# Index

Accident, definition, 75, 181–183, 184–185
Accident models, xix, 15–33, 58
 chain of events, 17–33, 56, 58, 67, 353
 domino, 16–17, 19
 Rasmussen and Svedung, 31, 32
 Swiss cheese, 17, 19, 34, 389–390
Accident process, 52, 59, 100, 211, 350, 383–384, 390
Active control, 77
Adaptation, 51–52, 81, 101, 166, 396, 398–400. *See also* Migration to high-risk states
Air traffic control, 12, 70, 184, 186, 192–193, 321–322
 conflicting goals, 12, 70, 199, 203
 coordination of multiple controllers, 294–295
 hazards, 184, 186
 safety constraints, 192–193
Alarms, 299–302
Assumptions
 environmental and use, 328–329, 333–334, 393
 monitoring, 328, 334, 401
Asynchronous evolution, 85, 95, 514–516
Audits, performance assessments
 based on incidents and anomalies, 387, 396, 404
 limitations, 401
 participatory, 401–403
 SUBSAFE, 455–458
 using assumptions underlying hazard analysis, 213, 227, 387, 393
Aviation, commercial, reporting systems, 407–409
Aviation Safety Action Program (ASAP), 408
Aviation Safety Reporting System (ASRS), 407–409, 431

Ballistic missile defense systems (BMDS, ICBM)
 history, xviii, 37, 69, 433
 STPA of, 214–217, 219–220, 225–226, 248–249
Batch chemical reactor accident, 9, 10, 49, 220–221
Bhopal, 24–28, 34–35, 90, 410
Black Hawk shootdown. *See* Friendly fire accident
Blame, 53–57, 59, 274, 390, 401, 426–433
 getting beyond, 56, 101, 349, 383–384, 410, 431–433

Cali American Airlines B-757 accident, 23–24, 39–40, 88, 97, 101, 174–175
Causal factors, organizational and contextual, 361–362
 symptoms vs. causes, 377
Causal filtering, 53–54
Certification, SUBSAFE, 452–455
*Challenger* Space Shuttle accident, 319, 411
 inadequate control, 67, 68
 migration to high-risk state, 231–232, 399
 silent safety program, 391
 systemic factors in, 55, 58, 197, 399, 428
Change, 175–176, 180, 186, 213, 226–227, 393–394, 396–400, 514–516
 monitoring for change, 95
 planned, 213, 227, 386, 397–398
 supporting with specifications, 308, 313, 347
 unplanned, 213, 227, 398–400
Chemical plants, 184, 185–186, 355, 356, 359
Cognitive fixation, 279, 280
Columbia Space Shuttle accident, 319
 ITA recommendation, 196
 metrics, 400
 migration to high-risk state, 51, 231–232, 417–419
 systemic factors, 55, 197, 227, 398–399, 426, 427–428, 434
Comair. *See* Lexington Comair accident
Commitment. *See* Leadership
Communication, 378–381. *See also* Risk awareness; Multiple controllers; Working groups
 between controllers, 378, 400
 communication channels, 386, 387
 of safety information, 307, 435

Comparisons, evaluation of STAMP
STPA, 239, 248–249
CAST, 388–390
Complacency, 383, 424, 458
Complexity, 4
and component interaction accidents, 173, 248
dealing with, 307
and redundancy, 264
types, 4
Component interaction accidents, 8–10
preventing, 173, 264
and probabilistic risk assessment, 35
and process models, 88, 95
and software 50
Constraints. *See also* Safety constraints
requirements vs. constraints, 11–12
in systems theory, 63, 65
Control loops. *See* Safety control structure
Control structure design. *See* Safety control structure
Coordination. *See* Multiple controllers
Cost, cost-effectiveness of safety activities, 171–176, 177–179, 251, 390, 415–420, 420–421
Culture, 52, 426–433
compliance culture, 172
culture of denial, 428–429
learning culture, 395
paperwork culture, 172, 429
role of leadership and commitment in, 177, 403
sharing information, shared responsibility, 401, 402
in SUBSAFE, 450

DC-10 accidents, 21–22, 303
Decentralized decision making, 43–45
Deepwater Horizon oil platform accident, 417, 424–425
Design rationale, documenting, 179, 224, 309, 310, 331, 338, 340, 341, 393, 411
Documentation, 179. *See also* Specification

