

# Prefazione

Il rapido avanzamento tecnologico dei nostri giorni ha introdotto nella nostra vita una serie di infrastrutture, sistemi e applicazioni su cui facciamo affidamento per svolgere le nostre attività quotidiane. L'informatizzazione si è introdotta in modo molto pervasivo nelle attività umane e molti servizi sono percepiti come parte integrante dell'ambiente in cui siamo immersi. Alcuni di questi sistemi e infrastrutture sono critici perché la loro distruzione o un'interruzione del loro funzionamento può avere effetti catastrofici sulla sicurezza, sull'economia, sull'ambiente o sulla salute, del singolo individuo o della società intera. Sono ad esempio infrastrutture critiche le telecomunicazioni, i trasporti, il sistema elettrico, gli acquedotti, la finanza, la distribuzione del gas; sono esempi di sistemi critici il sistema di pilotaggio di un treno o di un aereo, il controllo elettronico di stabilità di un'automobile, il sistema di telecomunicazioni di un satellite. A causa della loro criticità, è quindi necessario poter garantire un certo livello di affidabilità, sicurezza o disponibilità per questo tipo di servizi.

Fondamentale per un funzionamento corretto ed efficace di tali sistemi è la capacità di analizzarne aspetti quantitativi relativi sia a caratteristiche prestazionali sia a caratteristiche di sicurezza, disponibilità o affidabilità che dimostrino e ci convincano della adeguatezza dei nostri manufatti per i compiti sempre più critici e delicati per i quali li utilizziamo. I due principali approcci per la analisi quantitativa sono la costruzione di modelli e la loro soluzione (analitica o tramite simulazione), in cui il comportamento del sistema è riprodotto tramite un modello, e la osservazione e la valutazione (anche con stimoli specifici) sperimentale. La descrizione di varie tecniche a formalismi appartenenti a questi due approcci costituisce il corpo di questo libro.

Questo testo viene proposto ed è utilizzato dagli autori come libro di testo per insegnamenti a corsi di laurea specialistica o magistrale in Informatica o Ingegneria Informatica anche se può essere adottato anche in insegnamenti per le corrispondenti lauree triennali. Il libro si compone di tre parti e 7 Capitoli scritti da autori diversi. La parte introduttiva contiene un primo capitolo che tratta i concetti di dependability ed un secondo che tratta richiami di pro-

babilità e di teoria della misura. La seconda parte comprende capitoli per descrivere le tecniche ed i modelli combinatori, i modelli Markoviani, basati sullo spazio degli stati, ed uno per le Reti di Petri nelle loro estensioni stocastiche nonché per gli strumenti automatici per la definizione e soluzione di tali modelli. La terza parte infine tratta la analisi sperimentale ed è suddivisa in un capitolo che descrive le problematiche di osservazione e monitoraggio ed uno che tratta tecniche di ‘fault injection’ e di ‘robustness testing’. I capitoli che compongono questo libro sono:

### **Cap 1: ‘Introduzione’**

*di Andrea Bondavalli*

Il capitolo introduce le motivazioni che spingono allo studio degli aspetti quantitativi delle caratteristiche dei sistemi ed infrastrutture critici, e descrive i concetti fondamentali della dependability intesa come la proprietà di un sistema di fornire un servizio su cui poter fare affidamento.

### **Cap 2: ‘Richiami di Probabilità e Metrologia’**

*di Paolo Lollini, Andrea Ceccarelli e Michele Vadursi*

Il capitolo introduce i richiami di teoria delle probabilità ed i concetti fondamentali di teoria delle misure necessari per la comprensione dei fondamenti e delle tecniche per la valutazione – analitica e sperimentale – presentati nel libro.

### **Cap 3: ‘Metodi Combinatori’**

*di Andrea Bondavalli e Leonardo Montecchi*

Questo capitolo illustra una panoramica sui modelli di tipo combinatorio per l’analisi di dependability ed introduce i formalismi grafici a supporto di tali metodi: reliability block diagrams, reliability graphs e fault trees.

