failure to implement system safety definition task requirements, or from problems with such requirements.

System Definition Requirements

My initial search of dominant system safety literature for guidance about system definition task requirements occurred during the 1988-1991 period. (Refs 1-9) I found essentially no system definition task guidance for system safety analysts at that time. Most defined what a system is, but with one exception, (Ref 3) the task of defining the system to be analyzed was not addressed.

Frequent references were made to participation in the preliminary design and subsequent design stages of a project. The apparent thinking seemed to be that system safety analysts would use whatever descriptions and definitions of systems were provided to them for their analysis, and try to influence designs progressively. Documentation of the system components and their interactions, or a quality check for adequacy of such system definitions, was apparently not considered a system safety analysis function.

In the absence of system definition task guidance within the system safety community, my company established such a requirement for its work, and developed its own method for defining the systems to be analyzed. Typically the flow charting of system interactions to be analyzed required from 3 to 5 revisions before the system was adequately described for system safety analyses. The number of hazards that could then be identified increased significantly over those that could be found by applying checklists or experienced judgments to ill-defined systems.

Update of current system safety guidance search

To determine if the need for system definition guidance has been satisfied since the last search, the contents of the System Safety Analysis Handbook were analyzed recently. For this search, I asked two basic questions. First, is there a task requirement to define the system to be analyzed before the hazard discovery process begins? Next, if the task is specified, what are the system definition specifications and methods for performing that task?

System definition Vs System Description. While examining the techniques to answer these questions, a clear yes or no categorization did not show the differences among the techniques. I discerned a distinction between requiring *definitions* of the system operation, and *descriptions* of the system attributes.

A *system definition* identifies each component of the system or subsystem, and what it must do, when it must do it, and on whom or what it must act to produce the desired outcomes. A system definition describes dynamic interactions, among people, procedures and things -- and their influences on the outcomes.

A *system description,* on the other hand, may describe the system in terms of its components and their specifications, functions, physical or spatial relationship to each other, content flows, accident experiences, failures, failure rates, or other static *attributes, rather than interactions*

Criteria for categorizing techniques. Some system safety analysis techniques required descriptive data inputs before the analysis begins. Others postulated that the system definition be developed progressively as the hazard search progressed. They also differed about whether system definitions or descriptions were expressly specified, were only implied or were ignored. Some “techniques” were compilations of several techniques applied to specific circumstances, further complicating the review.

As I examined the techniques, I also found it necessary to provide for four different kinds of answers to the question about specifying tasks to define the systems. Were the tasks defined, specifically mentioned, only implied or ignored. Final criteria were selected to assign categories to the 90 published system safety techniques. The criteria and the codes used for each criterion are shown in Table 1.

During the examination, I observed that the techniques differed widely as to the starting points or starting data specified for the hazard search. The differences appeared to reflect different intentions, scope or acknowledged limitations of the technique. These data were noted for each technique.

The results of the examination and categorization process are presented in detail in Appendix 1.

Table 1 Criteria for Assigning System Definition Task Requirements Categories

1. Does the description of the technique have a requirement for a system definition to support hazard discovery?

A. requires definition of system elements and interaction sequences as basis for hazard analyses
B. requires definition of specified system elements and interactions interactively during hazard analyses
C. requires description of system or subsystem elements or functions
D. requires description of selected system attributes
E. implies or states that understanding of system operation is needed
F. has no requirements for system definition

2. Does the description of the technique speak to the system definition tasks to be performed to define the system? The answers observed ranged from descriptions of system definition task steps to no mention of them. Techniques marked "na" fit none of the above criteria.

1. System or subsystem definition task steps are specified
2. System or subsystem definition task steps mentioned but undefined
3. System definition tasks steps implied but undefined
4. System definition task steps ignored

Discussion of results.

This review was not intended to be an assessment of the merit of the techniques, and Appendix 1 should not be so construed. It *was* a review to determine the requirements for system definitions to permit an orderly, principled search for hazards. The criteria are essentially mutually exclusive, but several application issues arose during the review.

