HARNESSING THE POWER OF FAILURE: USING STORYTELLING AND SYSTEMS ENGINEERING TO ENHANCE ORGANIZATIONAL LEARNING

HARNESSING THE POWER OF FAILURE: USING STORYTELLING AND SYSTEMS ENGINEERING TO ENHANCE ORGANIZATIONAL LEARNING

BY

JOHN STEVEN NEWMAN
STEPHEN M. WANDER

United Kingdom – North America – Japan – India – Malaysia – China

Emerald Publishing Limited
Howard House, Wagon Lane, Bingley BD16 1WA, UK

First edition 2018

Copyright © 2018 Emerald Publishing Limited

Reprints and permission service
Contact: permissions@emeraldinsight.com

No part of this book may be reproduced, stored in a retrieval system, transmitted in any form or by any means electronic, mechanical, photocopying, recording or otherwise without either the prior written permission of the publisher or a licence permitting restricted copying issued in the UK by The Copyright Licensing Agency and in the USA by The Copyright Clearance Center. Any opinions expressed in the chapters are those of the authors. Whilst Emerald makes every effort to ensure the quality and accuracy of its content, Emerald makes no representation implied or otherwise, as to the chapters' suitability and application and disclaims any warranties, express or implied, to their use.

British Library Cataloguing in Publication Data
A catalogue record for this book is available from the British Library

ISBN: 978-1-78754-200-6 (Print)
ISBN: 978-1-78754-199-3 (Online)
ISBN: 978-1-78754-201-3 (Epub)

ISOQAR certified Management System, awarded to Emerald for adherence to Environmental standard ISO 14001:2004.

Certificate Number 1985
ISO 14001

INVESTOR IN PEOPLE

John Steven Newman

~

For my Mary, Scott, and Matt

Stephen M. Wander

~

To my beloved wife Sandy, “Until we meet again.”

And for my children, ShariLynn, TariLee, CJay

Contents

Acknowledgments *ix*

About the Authors *xi*

Prologue *xiii*

Part I Introduction and Overview *1*

Overarching Goals *2*
Layout and Flow *4*

Part II System Failure Case Studies *7*

Case Study Format *8*
Quick-Look Guide *9*
That Sinking Feeling *12*
Lewis Spins Out of Control *19*
Almost Perfect *27*
Two Rods Don't Make It Right *34*
Supercritical *40*
Submarine Down *47*
Fire in the Cockpit *52*
Derailed *59*
Powerless *65*
Fender Bender *72*
Innovation Pushed Too Far Too Fast *79*
No Left Turns *86*
Forrestal in Flames *93*
Tunnel of Terror *100*
Death on the Steppes *107*
Rocky Mountain Death Trap *113*
Refinery Ablaze – 15 Dead *120*
The Million Mile Rescue *125*

Part III Recurrent Themes – Integrated Analysis *133*
Introduction *133*
Enterprise/Business Management Framework *136*
Enterprise/Business Management: Observations *138*
Engineering Framework *141*
Engineering Framework: Observations *144*
Another Way of Looking at the Data *145*

Part IV Harnessing the Power… or Not *149*
Introduction *149*
Navy SSP – 'Always Had It and Kept It' *149*
Navy SUBSAFE – 'Learning from Early Failure' *152*
Petrobras – 'Had It and Gave It Away' *155*
WMATA Metro System – 'Lacked Initial Safety Culture but Recovering' *155*
Metro Renaissance – The Winds of Change *159*
Summary *161*

Part V Roadmap to Harnessing the Power *163*
Introduction *163*
Leadership that Leads *163*
Developing Enterprise Success Factors *166*
Understanding Enterprise Vulnerabilities *171*
People and Culture *176*
Control – Checks and Balances *181*
Embracing the Gift of Failure *188*

Part VI Applying the Power of Failure *191*
Introduction *191*
Organizations/Enterprises *192*
Academia *195*
Summary *199*

