**Winter Workshop (3 Credit Cont. Ed.) Program on**

**Cyber-Risk Informatics by UNTREF on Aug. 9-12, 2016**

**(See Appendix for Chapters)**

**(Highly suggested: Workshop attendees acquire the book\* to follow from if possible)**

Aug.9, 2016 →

*Day 1*: Tuesday (8:45-12:30); Chap. 4 (supported by Chap. 5 and 10); 8:45 to 10:00, 10:15 to 11:30, 11:40 to 12:30.

Aug. 10, 2016 →

*Day 2*: Wednesday (8:45-12:30); Chap. 6 (supported by Chap. 1 & 2); 8:45 to 10:00, 10:15 to 11:30, 11:40 to 12:30.

Aug.11, 2016 →

*Day 3*: Thursday (8:45-12:30); Chap. 7 (supported by Chap. 1 & 6); 8:45 to 10:00, 10:15 to 11:30, 11:40 to 12:30.

Aug. 12, 2016 →

*Day 4*: Friday (8:45-12:30); Chap. 3 on Reliability & Security Testing and Chap. 8 on SW Reliability;

8:45 to 10:00, 10:15 to 11:30, 11:40 to 12:30.

Closure & Certifications by the Comp. Eng. Dept. and the Higher Admin. Office of UNTREF Rectorate; 12:30 to 13:00.

\*APPENDIX ↓

**Cyber-Risk Informatics**

***E****ngineering* ***E****valuation* ***w****ith* ***D****ata* ***S****cience*

**Mehmet Sahinoglu, Ph.D**

*Auburn University at Montgomery*



El carácter múltiple de la seguridad de la red nos recuerda de la antigua fábula “Los Ciegos y el Elefante”, donde los ciegos (o investigadores de riesgo de seguridad de hoy) están tocando el elefante (o seguridad de la red) para entender que es—porque jamás han encontrado a un elefante. Cada uno toca una parte diferente, tal como el lado, tronco, o pierna. En las notas que comparan, se enteran de que están en desacuerdo; uno piensa que el tronco es una culebra y el otro que la pierna es un árbol.

Esta conferencia proporciona un remedio oportuno a esa metáfora simbólica, ofreciendo un enfoque holístico (teórico) y práctico (aplicado) bien fundamentado. Esos hombres ciegos ya no serán sin conocimiento del elefante! El mensaje universal aquí, no es buscar la seguridad total (un conocimiento perfecto del elefante, algo que nunca sucederá para los ciegos), si no manejar la inseguridad (conociendo a el elefante de la mejor manera que los ciegos pueden), que es de lo que este libro esclarecedor titulado “Informáticas de Riesgo Cibernéticos”, se trata.

