

Index

A

- Adaptive cruise control (ACC)
 - CarSim simulation results, 117–119
 - contract relationships, 114–115
 - definition, 99
 - fundamental objectives, 114
 - linearized force-balance equation, 99
 - low-fidelity simulation results, 117, 118
 - monolithic controller, 100
 - PI controller, 119–120
 - realizability, 116–117
- Adaptive stress testing (AST), 3
 - accelerated search algorithm, 78
 - aircraft collision avoidance system, 78
 - ACAS X, 88, 89
 - aircraft dynamics model, 91
 - COC advisory, 89
 - DND and DNC advisories, 89
 - DS2500 and CL2500 advisories, 89
 - initial state, 89
 - MAINTAIN advisory, 89
 - MCTS and Monte Carlo with
 - computation time, 93–94
 - NMAC, 88, 91–93
 - pilot model, 90–91
 - resolution advisories, 88
 - sensor model, 89
 - system diagram, 89, 90
 - TCAS, 88
 - definition, 78
 - full observability, 82–83
 - overview, 81, 82
 - partial observability
 - computational complexity, 87
 - modified MCTS algorithm, 85–87
 - seed–action simulator, 84–85
- aDOBO, 68
- Advanced driver assistance system (ADAS), 163
 - failure rate of
 - brute-force Monte Carlo method, 24–28
 - intermedia failure regions, 23–24
 - probability, 23
 - STOP sign detection system (*see* STOP sign detection system)
 - subset sampling algorithm, 23–24
 - functions, 5
 - robust, 6
 - test data generation
 - circuit aging, 14–16
 - corner case generation, 16–20
 - temperature variation, 11–13
 - visual perception system
 - image processing, 8–10
 - image sensing, 7–8
 - traffic sign detection system, 10–11
- Airborne collision avoidance system (ACAS X), 88, 89
- Airborne collision avoidance system for unmanned aircraft (ACAS Xu) case study, 192–193
- Aircraft collision avoidance system, 78
 - ACAS X, 88, 89
 - aircraft dynamics model, 91
 - COC advisory, 89
 - DND and DNC advisories, 89
 - DS2500 and CL2500 advisories, 89
 - initial state, 89

- Aircraft collision avoidance system (*cont.*)
 MAINTAIN advisory, 89
 MCTS and Monte Carlo with computation time, 93–94
 NMAC, 88, 91–93
 pilot model, 90–91
 resolution advisories, 88
 sensor model, 89
 system diagram, 89, 90
 TCAS, 88
- Airman Certification Standards (ACS), 149, 150
- Assume-guarantee formalism, 97, 100
- AST, *see* Adaptive stress testing
- Automatic emergency braking system, 193–195
- Automatic theorem proving (ATP), 79
- Autonomous driving functions
 adaptive cruise control
 CarSim simulation results, 117–119
 contract relationships, 114–115
 definition, 99
 fundamental objectives, 114
 linearized force-balance equation, 99
 low-fidelity simulation results, 117, 118
 monolithic controller, 100
 PI controller, 119–120
 realizability, 116–117
- LK control system
 CarSim simulation results, 117–119
 contract relationships, 114–115
 definition, 99
 fundamental objectives, 114
 goal of, 100
 low-fidelity simulation results, 117, 118
 PI controller, 119–120
 realizability, 115–116
- Autonomous intersection management, 182
- AUTOSAR, 168–170
- Aviation licensing exams, 148–151
- trajectories, 59
 worst-case disturbance, 61
- BreakingSystem*, 193, 194
- C**
- CarSim simulation results, 3, 117–119
- Certification of autonomous systems, 4
 aviation licensing exams, 148–151
 checkrides, 145, 155–156
 driving licensing exams, 146–148
 FAA's software certification, 158
 graduated licensing, 156–157
 knowledge tests, 155–156
 LIDAR, 158
 machine learning algorithms, 157–159
 software bugs and failures, 158
 SRKE taxonomy
 knowledge-based reasoning, 154
 robust physical perturbations, 153
 rule-based behaviors, 152, 153
 schematic diagram, 151
 sensory-motor actions, 152
 skill-based control, 152
 vision tests, 154–155
- Circuit aging, 6, 14–16, 22–23
- CMOS color sensor
 active and dark pixels, 9
 derivation, 8
 designing process, 18, 20
 growth rate of defect density for, 14
 image sensing, 7–8
- Convex-Hull computation
 with convex projections, 112–113
 with monotone functions, 111–112
- Cooperative adaptive cruise control (CACC), 182
- Crazyflie 2.0, 67
- CuSTOM, 70
- Cyber-physical systems (CPS), 2, 4
 adaptive control approach, 34
 architectural vulnerabilities, 34
 closed-loop system, 37
 computer-oriented security architecture, 33
 control law/strategy, 36, 37
 cost function, 36
 cross-layer codesign, 181–182
 cryptographic tools, 33
 cyberattack mitigation problem, 37–38
 discrete-time linear CPS model, 35–36
 DoS attacks, 33–34
- B**
- Backward reachable set (BRS)
 collision avoidance protocols, 59
 implicit surface function, 62
 level set method, 61
 non-anticipative strategies, 61
 obstacle function, 61
 ordinary differential equation, 60
 reach-avoid set, 61, 62
 safety-critical scenarios, 59