Early design decisions, 172–174, 178–179, 318–319
Emergence, emergent properties, 63, 64, 67, 75
Event trees, 211, 212

Failure modes and effects analysis (FMEA), xvii, 14, 211
Fault tree analysis (FTA), xvii, 14, 58, 211, 212, 221, 249, 268
Feedback
about accident report recommendations, 388, 396, 404
designing and processing, 265–268, 295–305, 376–377
during operations, 393, 395, 396, 400–410, 425
in management of change, 394, 398
role in accidents, 35–36, 68, 79, 96–97, 380, 424
role in updating process models, 42, 43, 229
in STPA, 214, 221, 262
in systems theory, 65–66, 83, 96
Flexibility (resilience), 70, 398
Flixborough, 397
FOQA (flight operational quality assurance), 409
Friendly fire accident, 20–21, 85, 94, 99, 103–169, 225, 378–379, 396–397
Fukuchiyama train derailment, 432

Hazard, 184–191, 317–318
Hazard analysis, 179, 211
and human error, 230
revisiting after accidents and incidents, 227
Hazard assessment, 319–320, 322
Hazard log, 171, 217, 308, 317, 324–326, 332, 393
HAZOP, 211, 212, 221, 347
*Herald of Free Enterprise*, 12–14, 29–30, 67, 88
HFACS (human factors analysis and classification system), 389–390
Hierarchy, hierarchy theory, 63–65
HRO (high reliability organization) theory, 7, 12, 44–45, 410
Hindsight bias, 38–39, 43, 349, 361, 372–378
Human error, 36–47, 59, 361
in accident reports, 174–175
in continuous control tasks, 45–46
in control loops, 227–230
design for error tolerance, 46–47, 282–283, 296
design to reduce human error, 264, 273–305
impact of system design on, 39–41, 46–47, 59, 314
new types, 5, 175
in planning, 278–280
Human role in systems
backup, 276
monitor, 275–276
Human task analysis, 175, 179, 256, 330

Incident (definition), 185
Incremental control, 282
Independent Technical Authority (ITA), 195–202, 231–239, 451–452
ICBM. *See* Ballistic missile defense systems
INPO (Institute for Nuclear Power Operations), 406
Intent specifications, 309–313, 393, 397
Interfaces, 314

Just culture, 401, 430–433

Leadership, role of in safety, 177, 398, 401, 402, 403, 421–422, 427
Leading indicators. *See* Metrics
Lexington Comair accident, 270, 361, 389, 424
Limitations, 255, 345–347

Mars Polar Lander, 8, 10, 49, 66–67, 88
Management by exception, 284, 302
Management of change. *See* Change
Mental models, 41–44, 46, 54, 96, 226
Metrics, 59–60, 102, 400
Migration to high-risk states, 28, 51–52, 231, 382. *See also* Adaptation
 controlling, preventing 213, 383, 398–400, 419–420, 425–425
 examples, 28, 51, 166, 231–232, 417–419
 modeling and prediction, 243–248, 400, 417–419
Millstone nuclear power plant, 407, 428. *See also* Nuclear power
Mode confusion, 226, 277, 289–294
MORT (management oversight risk tree), 30–31
Multiple controllers, coordination, 98–100, 192–195, 277, 378–381
 ensuring consistent process models, 294–295
 examples, 99, 100, 192, 226, 235, 237–238, 294–295, 378
 identifying coordination risks, 237–238

Nagoya A300 accident, 21
Nimrod accident, 172, 429
Nuclear power, 406–407
Nuclear weapons, hazards, 191

Objective quality evidence, 450, 452
Occupational safety, 414
Operator error. *See* Human error

Paperwork culture. *See* Culture
Passive control, 76
Performance assessments. *See* Audits
Pharmaceutical safety, 70, 176, 198–209, 239–248
Plan continuation, 280
Preliminary hazard analysis (PHA), 254–255, 317
Problem reporting, 380–381, 386, 431, 458. *See also* Reporting systems
Process. *See* Accident process
Process improvement, 394–396, 403
Process models
 in analyzing accident causality, 374
 in human controllers, 228, 229–230
 initializing and updating, 266, 267–270, 286, 296–299, 383
 model condition in systems theory, 65, 66–67
 in STAMP (role in safety), 87–89, 95–97
 in STPA, 221, 243, 261
 and training, 411