**Contents**

**Prologue xv**

**Reviews xvii**

**Preface xxiii**

**Acknowledgments and Dedication xxxi**

**About the Author xxxiii**

**1 Metrics, Statistical Quality Control, and Basic Reliability in Cyber‐Risk 1**

1.1 Deterministic and Stochastic Cyber‐Risk Metrics 1

1.2 Statistical Risk Analysis 2

1.2.1 Introduction to Statistical Hypotheses 2

1.2.2 Decision Rules 3

1.2.3 One‐Tailed Tests 4

1.2.4 Two‐Tailed Tests 4

1.2.5 Decision Errors 6

1.2.6 Applications to One‐Tailed Tests Associated with Both

Type I and Type II Errors 7

1.2.7 Applications to Two‐Tailed Tests (Normal Distribution

Assumption) 11

1.3 Acceptance Sampling in Quality Control 16

1.3.1 Introduction 16

1.3.2 Definition of an Acceptance Sampling Plan 16

1.3.3 The OC Curve 16

1.4 Poisson and Normal Approximation to Binomial in Quality Control 19

1.4.1 Approximations to Binomial Distribution 19

1.4.2 Approximation of Binomial to Poisson Distribution 19

1.4.3 Approximation to Normal Distribution 20

1.4.4 Comparisons of Normal and Poisson Approximations

to the Binomial 21

1.5 Basic Statistical Reliability Concepts and Mc Simulators 21

1.5.1 Fundamental Equations for Reliability, Hazard, and

Statistical Notions 23

1.5.2 Fundamentals for Reliability Block Diagramming and Redundancy 27

1.5.3 Solving Basic Reliability Questions by Using Student‐Friendly

Pedagogical Examples 30

1.5.4 MC Simulators for Commonly Used Distributions in Reliability 47

1.6 Discussions and Conclusion 52

1.7 Exercises 52

References 60

**2 Complex Network Reliability Evaluation and Estimation in Cyber‐Risk 61**

2.1 Introduction 61

2.2 Overlap Technique to Calculate Complex Network Reliability 62

2.2.1 Network State Enumeration and Example 1 63

2.2.2 Generating Minimal Paths and Example 2 64

2.2.3 Overlap Method Algorithmic Rules and Example 3 68

2.3 The Overlap Method: Monte Carlo and Discrete Event Simulation 70

2.4 Multistate System Reliability Evaluation 71

2.4.1 Simple Series System with Single Derated States 73

2.4.2 Active Parallel System 73

2.4.3 Simple Series–Parallel System 74

2.4.4 A Simple Series–Parallel System with Multistate Components 75

2.4.5 A Combined System: Power Plant Example 76

2.4.6 Large Network Examples Using Multistate Overlap Technique 77

2.5 Weibull Time Distributed Reliability Evaluation 78

2.5.1 Motivation behind Weibull Probability Modeling 78

2.5.2 Weibull Parameter Estimation Methodology 79

2.5.3 Overlap Algorithm Applied to Weibull Distributed Components 80

2.5.4 Estimating Weibull Parameters 80

2.5.5 Fifty‐Two‐Node Weibull Example for Estimating Weibull Parameters 85

2.5.6 A Weibull Network Example from an Oil Rig System 90

2.6 Discussions and Conclusion 90

Appendix 2.A Overlap Algorithm and Example 93

2.A.1 Algorithm 93

2.A.2 Example 95

2.7 Exercises 101

References 103

**3 Stopping Rules for Reliability and Security Tests in Cyber‐Risk 105**

3.1 Introduction 105

3.2 Methods 107

3.2.1 LGM by Verhulst 108

3.2.2 Compound Poisson Model 110

3.3 Examples Merging Both Stopping Rules: LGM and CPM 114

3.3.1 The DR5 Data Set Example 114

3.3.2 The Dr4 Data Set Example 118

3.3.3 The Supercomputing Cloud Historical Failure Data—Case Study 119

3.3.4 Appendix for Section 3.3 121

3.4 Stopping Rule for Testing in the Time Domain 131

3.4.1 Review of Compound Poisson Process and Stopping Rule 131

3.4.2 Empirical Bayes Analysis for the Poisson^Geometric

Stopping Rule 132

3.4.3 Howden’s Model for Stopping Rule 135

3.4.4 Computational Example for Stopping‐Rule Algorithm

in Time Domain 136

3.5 Discussions and Conclusion 139

Appendix 3.A Solutions to T4 Data Set MESAT‐2 Analysis 142

3.6 Exercises 142

References 143

**4 Security Assessment and Management in Cyber‐Risk 147**

4.1 Introduction 147

4.1.1 What Other Scoring Methods Are Available? 148

4.2 Security Meter (SM) Model Design 152

4.3 Verification of the Probabilistic Security Meter (SM) Method

by Monte Carlo Simulation and Math‐Statistical Triple‐Product Rule 154

4.3.1 The Triple‐Product Rule of Uniforms 156

4.3.2 Data Analysis on the Total Residual Risk of the Security

Meter Design 158