### **Cap 4: ‘Catene di Markov: fondamenti’**

*di Paolo Lollini*

Il capitolo introduce i processi stocastici di tipo Markoviano ed in particolare le catene di Markov a tempo discreto e continuo. Descrive poi sia la struttura del processo e come studiare sia il comportamento transiente che quello stazionario.

### **Cap 5: ‘Reti di Petri ed Estensioni’**

*di Silvano Chiaradonna*

Questo capitolo introduce il formalismo delle Reti di Petri (reti P/T) e alcune delle sue estensioni stocastiche quali SPN, GSPN, SAN. Illustra poi come analizzarne il comportamento e gli strumenti Möbius e DEEM per la specifica e la analisi.

**Cap 6: ‘Monitoring di Sistemi’**

*di Andrea Bondavalli, Francesco Brancati e Andrea Ceccarelli*

Il capitolo descrive i fondamenti, la struttura di un sistema di monitoraggio, le problematiche che si incontrano e le principali categorie di sistemi per cui si fa monitoraggio. Il capitolo descrive poi un caso di studio legato alla osservazione del comportamento di un orologio software.

**Cap 7 ‘Fault Injection e Robustness Testing’**

*di Domenico Cotroneo e Roberto Natella*

Questo ultimo capitolo introduce i concetti di base della Fault Injection, le principali applicazioni e le metodologie utilizzate per iniettare guasti. Il capitolo prosegue con una trattazione di Robustness Testing descrivendo una metodologia generale e due applicazioni al testing di Sistemi Operativi e Web Services.



# Indice

<b>Ringraziamenti</b>	<b>xiii</b>
-----------------------	-------------

<b>I INTRODUZIONE E RICHIAMI</b>	<b>1</b>
----------------------------------	----------

<b>1 Introduzione</b>	<b>3</b>
-----------------------	----------

1.1 La dependability . . . . .	4
1.1.1 Le Minacce: guasti, errori e fallimenti . . . . .	5
1.1.2 Gli attributi della dependability . . . . .	7
1.1.3 I mezzi per ottenere la dependability . . . . .	9

<b>2 Richiami di Probabilità e Metrologia</b>	<b>13</b>
---	-----------

2.1 Richiami di Probabilità . . . . .	13
2.1.1 Algebra degli eventi . . . . .	14
2.1.2 Probabilità, Probabilità Condizionale ed Indipendenza di Eventi . . . . .	16
2.1.3 Reliability per Sistemi in Serie e in Parallelo . . . . .	17
2.1.4 Teorema delle probabilità totali e Formula di Bayes . . . . .	19
2.1.5 Prove di Bernoulli . . . . .	20
2.1.6 Variabili Casuali Discrete . . . . .	21
2.1.7 Esempi di distribuzioni discrete . . . . .	23
2.1.8 Variabili Casuali Continue . . . . .	31
2.1.9 La distribuzione Esponenziale . . . . .	32
2.1.10 Minimo di due esponenziali indipendenti . . . . .	34
2.1.11 Competizione tra due esponenziali indipendenti . . . . .	35
2.1.12 Reliability, Failure Rate, Cumulative Failure Rate e Con- ditional Reliability . . . . .	36
2.1.13 Esempi di distribuzioni continue . . . . .	38
2.1.14 Expectation . . . . .	44
2.2 Richiami di Metrologia . . . . .	46
2.2.1 Fondamenti di teoria della misurazione . . . . .	47

2.2.2	Caratteristiche di una misurazione . . . . .	48
2.2.3	Incertezza di misura . . . . .	49
2.2.4	Compatibilità dei risultati . . . . .	54
2.2.5	Indicazioni conclusive e approfondimenti . . . . .	54