Epilogue *201*

Bibliography and References *203*

Acronym List *221*

Index *225*

Acknowledgments

The System Failure Case Study (SFCS) concept evolved from the notion of "hind casting," or learning from failure events - a method Dr. Newman encountered in class at George Washington University in the Fall of 1999 (Risk and Crisis Management). In early 2000, the first prototype system failure case studies were developed based on a series of Titan IV launch mishaps. While addressing other issues, including support to the Columbia Accident Investigation (2003), the authors together evolved the SFCS to incorporate an increasingly sharp systems engineering "lens." In the post-Columbia accident era, with an increased emphasis on knowledge management and lessons learned activities, the SFCS format underwent further evolution and development. The National Aeronautical and Space Administration (NASA), Review and Assessment Division (RAD) began developing and widely disseminating SFCSs in the 2005 time frame, employing NASA's first operational knowledge management system. We wish to salute our colleagues in the RAD and the Office of Safety and Mission Assurance (OSMA) who supported SFCS implementation, in particular, Mr. John Castellano, and Mr. Bryan O'Connor, NASA Chief Safety Officer. We would also like to recognize Bryan for his 'thought leadership' relevant to safety, mission assurance, and organizational accountability in high reliability organizations (HRO). In developing our roadmap to harnessing the power of failure we draw on HRO philosophy evolved from leaders in the aerospace community but also derived from the joint NASA/Navy Benchmarking Exchange (NNBE) (2000–2003). In particular, we acknowledge our Navy counterparts, Messers Al Ford, Jimmy Lawrence, and Storm Kauffman for their valuable insights related to safety and risk management within the Navy nuclear propulsion and SUBSAFE programs. Most recently, we have had the opportunity to gain deep insights into the Navy Strategic Systems Program high reliability assurance culture and focus on multilevel leadership and human element weakness. We thank Vice Admiral Terry Benedict and Mr. Steve Zavadil for their valued time and effort in meeting with us. Very special thanks is extended to Mr. Don Vecellio, a long-time and valued colleague, for his

encouragement and thought-provoking ideas and advice concerning the overall form and structure of the book, and to Mr. Coleman Cunningham for his insights and experience related to undergraduate general business and strategic management curriculum at the Fisher College of Business, The Ohio State University. The authors also wish to acknowledge Dr. Michael Stankosky for his support in encouraging us to move forward with this project and providing us navigational assistance along the challenging road to publication. Finally, the authors are deeply indebted to Ms. Charlotte Maiorana, Mr. Nick Wolterman, and S. Rajachitra of Emerald Publishing for their unwavering faith, guidance, and patience offered during the development and evolution of the themes, ideas, and production of this work.

About the Authors

J. Steven Newman, D.Sc. John Steven Newman had a distinguished 32 year career in government, with the National Aeronautics and Space Administration (NASA) and the Federal Aviation Administration (FAA). His experience base spans the Concorde Supersonic Transport, the Titan IV launch vehicle, the Space Shuttle, the International Space Station, and NASA Space Shuttle / Nuclear Submarine Benchmarking Exchange Program. Dr. Newman served in diverse leadership roles spanning project management, flight test, safety, quality, risk management, environmental management, accident and failure analysis. After retiring from NASA in 2006 Dr. Newman has served as an aerospace consultant, educator, and fine arts student. Dr. Newman holds a Bachelor of Science in Electrical Engineering, a Master of Science in Environmental Engineering from Northwestern University, and a Doctor of Science in Systems Engineering from The George Washington University.

Stephen M. Wander, B.M.E., M.E.A. Steve Wander has over 45 years of engineering management, research and development experience with the National Aeronautics and Space Administration (NASA), Energy Research and Development Administration (ERDA)/Department of Energy (DOE), and the United States Air Force. Since retirement from NASA Mr. Wander has served as a senior consultant in the fields of engineering management, risk management and systems engineering. Mr. Wander has also served as a Professorial Lecturer at George Washington University in the School of Engineering and Applied Sciences teaching graduate courses in engineering management, decision-making and problem-solving and undergraduate courses in probability, statistics, and statistical inference methods. Mr. Wander holds a Bachelor of Mechanical Engineering degree from The Ohio State University, and a Master of Engineering Administration degree from George Washington University.

Prologue

A quick navigational tip – The authors have attempted and intended that each part of this text stand on its own with respect to focus, structure, and informational content. Accordingly, it is not necessary nor required to read or review all the case studies presented in Part II before proceeding to other parts – 'analysis,' 'organizational examples,' 'system engineering tools and techniques,' or 'teaching models and methods.' It is, indeed, up to the needs and desires of the reader. So, feel free to pick and choose the cases of greatest interest – then move on through the rest of the book cycling-back at any point to explore additional cases.