Not all techniques listed in Appendix 1 could be categorized with the system definition task for the hazard search. For example, Technique number 45 (Management Oversight and Risk Tree) focuses on the safety program as well as generic accident "causes" rather than specific hazard discovery with a systematic search of a defined system. Technique 16, (Critical Path Analysis) Technique 48 (Modeling (IDEF)) and Technique 66 (Safety Review) similarly focus on the Safety Management Plan and process. It might be argued that deficiencies in a safety management system create hazards. However for this review safety systems were considered to reflect good hazard discovery, definition and recommended control task needs, defined in the hazard analyst's work products.

Some techniques such as Technique 28 (Facility System Safety Analysis), Technique 34 (Fire Hazard Analysis), Technique 52 (Nuclear Safety Analysis), Technique 60 (Process Hazard Analysis) and Technique 74 (Software Hazard Analysis) covered several techniques. Thus the burden of defining the system to search for hazards systematically would rest on the included hazard search techniques.

Other techniques had differing purposes, such as Technique 13 (Control Rating Code Method), Technique 15 (Criticality Analysis) and Technique 86 (Uncertainty Analysis) which deal with ranking needs. Technique 76 (Statistical Process Control) addresses process reliability monitoring and measurements. Technique 85 (Time/Loss Analysis) is used to evaluate emergency response effectiveness, and only indirectly defines hazards.

Techniques 19 (Digraph Utilization within System Safety), Technique 55 (Petri Analysis) and Technique 69 (Sequentially Timed Events Plots) address ways to organize data, and thus have the potential to be used to define systems for methodical hazard discovery.

Table 2 summarizes the results of the analysis. Note that only on 21 of the 74 categorized techniques require any degree of system definition or description of system functions before a hazard discovery effort is launched. 28 have no specific requirements to understand the system before the hazard discovery effort is initiated. 31 of the techniques do not even mention any steps that might be required to define a system for analysis, whether before the analysis begins, or interactively. Only two require a system to be defined and state steps to do so.

Table 2 Number of Techniques Requiring System Definitions

	Requirements		Implementation			
	Total Count	Definition requirement	Steps Prescribed			
			stated	mention	imply	none
Define whole system	7	A	2	3	2	
Define specific subsystem	6	B	1	3	1	1
Describe elements, functions	8	C		1	6	1
Describe selected attributes	25	D	1	7	10	7
Implies understanding needed	19	E		2	4	13
None of the above	9	F				9
Not categorized	16					
Total	90		4	16	23	31

Source: Tabulated from Appendix 1

The column describing the input data in Appendix 1 is worth special attention, from the perspective of assuring the "proper" quality of the inputs before the hazard discovery effort is initiated. Specifications for the nature, form and content of the inputs were not available for most techniques. Without input specifications, *quality assurance checks of inputs for use in analyses are not possible*. This is another manifestation of the deficiencies cited.

Implications of Findings.

Analysis of the 90 techniques in the System Safety Analysis Handbook show that the system safety community has devoted much energy to developing hazard discovery tools for analyzing systems. System safety practitioners have clearly devoted far less energy to developing specifications for system definitions, or task requirements to assure adequate definition of systems they analyze.

The implications are clear. The likelihood of omissions during hazard discovery analyses is dependent on the quality of the inputs. Without an input quality assurance capability or method, the likelihood of omissions should be expected to be high, which is borne out by unexpected mishaps.

The consequences for system safety analysts are significant. They include

- a self-imposed constraint on system safety practitioners' hazard discovery capabilities,
- undiscovered hazards and inadequate risk predictions in system safety analyses,
- inability to perform objective quality assurance on analytical system safety work products,
- inability to monitor efficacy of predictions over the system life cycle, and therefore
- *unnecessary mishap losses.*

Conclusions

The work has disclosed that system definition ambiguities for system safety analysts result from deficiencies in system safety techniques and their requirements. The current body of system safety analysis techniques is deficient because it does not adequately address system definition tasks and methods. The system safety community needs to acknowledge these deficiencies. It then needs to devote significant energies to developing and formalizing a set of system definition techniques that permit methodical, consistent, complete, efficient and verifiable hazard discovery for systems it holds itself out to analyze. It also needs to work on the feedback deficiency by improving mishap investigations, as was proposed at the 1996 System Safety Society Conference (Ref 11.)

