Index

A
Accident 29
Accident scenario 31
ALARP. See As low as reasonably practical
Analysis techniques
  barrier analysis 456
  bent pin analysis 471
  cause consequence analysis 327
  common cause failure analysis 339
  environmental hazard analysis 224
  event tree analysis 316
  failure mode and effects analysis 278
  fault hazard analysis 406
  fault tree analysis 240
  functional hazard analysis 93
  HAZOP analysis 300
  health hazard analysis 199
  job hazard analysis 490
  Markov analysis 430
  MORT analysis 483
  operating & support hazard analysis 177
  Petri net analysis 446
  preliminary hazard analysis 125
  preliminary hazard list 109
  process hazard analysis 381
  requirements hazard analysis 212
  sneak circuit analysis 416
  software hazard analysis 363
  subsystem hazard analysis 145
  system hazard analysis 164
  system of systems hazard analysis 520
  test hazard analysis 390
  threat hazard analysis 506
  AND gate 246
  As low as reasonably practical (ALARP) 552

B
BA. See Barrier analysis
Barrier 458, 463
Barrier analysis (BA) 456
  worksheet 465
  Bent pin analysis (BPA) 471
  worksheet 474
  Bottom-up analysis 64
  BPA. See Bent pin analysis

C
Cascading failure 343, 345
Cause-consequence analysis (CCA) 327
Cause-consequence diagram (CCD) 327, 330
  symbols 332
  CCA. See Cause-consequence analysis
  CCD. See Cause-consequence diagram
  CCF. See Common cause failure
CCFA. See Common cause failure analysis
CMF. See Common mode failure
Combinatorial model 553
Command fault 247
Commercial off-the-shelf (COTS) 552, 553
Common cause failure (CCF) 339, 342, 553
Common cause failure analysis (CCFA) 339
Common mode failure (CMF) 342, 554
Computer software configuration item (CSCI) 554
Computer software unit (CSU) 554
COTS. See Commercial off-the-shelf
Critical item list (CIL) 280, 554
CS. See Cut set
CSCI. See Computer software configuration item
CSU. See Computer software unit
Cut set (CS) 254
order 247

D
Deductive hazard analysis techniques 63
Dependent event 555
Deterministic process 555
Dynamic fault tree analysis 274

E
EHA. See Environmental hazard analysis
Engineering development lifecycle model 555
Engineering development model 15
Environmental hazard analysis (EHA) 224
worksheet 230
Error 556
ET. See Event tree
ETA. See Event tree analysis
Event tree (ET) 316
Event tree analysis (ETA) 316
diagram 323
Evidence event gate 271
Exclusive OR gate 246
Exposure time 248

F
Failure 280
cause 280
effect 280
mode 280
Failure mode and effects analysis (FMEA) 278
Failure mode effects and criticality analysis (FMECA) 278
worksheet 289
Fault 556
Fault hazard analysis 406
worksheet 410
Fault tree (FT) 240
Fault tree analysis (FTA) 240
FHA. See Functional hazard analysis
Firmware 366
FMEA. See Failure mode and effects analysis
FMECA. See Failure mode effects and criticality analysis
FT. See Fault tree
FTA. See Fault tree analysis
Function 11
Functional hazard analysis (FHA) 93
worksheet 97

G
Guide word 557

H
Hardware configuration item (HWCI) 557
Hazard 29
checklists 567
components 33
filter 47
mishap relationship 31
mitigation 559
recognition 40, 68, 74
risk 33
theory 31
triangle 35, 557
Hazard analysis
relationships 545
steps 70
technique 46
timing 57
type 46
Hazard and operability (HAZOP) 300
analysis 300
worksheet 309
Hazard causal factor (HCF) 37, 557
Hazard source (HS) 34
HAZOP. See Hazard and operability
HCF. See Hazard causal factor
Health hazard analysis (HHA) 199
worksheet 204
HHA. See Health hazard analysis
Hierarchy table 16
HIS. See Human system integration
Human error 558
Human system integration (HSI) 558
HWCI. See Hardware configuration item
INDEX 615