Part I

Introduction and Overview

Failure informs. Failure informs as no analytical method can. Failure informs more generously and reliably than success. Failure is the best indicator of what's working and what's not in any system or enterprise. Certainly, it is never the intent to set out to fail, however, when failure events do occur, the opportunity will exist to learn something very important. Clearly, any failures that occur in a benign way with no injury, loss of life, or catastrophic damage are truly gifts. However, all failures will inevitably reveal latent defects and/or failure modes that are invariably buried within the people, processes, materials, design, manufacturing, and management that comprise and define any complex system. As will be described subsequently, the authors, whose combined 85+ years of experience in engineering, engineering management, systems engineering, system safety, and failure analysis, developed the system failure case study (SFCS) concept to entertain and inform and more importantly to assist individuals in developing a systems perspective in thinking about failure events. The intent is also to present this 'way of thinking' to a broad range of organizations and institutions (business, engineering, and academia) as an important element in evolving high reliability performance and failure avoidance.

"The Greatest Teacher, Failure Is"
Jedi Master Yoda

The SFCS concept blends systems thinking and systems engineering with storytelling. Our approach draws on two previous works (1) Charles Perrow's (1999), "Normal Accidents" that projects a certain fatalistic notion that failures are inevitable in complex, tightly coupled systems, and (2) James Reason's, "Managing the Risks of Organizational Accidents" that offers an optimistic belief that failures are understandable and preventable. The storytelling dimension is a very important and empowering aspect of our approach. Certainly, storytelling has been an essential element in the evolution of human kind. Long before the invention of the printing press, much less the Internet, storytelling was the only means of transferring important and critical information and

knowledge from one group to another, from one generation to the next and has thus been fundamentally engrained in human nature. Consequently, we have endeavored to make each case study a truly engaging story designed to enhance what we believe to be a very important and necessary learning experience.

Overarching Goals

Entertain

Failure events are thought-provoking, subtle and, in most cases, highly nuanced. Failure events are often tragic. Most failures are action thrillers. One instinctively looks for heroes and villains which may or may not exist. Nevertheless, the interaction of human nature and technological aspects of failures is often deeply interesting. Subsequent fact-finding and failure analysis can be a drama in and of itself. Results of investigations are often contested and subject to endless "spin." The legal and political finger-pointing can go on for years. Beyond these considerations, we have more serious goals that follow.

Understand the Lessons of Failure

As previously noted, and as many failure analysts have suggested, we invariably learn more from our failures than our successes. Thus, it is the stated purpose and objective of this text to present improved processes and techniques – based on detailed analysis of actual failures spanning a wide range of disciplines – that will expand our capability to better understand how failures often originate in system design and enhance our ability to learn from the failures that occur during operations.

Develop a Systems Perspective

A primary goal is to assist the reader in developing a systems perspective and if possible a systems safety and systems engineering way of thinking. Looking for interconnections, developing the "what-if?" mindset, embracing graphical tools and structured logic to think about how the elements in a system or system of systems may function or fail.

Recognize Danger

Our goals include illuminating recurrent themes and providing insight into the process of recognizing danger – vulnerability to potentially catastrophic failure events and the need to take early action to eliminate or mitigate their likelihood of occurrence.

Improve Decision Making

Failure events typically result from a chain of cascading conditions and/or actions (nonactions). Whether these are conditions that are uncontrollable (i.e., a weather event) or the direct result of active decisions (or both), action/nonaction is almost always the result of a deliberate decision or decision making process. In any event, decision making is deeply embedded in the causal web of most failure events. Thus, the study of recurrent themes in system failures will illuminate decision points that may seem mundane or inconsequential at the time but are ultimately critical decisions to the success of the enterprise.

Provide Action-based Response to Failure Events

This work develops the idea that decision makers, managers, technical process owners, politically appointed boards, need to assign emphasis, prominence, and priority, to understanding failure events, close-calls, near-misses, quality assurance issues, performance issues, and their underlying causes. Ideally, a better understanding of failures should lead to action – adjustment, re-design, re-training, change, process re-engineering, or corrective action.

