



# ROBUST CONTROL SYSTEM NETWORKS

HOW TO ACHIEVE RELIABLE  
CONTROL AFTER STUXNET

RALPH LANGNER



MOMENTUM PRESS

# Contents

<b>Preface</b>	<b>ix</b>
<b>About the Author</b>	<b>xiii</b>
<b>Chapter 1 Introduction: The Three Faces of Risk</b>	<b>1</b>
1.1 The Insurance Model of Risk: Risk as Statistical Probability and Projected Amount of Loss	1
1.2 The Logical Model of Risk: Risk as Cause and Consequence	3
1.3 The Financial Model of Risk: Risk as Volatility	5
1.4 From Risk to Fragility and from Security to Robustness	7
<b>Chapter 2 The Problem of Cyber Fragility in Industrial Automation and Control</b>	<b>9</b>
2.1 Cyber Fragility Defined	10
2.2 The Evolution of Complexity in Industrial Automation and Control	15
2.3 Entropy and IACS Networks	16
2.4 Cyber Contingency	20
2.5 Fragile Control	28
2.6 Control Clouds	31
<b>Chapter 3 Cyber Robustness</b>	<b>39</b>
3.1 Cyber Robustness Defined	39
3.2 Robustification Theory: Principles	43
3.3 Robustification Practice: Strategies	48
3.4 How to Approach Robustification Projects	50
3.5 Recommended Robustification Procedure	53

<b>Chapter 4 Building a System Model</b>	<b>59</b>
4.1 System Model Aspects and Criteria	60
4.2 Building a Structural System Model	61
4.3 Hardware Inventory	72
4.4 Software Inventory	74
4.5 Network Configuration	75
4.6 People, Policy, Procedures	76
4.7 Monitoring and Auditing	80
<b>Chapter 5 Requirements and System Specification</b>	<b>83</b>
5.1 The Role of Requirements for Robustification	84
5.2 Specification Items	85
5.3 The Specification Tree	86
5.4 Specifying Cyber Operating Conditions	87
<b>Chapter 6 Imposing Structure</b>	<b>89</b>
6.1 Removing Unnecessary Applications, Services, and Functions (System Hardening)	91
6.2 Reducing or Removing General-Purpose Software Services and Interfaces	95
6.3 Using Application-Specific Least-Functionality Interfaces	98
6.4 Reducing Static Open File Exchanges (Shared Folders)	101
6.5 Eliminating Hidden Hubs	103
6.6 Restricting User Access and User Interaction	105
6.7 Reducing Variation in Procedure (Standard Operating Procedures)	108
6.8 Reducing Network Exposure	112
6.9 Reducing Variation in Equipment Type, Product Version, and Configuration Options	115
<b>Chapter 7 Enforcing and Reinforcing Structure</b>	<b>119</b>
7.1 Resilient Code and Architecture	120
7.2 Code Execution and Configuration Tamper Control/Monitoring	124
7.3 Encoding and Verifying Meta Information for End-to-End Validity Checking	128
7.4 Context-Based Restrictions on Control Authority (Inherent Safety)	131
7.5 Safeguards and Process Monitoring	133
7.6 Redundancy	136
7.7 Derating (Performance Reserves)	140

<b>Chapter 8</b>	<b>Modifying Structure</b>	<b>145</b>
8.1	The Need for Adaptability in IACS Environments	146
8.2	Change Factors	147
8.3	Change Management Quality Levels	151
<b>Epilogue</b>		<b>155</b>
<b>Appendix</b>		<b>157</b>
A	Surprise! Nonobvious, Nonanticipated Cyber Fragility Effects	157
B	Conservative Engineering Habits Resulting in Cyber Fragility	163
C	Cyber Robustness Versus IT Security	171
<b>References</b>		<b>187</b>
<b>List of Acronyms</b>		<b>189</b>
<b>Index</b>		<b>195</b>