References

1. Miller, C. O., Requirements for a System Safety Programs as Delineated by MIL-STD-882, NASA Government Industry System Safety Conference, Greenbelt, Md. 1971
2. Hammer, Willie, Handbook of System and Product Safety, Prentice Hall, Inc. Englewood Cliffs, NJ 1972
3. Brown, D.B., Systems Analysis & Design For Safety, Prentice Hall, Inc. Englewood Cliffs, NJ 1976
4. Johnson, W.G., MORT Safety Assurance Systems, Marcel Dekker, New York 1980
5. Malasky, S.W., System Safety: Technology and Application, Garland STPM Press, New York 1982
6. Department of Defense, MILSTD 882B, 1984
7. Kayes, P.J. (Ed.), Manual of Industrial Hazard Assessment Techniques, World Bank, Washington, DC 1985
8. Olson, R. E., System Safety Handbook for the Acquisition Manager, System Safety Society, Littleton, CO undated (est. 1986)
9. Roland, H.E. and Moriarty, B, System Safety Engineering and Management (2nd Edition),, John Wiley & Sons, New York 1990
10. System Safety Society, System Safety Analysis Handbook. System Safety Society, Sterling, VA 1993.
11. Rimson, I.J. and Benner, L. Mishap Investigation: Tools for Evaluating the Quality of System Safety Programs, Hazard Prevention 33:1 1997.

Biography

Ludwig Benner, Jr. PE, BSChE is currently President of Ludwig Benner & Associates and Chairman of the Board of Directors of Events Analysis, Inc. 12101 Toreador Lane, Oakton, VA 22124 USA telephone - (703) 758 4800. e-mail - benner@mnsinc.com. Benner joined the System Safety Society in 1971, was elected a Fellow of the Society in 1981, and served as Executive Secretary of the Society in 1991-1992. He has performed many safety risk analyses and supervised or investigated industrial, transportation, and facility accidents, fires, explosions and injuries.

Appendix 1. Requirements for System Definition Hazard Analysis Techniques

		Requires System Definition Tasks	Specifies System Definition steps	
	System Safety Technique	|	|	Analysis starts with
1	Accident Analysis	na	na	assumed hazards, initial event
2	Barrier Analysis	C	3	hazardous energy flows
3	Bent Pin Analysis (BPA)	C	3	cable pin / functions
4	Cable Failure Matrix Analysis (CFMA)	C	3	cable functions, diagrams
5	Cause-Consequence Analysis	C	3	event types, safety functions
6	Change Analysis	D	3	modification
7	Check List Analysis	F	4	check list
8	Chemical Process Quant Risk Anal (CPQRA)	A	2	process definition
9	Common Cause Analysis	D	3	critical component
10	Comparison-To-Criteria (CTC)	E	4	safety criteria
11	Confined Space Safety	D	3	confine space, regulations
12	Contingency Analysis	E	4	credible mishaps in “given system”
13	Control Rating Code (CRC) Method	na	na	ranking technique
14	Critical Incident Technique	F	4	historical incident data, interviews
15	Criticality Analysis	na	na	ranking technique
16	Critical Path Analysis	na	na	activities/tasks
17	Cryogenic Systems Safety Analysis	D	3	cryogenic structure, hazardous effects
18	Damage Mode and Effects Analysis	A	3	schematic or functional block diagram, narrative
19	Digraph Utilization Within System Safety	na	na	defines interconnection of components
20	Electromagnetic Compatibility (EMC) Anal	C	3	protection plan
21	Energy Analysis	D	2	energy sources in system
22	Energy Trace Checklist	E	3	energy sources
23	Energy Trace and Barrier Analysis (ETBA)	A	1	system, energies , barriers and vulnerable targets
24	Environmental Risk Analysis	E	4	environmental regulations
25	Event and Causal Factor Charting	E	4	events
26	Event Tree Analysis	E	3	initiating events
27	External Events Analysis	E`	3	external events
28	Facilities System Safety Analysis	na	na	compilation of techniques
29	Failure Modes and Effects Analysis	E	4	components, functions, processes
30	Failure Modes & Effects & Criticality Anal	D	4	equipment in process
31	Fault Hazard Analysis	E	4	component, item or subsystem
32	Fault Isolation Methodology	C	4	system components
33	Fault Tree Analysis	D	4	undesirable event
34	Fire Hazards Analysis	na	na	compilation of techniques
35	Flow Analysis	E	4	energy flows
36	Hazard and Operability Study (HAZOP)	A	1	drawings, models, procedures and reports
37	Hardware/Software Safely Analysis	C	2	system specs, functional flow diagrams/data, etc.