## II MODELLI 57

### 3 Metodi Combinatori 59

3.1	Introduzione . . . . .	59
3.2	Modelli combinatori . . . . .	59
3.2.1	Componenti in Serie e in Parallelo . . . . .	61
3.2.2	Caso generico: $k$ su $n$ . . . . .	62
3.3	Metodi booleani . . . . .	63
3.3.1	Approcci di base per la valutazione . . . . .	64
3.3.2	Teorema di espansione di Shannon . . . . .	66
3.4	Formalismi grafici . . . . .	71
3.4.1	Reliability Block Diagrams . . . . .	72
3.4.2	Reliability Graphs . . . . .	74
3.4.3	Fault Trees . . . . .	76
3.5	Fault Tree Analysis (FTA) . . . . .	77
3.5.1	Elementi di un fault tree . . . . .	78
3.5.2	Costruzione del fault tree . . . . .	81
3.5.3	Generazione dei Minimal Cut Set . . . . .	81
3.5.4	Analisi quantitativa di un fault tree . . . . .	83
3.6	Caso di studio . . . . .	85
3.6.1	Descrizione del sistema . . . . .	85
3.6.2	Fault Tree del sistema . . . . .	86
3.6.3	RBD e RG del sistema . . . . .	88
3.6.4	Analisi quantitativa del sistema . . . . .	89

### 4 Catene di Markov: fondamentali 93

4.1	Introduzione ai Processi Stocastici e di Markov . . . . .	93
4.2	Catene di Markov a tempo discreto . . . . .	95
4.2.1	Vettore di probabilità di occupazione degli stati e Matrice di probabilità di transizione . . . . .	96
4.2.2	Tempo di permanenza in uno stato . . . . .	97
4.3	Comportamento transiente . . . . .	97
4.3.1	Esempio: andamento titolo . . . . .	99
4.3.2	Grafo associato alla catena . . . . .	100
4.4	Classificazione degli stati . . . . .	100

4.4.1	Stati accessibili, comunicanti ed assorbenti . . . . .	100
4.4.2	Stati transitori, ricorrenti, ricorrenti positivi e ricorrenti nulli . . . . .	101
4.4.3	Stati periodici e aperiodici . . . . .	104
4.5	Comportamento a regime . . . . .	104
4.5.1	Esempio: andamento titolo (continua) . . . . .	106
4.5.2	Analisi di catene con stati assorbenti . . . . .	107
4.5.3	Esempio: la camminata aleatoria con barriera riflettente . . . . .	109
4.6	Catene di Markov a tempo continuo . . . . .	112
4.7	Comportamento transiente . . . . .	112
4.7.1	Grafo associato alla catena . . . . .	114
4.8	Uniformizzazione di catene di Markov . . . . .	114
4.9	Stati assorbenti, istantanei, stabili . . . . .	115
4.9.1	Esempio . . . . .	116
4.10	Calcolo del MTTF in catene con stati assorbenti . . . . .	116
4.10.1	Esempio . . . . .	117
4.11	Stati accessibili, ricorrenti e transitori . . . . .	118
4.12	Comportamento a regime . . . . .	119
4.13	Metodi per il calcolo di $\pi$ . . . . .	121
4.13.1	Metodi diretti . . . . .	121
4.13.2	Metodi iterativi stazionari . . . . .	121
4.14	Esempio: sistema con tre server in parallelo . . . . .	123
<b>5</b>	<b>Reti di Petri ed Estensioni</b>	<b>127</b>
5.1	Introduzione . . . . .	127
5.2	Caratteristiche dei formalismi di modellazione . . . . .	128
5.3	Reti di Petri di tipo Place/Transition . . . . .	129
5.3.1	Definizione . . . . .	129
5.3.2	Firing di una transizione . . . . .	132
5.3.3	Proprietà e comportamento . . . . .	133
5.3.4	Potenza di modellazione . . . . .	136
5.4	Reti di Petri con priorità . . . . .	138
5.5	Analisi delle reti di Petri . . . . .	142
5.6	Transizioni temporizzate . . . . .	145
5.7	Stochastic Petri Nets . . . . .	147
5.7.1	Definizione . . . . .	147
5.7.2	Conflitto . . . . .	149
5.7.3	Concorrenza . . . . .	151
5.7.4	Tasso di transizione dipendente dalla marcatura . . . . .	153
5.7.5	SPN e processo stocastico sottostante . . . . .	155
5.8	Misure di interesse . . . . .	156