- fault-tolerance
 - embedded error detection, 174–178
 - explicit output comparison, 174–178
 - industrial case study, 178
 - optimization formulations, 175–177
 - for single-rate systems, 177–178
 - soft errors, 173
 - system error coverage, 174–175
 - game theoretical approach, 34, 35
 - holistic timing-driven synthesis
 - alpha ratio, 169
 - AUTOSAR standard, 169, 170
 - FETA, 169, 171
 - optimization constraints and objectives, 171–172
 - synthesis algorithms, 172–173
 - system model, 170
 - hybrid controller
 - analytical performance verification, 43–45
 - attack energy, 41
 - continuous state dynamics, 39
 - discrete state transition function, 39, 42
 - guard condition, 41–42
 - H_∞ optimal controller, 49–50
 - H_2 optimal controller, 49
 - infinite time horizon attack mitigation problem, 46
 - recursive hybrid state evolution, 48
 - RHC, 46–48
 - schematic diagram, 38, 39
 - simulation results, 51–53
 - sub-controller feedback, 38
 - switching logic, 39–42
 - UAS model, 50–51
 - integrity attacks, 34
 - model-based design
 - application layer, 167
 - cross-layer codesign, 169
 - functional models, 167–168
 - hardware platform, 168
 - holistic timing consideration, 168
 - multi-objective optimization, 168–169
 - schematic diagram, 166, 167
 - software models, 168
 - reachability analysis, 34
 - regulation objective, 36
 - security, 178–181
 - software challenges
 - architectural complexity, 165
 - cyber elements execute algorithms, 163
 - diverse and stringent design requirements, 165–166
 - environment uncertainty, 165
 - functional complexity, 163–164
- D**
- Deep neural networks (DNNs), 4
 - ACAS Xu case study, 192–193
 - adversarial perturbations, 190
 - automatic emergency breaking system, 193–195
 - brute-force enumeration, 190
 - clustering techniques, 188
 - compositional assume-guarantee verification, 187–190
 - input–output behavior, 191
 - MNIST dataset, 191
 - neurons, 190
 - Reluplex, 191
 - run-time monitoring and control, 195
 - targeted safety, 191
 - Denial of Service (DoS) attacks, 33–34
 - DNNs, *see* Deep neural networks
 - Driving licensing exams, 146–148
- E**
- Embedded error detection (EED)
 - examples, 174
 - industrial case study, 178, 179
 - performance overhead, 174
 - reliability, 174
 - schedulability, 174, 175
 - task execution time, 176
 - Explicit output comparison (EOC)
 - error detection, 174
 - industrial case study, 178, 179
 - reliability, 174
 - schedulability, 174, 175
 - task execution time, 176
- F**
- FAA’s software certification, 158
 - Fast and safe tracking (FaSTrack) algorithm, 70–72
 - Firing and Execution Time Automaton (FETA), 169, 171
 - Function approximator-based model learning, 66–67

G

- Game-theoretic attack mitigation problem, 38
- Gamma compensation, 10
- General attack mitigation problem, 37–38
- Goal-driven model learning, 67–68
- Graduated licensing (GL), 156–157

H

- Hamilton–Jacobi (HJ) reachability analysis, 2
 - advantages, 59
 - BRS, 59–62
 - high-dimensional state spaces, 58
 - limitations, 64–65
 - multi-vehicle trajectory planning, 62–64
 - safety analysis, 59
- Hybrid systems theorem proving (HSTP), 79

I

- Image processing, 8–10
- Image sensing, 7–8
- Integrity attacks, 34

K

- Knowledge tests, 155–156

L

- Lane-keeping (LK) control system
 - CarSim simulation results, 117–119
 - contract relationships, 114–115
 - definition, 99
 - fundamental objectives, 114
 - goal of, 100
 - low-fidelity simulation results, 117, 118
 - PI controller, 119–120
 - realizability, 115–116
- Learning-based schemes
 - function approximator-based model
 - learning, 66–67
 - goal-driven model learning, 67–68
 - HJ reachability analysis
 - advantages, 59
 - BRS, 59–62
 - high-dimensional state spaces, 58
 - limitations, 64–65
 - multi-vehicle trajectory planning, 62–64
 - safety analysis, 59
 - MB approaches, 65
 - MF approaches, 65