4.3.3 Triple‐Product Rule Discussions and Conclusion 169

4.4 Modifying the SM Quantitative Model for Categorical, Hybrid,

and Nondisjoint Data 170

4.5 Maintenance Priority Determination for 3 × 3 × 2 SM 178

4.6 Privacy Meter (PM): How to Quantify Privacy Breach 183

4.6.1 Methodology 184

4.6.2 Privacy Risk‐Meter Assessment and Management Examples 185

4.7 Polish Decoding (Decompression) Algorithm 187

4.8 Discussions and Conclusion 189

4.9 Exercises 190

References 199

**5 Game‐Theoretic Computing in Cyber‐Risk 201**

5.1 Historical Perspective to Game Theory’s Origins 201

5.2 Applications of Game Theory to Cyber‐Security Risk 203

5.3 Intuitive Background: Concepts, Definitions, and Nomenclature 204

5.3.1 A Price War Example 205

5.4 Random Selection for Nash Mixed Strategy 208

5.4.1 Random Probabilistic Selection 208

5.4.2 Does Nash Equilibrium (NE) Exist for the Company A/B

Problem in Table 5.1? 209

5.4.3 An Example: Matching Pennies 210

5.4.4 Another Game: The Prisoner’s Dilemma 210

5.4.5 Games with Multiple NE (Terrorist Game: Bold Strategy Result

in Domination) 211

5.5 Adversarial Risk Analysis Models by Banks, Rios, and Rios 213

5.6 An Alternative Model: Sahinoglu’s Security Meter

for Neumann and Nash Mixed Strategy 215

5.7 Other Interdisciplinary Applications of Risk Meters 220

5.8 Mixed Strategy for Risk Assessment and Management‐University

Server and Social Network Examples 221

5.8.1 University Server’s Security Risk‐Meter Example 221

5.8.2 Social Networks’ Privacy and Security Risk‐Meter (RM) Example 222

5.8.3 Clarification of Risk Assessment and Management Algorithm

for Social Networks 224

5.9 Application to Hospital Healthcare Service Risk 226

5.10 Application to Environmetrics and Ecology Risk 229

5.11 Application to Digital Forensics Security Risk 234

5.12 Application to Business Contracting Risk 239

5.13 Application to National Cybersecurity Risk 245

5.14 Application to Airport Service Quality Risk 253

5.15 Application to Offshore Oil‐Drilling Spill and Security Risk 257

5.16 Discussions and Conclusion 264

5.17 Exercises 266

References 271

**6 Modeling and Simulation in Cyber‐Risk 277**

6.1 Introduction and a Brief History to Simulation 277

6.2 Generic Theory: Case Studies on Goodness of Fit for Uniform Numbers 278

6.3 Why Crucial to Manufacturing and Cyber Defense 279

6.4 A Cross Section of Modeling and Simulation in Manufacturing Industry 280

6.4.1 Modeling and Simulation of Multistate Production Units

and Systems in Manufacturing 281

6.4.2 Two‐State SL Probability Model of Units with Closed‐Form

Solution 283

6.4.3 Extended Three‐State SL Probability Model

of Up–Down –Derated Units with MC Simulation 284

6.4.4 Statistical Simulation of Three‐State Units to Estimate the Density

of Up–Down –Der 289

6.4.5 How to Generate Random Numbers from SL pdf to Simulate

Component and System Behavior 296

6.4.6 Example of SL Simulation for Modeling Network

of 2‐in‐Simple‐Series Two‐State (Up–Dn) Units 297

6.4.7 Example of SL Simulation for Modeling a Network

of 7‐in‐Complex‐Topology Two‐State (Up–Dn) Units 300

6.5 A Review of Modeling and Simulation in Cyber‐Security 301

6.5.1 MC Value‐at‐Risk Approach by Kim et al. in Cloud Computing 301

6.5.2 MC and DES in Security Meter (SM) Risk Model 302

6.6 Application of Queuing Theory and Multichannel Simulation

to Cyber‐Security 306

6.6.1 Example 1: One Recovery‐Crew Case for Cyber‐Security

Queuing Simulation 306

6.6.2 Example 2: Two Recovery‐Crew Case for Cyber‐Security

Queuing Simulation 308

6.7 Discussions and Conclusion 308

Appendix 6.A 311

6.8 Exercises 315

References 335

**7 Cloud Computing in Cyber‐Risk 339**

7.1 Introduction and Motivation 339

7.2 Cloud Computing Risk Assessment 342

7.3 Motivation and Methodology 343

7.3.1 History of Theoretical Developments on CLOUD Modeling 343

7.3.2 Notation 344

7.3.3 Objectives 344

7.3.4 Frequency and Duration Method for the Loss of Load or Service 345

7.3.5 NBD as a Compound Poisson Model 346

7.3.6 NBD for the Loss of Load or Loss of Cloud Service Expected 348

7.4 Various Applications to Cyber Systems 349