Facilitate Organizational Development

Finally, a primary objective of this book is to provide a readily accessible and user-friendly data base, that is, "starter kit" for organizations to begin integrating the study and discussion of failure as an integral element in their organizational development – assessing the applicability of failure events to their own activities and operations. Employing failure case studies on a recurrent basis will clearly assist an organization in developing

and sustaining a safety culture. Associated benefits typically include enhanced organizational learning and team development as employees analyze and discuss each case.

Layout and Flow

Figure 1.1 provides a graphical snapshot of the content flow. A brief introduction to each part is provided in the following paragraphs. In Part II, *System Failure Case Studies,* the authors explore a broad array of failures in technologically/managerially complex systems and the inherent power of learning embedded in a focused and detailed analysis of those failures. Some events are well known, others more obscure – but each vignette serves to illuminate one or more key elements to harnessing the power of failure. There is always the question of how deep and how wide to examine the abundance of failure cases. We have chosen to cast a wide net considering failure events in multiple sectors of transportation, industry, aerospace, construction, and other critical infrastructure endeavors. Our case studies employ a format (discussed in detail in Part II) that has evolved and expanded from concepts we originally developed at NASA in the 2000–2003 time-frame.

In Part III, *Recurrent Themes – Integrated Analysis,* several frameworks for analysis are presented looking across the case study data presented in Part II seeking trends, patterns, and universally applicable insights. The reader is encouraged to translate the emergent failure modes to potential vulnerabilities within their own businesses, enterprises, and organizational activities. Part III also serves as a springboard for proactive failure

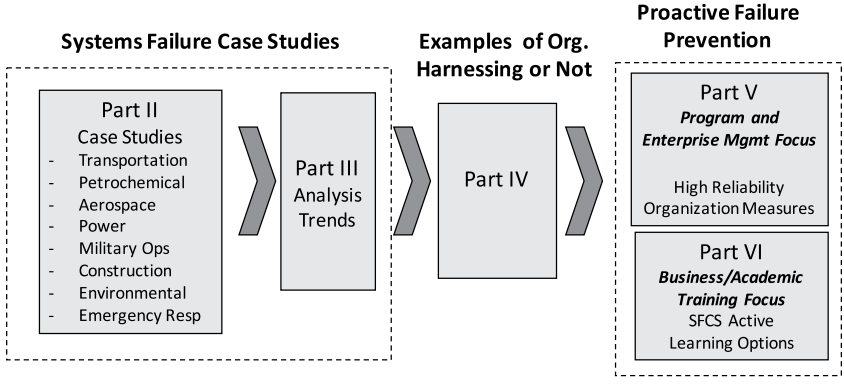

Fig. 1.1: Road Map to Harnessing the Power of Failure.

prevention measures the reader may consider and which are more fully developed and described in subsequent parts.

In Part IV, *Harnessing the Power … or Not*, provides examples of organizations that reflect a range of approaches, abilities, and willingness (or lack thereof) to prevent or learn from failures. As the reader will observe some organizations intensively study failures to establish sustainable safety and risk aware cultures. On the other hand, there are noted cases where organizations seem to never look back – much less forward – even as failures continue to plague their operations.

In Part V, *Road Map to Harnessing the Power*, presents a practical guide for organizations – in broadly diverse fields of endeavor – seeking to harden themselves against potential failure. The guide draws from the most simple, powerful, and highly transferable elements of systems engineering. The chapter presents methods – typically within the span of control of enterprise leaders, project managers, process owners, and operators – that will assist in identifying and understanding risks and potential ways to obviate failures within their activities.

Part VI, *Applying the Power of Failure*, provides detailed examples of SFCS-based learning activities. Tailored options are provided specifically for a business context and other options are presented for academic/classroom application. Commercial business training/teaching options range from a short (30 minutes) SFCS orientation and familiarization briefing to a half-day Knowledge Café (multiple case studies) and decision making seminars. On the academic side, generally applicable for both graduate- and undergraduate-level instructions, we offer a "blended learning" approach integrating video content with face-to-face interaction involving active student participation. In summary, the authors reflect on the importance of becoming students and critical observers of failure and the often-untapped reservoir of knowledge embedded in failure events.