- in partially observable environments, 70–72
- safety analysis, 68–70

LIDAR, 158

Lincoln Laboratory Correlated Aircraft
Encounter Model (LLCEM), 89

LK control system, *see* Lane-keeping control
system

Lyapunov function, 44–45

M

- Magnetic levitation systems (Maglev)
 - control strategies, 137
 - description, 136
 - neural network model, 137–139
 - principle, 136
 - reachable set estimation, 139–141
- Markov Chain Monte Carlo algorithm, 2, 29
- Markov decision process (MDP), 80, 82
- Mixed integer linear programming (MILP),
172
- Model-based (MB) approaches, 65
- Model-free (MF) approaches, 65
- Monte Carlo sampling, 78, 79
- Monte Carlo tree search (MCTS), 81, 83, 93,
94
- Monte Carlo tree search with double
progressive widening
(MCTS-DPW), 81
- Multi-layer perceptrons (MPLs)
 - black box, 127
 - hidden layers, 125
 - input layer, 125, 126
 - input–output relation, 126
 - nonlinear real-valued function, 126
 - output layer, 125, 126
 - reachable set estimation, 131
 - bias vectors, 131
 - bounded input set, 128
 - cell construction process, 129
 - computation time and number of
reachtubes, 132, 133
 - layer-by-layer approach, 129, 130
 - output, 132, 133
 - partition, 129
 - reachMLP function, 130–132

N

- NARMA model, *see* Nonlinear autoregressive-
moving average model
- NARMAX model, 66

- Near mid-air collision (NMAC), 88, 91–93
- Nonlinear autoregressive-moving average (NARMA) model, 3
- action of neuron, 125
- activation function, 125–126
- discrete-time process, 125
- initial state of, 125
- Maglev (*see* Magnetic levitation systems)
- MLPs (*see* Multi-layer perceptrons)
- reachable set/state estimation, 124, 132–136
- ReLU, 124
- P**
- Partially observable Markov decision process (POMDP), 80
- Polyhedral controlled-invariant sets
- computation of, 106–108
- over-approximation of nonlinear parametrizations, 108–109
- removal of nonlinearities, 109–113
- Probabilistic model checking (PMC), 78–79
- Proportional integral (PI) controller, 119–120
- R**
- Real-time road test, 6
- Receding horizon control (RHC), 46–48
- Receiver operating characteristic (ROC) curves, 21–23
- Rectified linear unit (ReLU), 124
- Reinforcement learning algorithms, 80
- Reluplex, 191
- Resolution advisories (RA), 88
- S**
- SAFEOPT, 69
- Safety-critical systems
- AST (*see* Adaptive stress testing)
- exhaustive enumeration/mathematical proofs, 77
- formal methods, 78–79
- MCTS, 81
- sequential decision process, 80–81
- simulation-based methods, 78, 79
- Satisfiability modulo theory (SMT), 124
- Seed-action simulator, 84–86
- Sequential decision process, 80–81
- Skills, rules, knowledge, and expertise (SRKE) taxonomy
- knowledge-based reasoning, 154
- robust physical perturbations, 153
- rule-based behaviors, 152, 153
- schematic diagram, 151
- sensory-motor actions, 152
- skill-based control, 152
- STOP sign detection system, 6
- circuit aging, 22–23
- error estimation, 29
- failure rate estimation, 28–29
- histogram for estimated failure rates, 29–30
- temperature variation, 21–22
- three-stage cascade classifiers, 20–21
- Subset sampling (SUS) algorithm, 2
- failure rate estimation, 29
- histograms for classifier evaluations, 29–30
- intermediate failure regions, 23–24
- STOP sign detection system, 28
- T**
- Temperature variation, 6, 11–13
- Traffic alert and collision avoidance system (TCAS), 88
- Traffic sign detection system, 10–11
- U**
- Universal approximation theorem, 126
- Unmanned aircraft system (UAS) model, 50–51
- V**
- Validation, of ADAS, *see* Advanced driver assistance system (ADAS)
- Vehicle safety systems
- adaptive cruise control
- CarSim simulation results, 117–119
- contract relationships, 114–115
- definition, 99
- fundamental objectives, 114
- linearized force-balance equation, 99
- low-fidelity simulation results, 117, 118
- monolithic controller, 100
- PI controller, 119–120
- realizability, 116–117
- assume-guarantee formalism, 97
- invariant sets
- assume-guarantee contract, 100–103
- contract realizability problem, 104–105
- contract refinement heuristic, 105

- Vehicle safety systems (*cont.*)
 - controlled invariant sets, 101, 102
 - dynamical systems, 101
 - non-separable controlled-invariant set, 102
 - polyhedral controlled-invariant sets, 105–113
 - separable and centralized invariant sets, 102, 103
 - system decomposition, 104
- LK control system
- CarSim simulation results, 117–119
- contract relationships, 114–115
- definition, 99
- fundamental objectives, 114
- goal of, 100
- low-fidelity simulation results, 117, 118
- PI controller, 119–120
- realizability, 115–116
- polytopic robustly controlled-invariant sets, 98
- Vision tests, 154–155