7.4.1 Small Sample Experimental Systems 349

7.4.2 Large Cyber Systems 353

7.5 Large Cyber Systems Using Statistical Methods 357

7.6 Repair Crew and Product Reserve Planning to Manage Risk

Cost Effectively Using CyberRiskSolver Cloud Management Java Tool 359

7.6.1 Cloud Resource Management Planning for Employment of Repair Crews 360

7.6.2 Cloud Resource Management Planning by Production Deployment 365

7.7 Remarks for “Physical Cloud” Employing Physical Products

(Servers, Generators, Communication Towers, Etc.) 368

7.8 Applications to “Social (Human Resources) Cloud” 372

7.8.1 Numerical Example for Social Cloud (200 Employees Performing) 376

7.8.2 Input Wizard Example for Social Cloud (200 Employees Performing) 379

7.9 Stochastic Cloud System Simulation 379

7.9.1 Introduction and Methodology 381

7.9.2 Numerical Applications for SS to Verify Non‐SS 385

7.9.3 Details of Probability Distributions Used in Stochastic Simulation 387

7.9.4 Varying Product Repair and Failure Date with Empirical

Bayesian Posterior Gamma Approach 393

7.9.5 Varying Link Repair and Failure Using Gamma Distribution 393

7.9.6 SS Applied to a Power or Cyber Grid 394

7.9.7 Error Checking or Flagging 396

7.10 Cloud Risk Meter Analysis 397

7.10.1 Risk Assessment and Management Clarifications for Figures 7.72 and 7.73 402

7.11 Discussions and Conclusion 405

7.12 Exercises 407

References 416

**8 Software Reliability Modeling and Metrics in Cyber‐Risk 421**

8.1 Introduction, Motivation, and Methodology 421

8.2 History and Classification of Software Reliability Models 422

8.2.1 Time‐between‐Failures Models 422

8.2.2 Failure‐Counting Models 422

8.2.3 Bayesian Model 423

8.2.4 Static (Nondynamic) Models 423

8.2.5 Others 424

8.3 Software Reliability Models in Time Domain 424

8.4 Software Reliability Growth Models 425

8.4.1 Negative Exponential Class of Failure Times 425

8.4.2 J–M De‐eutrophication Model (Binomial Type) 425

8.4.3 Moranda’s Geometric Model (Poisson Type) 426

8.4.4 Goel–Okumoto Nonhomogeneous Poisson Process (Poisson Type) 427

8.4.5 Musa’s Basic Execution Time Model (Poisson Type) 428

8.4.6 Musa–Okumoto Logarithmic Poisson Execution Time Model (Poisson Type) 429

8.4.7 L–V Bayesian Model 431

8.4.8 Sahinoglu’s Compound Poisson^Geometric and Poisson^Logarithmic Series Models 433

8.4.9 Gamma, Weibull, and Other Classes of Failure Times 435

8.4.10 Duane Model (Poisson Type) 439

8.5 Numerical Examples Using Pedagogues 440

8.5.1 Example 1 440

8.5.2 Example 2 441

8.6 Recent Trends in Software Reliability 441

8.7 Discussions and Conclusion 442

8.8 Exercises 444

References 445

**9 Metrics for Software Reliability Failure‐Count Models in Cyber‐Risk 451**

9.1 Introduction and Methodology on Failure‐Count Estimation

in Software Reliability 451

9.1.1 Statistical Estimation Models, Computational Formulas, and Examples 452

9.1.2 Interpretations of Numerical Examples and Discussions 464

9.2 Predictive Accuracy to Compare Failure‐Count Models 466

9.2.1 Classical Distribution Approach 468

9.2.2 Prior Distribution Approach 469

9.2.3 Applications to Data Sets and Comparisons 472

9.3 Discussions and Conclusion 473

Appendix 9.A 477

9.4 Exercises 478

References 482

**10 Practical Hands‐On Lab Topics in Cyber‐Risk 483**

10.1 System Hardening 483

10.1.1 General 483

10.1.2 Windows Servers 484

10.1.3 Wireless 484

10.1.4 Firewalls, Routers, and Switches 485

10.2 Email Security 486

10.2.1 Identifying Fake Emails 486

10.2.2 Emotion Responses 486

10.3 MS‐DOS Commands 487

10.3.1 Mapping Intel 488

10.4 Logging 492

10.4.1 Policy 493

10.4.2 Understanding Logs 494

10.5 Firewall 495

10.5.1 Traditional Firewalls 495

10.5.2 NGFs 496

10.5.3 Host‐Based Firewalls 496

10.6 Wireless Networks 496

10.7 Discussions and Conclusion 499

Appendix 10.A 500

10.8 Exercises 501

10.8.1 System Hardening 501

10.8.2 Email 501

10.8.3 MS‐DOS 502

10.8.4 Logging 503

10.8.5 Firewall 503

10.8.6 Wireless 505

10.8.7 Comprehensive Exercises 505

10.8.8 Cryptology Projects 507

References 509

**What the Cyber‐Risk Informatics Textbook and the Author are About? 511**

**Index 513**