5.8.1	Performance, dependability e performability . . . . .	156
5.8.2	Variabili di performance e struttura di guadagno . . . . .	157
5.8.3	Definizione delle variabili di performance . . . . .	159
5.8.4	Esempio di variabile di performance . . . . .	161
5.9	Generalized Stochastic Petri Nets . . . . .	162
5.9.1	Definizione . . . . .	162
5.9.2	Conflitto . . . . .	164
5.9.3	GSPN e processo stocastico sottostante . . . . .	166
5.9.4	Estensioni . . . . .	171
5.10	SAN . . . . .	172
5.10.1	Definizione . . . . .	172
5.10.2	Cambiamento di marcatura . . . . .	176
5.10.3	SAN stabilizzanti e ben specificate . . . . .	177
5.10.4	SAN e processo stocastico sottostante . . . . .	180
5.11	Möbius . . . . .	183
5.11.1	Caratteristiche Principali di Möbius . . . . .	183
5.11.2	Il framework di Möbius . . . . .	185
5.12	DEEM . . . . .	186
5.12.1	Sistemi a Fasi Multiple . . . . .	186
5.12.2	Caratteristiche Principali di DEEM . . . . .	187

### III METODI SPERIMENTALI

199

<b>6</b>	<b>Monitoring di sistemi</b>	<b>201</b>
6.1	Fondamenti del monitoring di sistemi . . . . .	201
6.2	Problematiche nel monitoring di sistemi . . . . .	205
6.3	Gestione dei Dati . . . . .	208
6.3.1	La Metodologia di Analisi OLAP . . . . .	208
6.3.2	Struttura di un repository OLAP . . . . .	209
6.3.3	OLAP per il monitoring . . . . .	211
6.4	Principali categorie per il monitoring di sistemi . . . . .	212
6.4.1	Automatic Failure Reporting per Componenti Software . . . . .	212
6.4.2	Sistemi di Intrusion Detection ed Intrusion Prevention . . . . .	214
6.4.3	Network Monitoring e QoS Monitoring . . . . .	215
6.4.4	Telemetria di Sistemi Embedded . . . . .	217
6.4.5	Monitoring di Large-Scale Enterprise Software . . . . .	218
6.4.6	RunTime Verification . . . . .	219
6.5	Un caso di studio: Monitoriamo un Clock software . . . . .	220
6.5.1	Il Reliable and Self-Aware Clock . . . . .	220
6.5.2	Pianificazione dell'attività monitoraggio . . . . .	221



6.5.3	Instrumentazione del codice . . . . .	225
6.5.4	Definizione della struttura del repository . . . . .	227
6.5.5	Parsing dei file di log . . . . .	228
6.5.6	Analisi OLAP . . . . .	229
<b>7</b>	<b>Fault Injection e Robustness Testing</b>	<b>233</b>
7.1	Introduzione . . . . .	233
7.2	Fault Injection: Concetti di base . . . . .	234
7.2.1	Definizioni . . . . .	234
7.2.2	Obiettivi . . . . .	237
7.2.3	Modelli di guasto e tecniche di iniezione . . . . .	239
7.3	Applicazioni della Fault Injection . . . . .	242
7.3.1	Interazione con metodi modellistici . . . . .	242
7.3.2	Analisi dei modi di fallimento e valutazione del rischio . . . . .	244
7.3.3	Selezione di componenti e Dependability Benchmarking . . . . .	246
7.4	Metodologie di Fault Injection . . . . .	248
7.4.1	Una metodologia per l'iniezione di guasti hardware . . . . .	248
7.4.2	Una metodologia per l'iniezione di guasti software . . . . .	254
7.5	Robustness Testing . . . . .	260
7.5.1	Approccio generale . . . . .	260
7.5.2	Robustness Testing di sistemi operativi . . . . .	264
7.5.3	Robustness Testing di web services . . . . .	266
	<b>Bibliografia</b>	<b>271</b>