Appendix 1. Requirements for System Definition Hazard Analysis Techniques (cont’d)

	Requires System Definition Tasks	Specifies System Definition steps	
System Safety Technique	|	|	Analysis starts with
38 Health Hazard Assessment (FHA)	D	4	hazardous materials exposures
39 Human Error Analysis	A	2	intended machine operation
40 Human Factors Analysis	C	3	experiential inputs
41 Human Reliability Analysis (HRA)	B	2	task, demands
42 Interface Analysis	D	4	drawings, task walkthrough
43 Job Safety Analysis	B	4	work process/operation
44 Laser Safety Analysis	E	4	lasers
45 Management Oversight &Risk Tree(MORT)	E	4	MORT chart,, safety system
46 Materials Compatibility Analysis	D	4	materials
47 Maximum Credible Accident-Worst Case	F	4	accidents
48 Modeling (IDEF)	na	na	addresses functional and information modeling
49 Naked man	D	3	“primordial” system
50 Network Logic Analysis	A	3	network of system logic elements
51 Nuclear Criticality Analysis	B	2	fissile material
52 Nuclear Safety Analysis (SAR)	na	na	compilation of techniques
53 Nuclear Safety Cross-Check Analysis	E	4	software
54 Operating and Support Hazard Analysis	B	2	operating tasks by people
55 Petri Net Analysis	na	na	addresses system states, abstractions
56 Preliminary Hazard Analysis	F	4	hazard checklists
57 Preliminary Hazard List	F	4	industry experience
58 Probabilistic Risk Assessment	A	2	system models, failure rate data bases, risk seq.
59 Procedure Analysis	D	2	personnel actions
60 Process Hazard Analysis	na	na	
61 Production System Hazard Analysis	D	4	hardware and software
62 Prototype Development	B	3	system replication
63 Relative Ranking	D	2	facility process areas, risk attributes
64 Repetitive Failure Analysis	E	4	repetitive failures
65 Root Cause Analysis	F	3	root cause checklists
66 Safety Review	E	3	product, operating procedures
67 Scenario Analysis	F	3	postulated scenarios
69 Sequentially-Timed Events Plot (STEP)	na	na	addresses event modeling
68 Seismic Analysis	D	2	structures, facilities
70 Single-Point Failure Analysis	D	3	single-point failure consequences
71 Sneak Circuit Analysis	D	3	circuits
72 Software Failure Modes and Effects Anal	B	1	process functional low charts
73 Software Fault Tree Analysis	E	3	software process flow
74 Software Hazard Analysis	na	na	compilation of techniques
75 Software Sneak Circuit Analysis (SSCA)	D	1	source code

Appendix 1. Requirements for System Definition Hazard Analysis Techniques (concluded)

	Requires System Definition Tasks	Specifies System Definition steps	
System Safety Technique	|	|	Analysis starts with
76 Statistical Process Control	na	na	process measurements
77 Structural Safety Analysis	D	3	structure design, applied loads
78 Subsystem Hazard Analysis	D	4	subsystem design
79 System Hazard Analysis (SHA)	E	4	subsystem hazards
80 Systemic Inspection	F	4	experiences, codes, checklists, etc.
81 Systematic Occupational Safely Analysis	F	4	work data
82 Task Analysis	D	2	task observations
83 Technique. for Human Error Predict. (THERP)	D	2	proposed procedure breakdowns
84 Test Safety Analysis (TSA)	D	3	test definition
85 Time/Loss Analysis (TL/A)	na	na	addresses emergency response evaluation
86 Uncertainty Analysis	na	na	addresses uncertainty of data
87 Walk-Through Task Analysis	E	2	task observations
88 What-If Analysis	E	2	hypoth. procedural, hardware/ software errors
89 What If/Checklist Analysis	D	2	area or step of process activity
90 Wind/Tornado Analysis	D	3	structures, contained hazards