I
Importance measures 259
Independent event 558
Inductive analysis 63, 558
Inhibit gate 246
Initiating event (IE) 317, 558
Initiating mechanism (IM) 34
I-N-S concept 248
Interlock 559

J
JHA. See Job hazard analysis
Job hazard analysis (JHA) 490

K
Latent failure 559
Less than adequate (LTA) 484

M
Management oversight and risk tree (MORT) 483
Markov analysis (MA) 430
Markov–FTA comparisons 441
Min cut set 247
Mind map 89
Minimal cut set 247
Mishap 29
risk, 541, 543
Mitigation 559
MOCUS algorithm 254
MORT. See Management oversight and risk tree
Multiple occurring branch (MOB) 247
Multiple occurring event (MOE) 247
Mutually exclusive event 560

N
Non developmental item (NDI)

O
Operating & support hazard analysis (O&SHA) 177
worksheet 183
Operational sequence diagram 186
OR gate 246
O&SHA. See Operating & support hazard analysis

P
Petri net analysis (PNA) 446
PHA. See Preliminary hazard analysis
PHL. See Preliminary hazard list
Pivotal event (PE) 318, 560
PNA. See Petri net analysis
Preliminary hazard analysis (PHA) 125
worksheet 130
Preliminary hazard list (PHL) 109
worksheet 114
Primary failure 247
Primary hazard analysis techniques 59
Priority AND gate 246
Probabilistic risk assessment (PRA) 318, 561
Process FMEA 283
Process hazard analysis 381
Product FMEA 283
P-S-C concept 248
Pseudo-hazards 547
Qualitative analysis 65, 560
Quantitative analysis 65, 560
Reachability 448
Redundancy 561
Reliability 561
Repair 448
Requirements hazard analysis (RHA) 212
worksheet 214
Residual risk 561
RHA. See Requirements hazard analysis
Risk 30, 561
assessment 562
mitigation 559
priority number 562
Safety-critical 171, 562
Safety-critical function (SCF) 171, 562
Safety-critical functional thread 171, 563
Safety requirements/criteria analysis (SRCA) 212, 563
SCA. See Sneak circuit analysis
SCF. See Safety-critical function
Secondary failure 247
Secondary hazard analysis techniques 59
SHA. See System hazard analysis
Sneak 418
circuit 416, 563
indicator 425
label 425
path 424
timing 424
Sneak circuit analysis (SCA) 416
Software 366
Software Control Code (CC) Categories 370
Software Criticality Index (SwCI) 371
Software criticality level 368
Software FMEA 283, 285
Software hazard analysis (SwHA) 363
    worksheet 368
SoS. See System of systems
SoSHA. See System of systems hazard analysis
SRCA. See Safety requirements/criteria analysis
SSP. See System safety program
SSPP. See System safety program plan
SSR. See System safety requirement
SS–SC concept 248
State 431, 448, 564
State transition diagram 432
Stochastic process 432, 564
Subsystem 11
Subsystem hazard analysis (SSHA) 145
    worksheet 149
SwHA. See Software hazard analysis
System 10
    attributes 12
    development model 15
    function 18
    hierarchy 16
    laws 26
    lifecycle 13
    requirements 21
    safety 5
    safety engineering 5
    safety management 5
    safety principles 7
    safety process 6
    safety standards 7
    views 18
System hazard analysis (SHA) 164
System mishap model (SMM) 84
System of systems (SoS) 520
System of systems hazard analysis (SoSHA) 520, 530
System safety program (SSP) 565
System safety program plan (SSPP) 565
System safety requirement (SSR) 23

T
Target/threat outcome (TTO) 34
Task 565
Test hazard analysis 390
THA. See Threat hazard analysis
Threat hazard analysis (THA) 506
    worksheet 511
Top-down analysis 64
Top level hazard (TLH) 85
Top level mishap (TLM) 84
TTO. See Target/threat outcome

V
Validation 566
Verification 566