Railroad car coupling accidents, 37
Rationale. *See* Design rationale
Recommendations (generating), 383–384
 assigning responsibility and followup, 388, 404
Reliability
 definition, 20–11
 vs. safety, 7–14, 47–50, 64, 184
Reporting systems, 404–409, 424–425. *See also* Problem reporting
 commercial aviation, 407–409 (*see also* ASAP; ASRS; FOQA)
 nuclear power, 405–407
 problems with, 407–408, 424–425
Resilience. *See* Flexibility
Responsibilities, assigning, 177, 334–336, 385–388, 433–440
Risk assessment, 102, 226, 319–327, 383, 423–425
 probabilistic risk assessment, 33–36, 59, 268, 395, 452
 risk analysis (programmatic or organizational), 231–239, 249
 risk matrix, 320
 risk metrics, 326
Risk awareness, 423–425
Root cause, 20–22, 28, 33, 56, 100, 349, 403

Safety case, 172
Safety constraints, 76–80
 enforcing, 261
 identifying, 191–195
 identifying and analyzing using STPA, 212–213, 218–219, 220–221, 261–263
 specifying, 329–338
 waiving, 398–399
Safety control structure
 constructing, 185–187, 195–209, 329, 334–336
 definition, 80–87
 assigning responsibilities, 433–440
Safety culture. *See* Culture
Safety-guided design, 171, 172–174, 251–263, 314
Safety information system, 440–442
Safety management plan (safety program plan), 177, 412–414, 442
Safety management system. *See* Safety control structure
Safety policy, 177, 183, 384, 422–423
Safety requirements. *See* Safety constraints
Safety working groups, 435
Sanity checks, 267
Separation of powers, 451–452
Social systems (engineering safety in), 176, 195, 198–209, 239–248
Software
 curse of flexibility, 50
 design, 173
 requirements errors, 48–50
 role in accidents, 47–50
Spacecraft
 defining accidents, 181–182
 defining hazards, 188, 218
 early trade decisions, 318–319, 322–327

Spacecraft (cont.)
risk management of Space Shuttle management structure, 195–202
STPA of JAXA HTV, 249
system boundaries, 187
Specifications, 179, 224, 307–309. *See also* Traceability; Design rationale
intent specifications, 309–313
SUBSAFE, 399, 411, 419–420, 445–461
System engineering, 176–180, 307–347
Systemic factors in accidents, 24–33, 55, 416–417, 420
examples of, 18
and probabilistic risk assessment, 33–34, 35
*USS Thresher* loss, 448
Systems nature of safety, 14
Systems theory, hierarchy, 63–65, 310, 463

TCAS (traffic alert and collision avoidance system), 97, 189, 191–192, 194–195, 312, 315–318, 328–347, 393
Thermal tile processing system (TTPS), 182–183, 188, 252–263
Three Mile Island (TMI), 10, 36, 39, 286, 300, 374, 406, 407
Time lags (delays), 66, 84–85, 94–95, 144, 154
Titanic, 34–35
Titanic coincidence, 34
Titanic effect, 34n
Traceability, 179, 309, 331, 338, 340, 341, 347, 393
Trade studies, 71, 318–327
Training and education, 402, 403, 410–412, 442–443, 459

Uberlingen accident, 100, 192–195, 378, 379–380

Working groups, 435

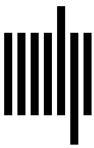
# Engineering a Safer World

## Systems Thinking Applied to Safety

**By:** Nancy G. Leveson

## Citation:

*Engineering a Safer World: Systems Thinking Applied to Safety*
**By:** Nancy G. Leveson
**DOI:** 10.7551/mitpress/8179.001.0001
**ISBN (electronic):** 9780262298247
**Publisher:** The MIT Press
**Published:** 2016



The MIT Press

For information about special quantity discounts, please email special_sales@mitpress.mit.edu

This book was set in Syntax and Times Roman by Toppan Best-set Premedia Limited. Printed and bound in the United States of America.

Library of Congress Cataloging-in-Publication Data

Leveson, Nancy.
Engineering a safer world : systems thinking applied to safety / Nancy G. Leveson.
p. cm.—(Engineering systems)
Includes bibliographical references and index.
ISBN 978-0-262-01662-9 (hardcover : alk. paper)
1. Industrial safety. 2. System safety. I. Title.
T55.L466 2012
620.8′6—dc23
2011014046

10 9 8 7 6 5 4 3 2 1