Epilogue

In the simpler world of the past, classic safety engineering techniques that focus on preventing failures and chains of failure events were adequate. They no longer suffice for the types of systems we want to build, which are stretching the limits of complexity human minds and our current tools can handle. Society is also expecting more protection from those responsible for potentially dangerous systems.

Systems theory provides the foundation necessary to build the tools required to stretch our human limits on dealing with complexity. STAMP translates basic system theory ideas into the realm of safety and thus provides a foundation for our future.

As demonstrated in the previous chapter, some industries have been very successful in preventing accidents. The U.S. nuclear submarine program is not the only one. Others seem to believe that accidents are the price of progress or of profits, and they have been less successful. What seems to distinguish those experiencing success is that they:

- Take a systems approach to safety in both development and operations
- Have instituted a learning culture where they have effective learning from events
- Have established safety as a priority and understand that their long-term success depends on it

This book suggests a new approach to engineering for safety that changes the focus from "prevent failures" to "enforce behavioral safety constraints," from reliability to control. The approach is constructed on an extended model of accident causation that includes more than the traditional models, adding those factors that are increasingly causing accidents today. It allows us to deal with much more complex systems. What is surprising is that the techniques and tools described in part III that are built on STAMP and have been applied in practice on extremely complex systems have been easier to use and much more effective than the old ones.

Others will improve these first tools and techniques. What is critical is the overall philosophy of safety as a function of *control*. This philosophy is not new: It stems from the prescient engineers who created System Safety after World War II in the military aviation and ballistic missile defense systems. What they lacked, and what we have been hindered in our progress by not having, is a more powerful accident causality model that matches today's new technology and social drivers. STAMP provides that. Upon this foundation and using systems theory, new more powerful hazard analysis, design, specification, system engineering, accident/incident analysis, operations, and management techniques can be developed to engineer a safer world.

Mueller in 1968 described System Safety as "organized common sense" [109]. I hope that you have found that to be an accurate description of the contents of this book. In closing I remind you of the admonition by Bertrand Russell: "A life without adventure is likely to be unsatisfying, but a life in which adventure is allowed to take any form it will is sure to be short" [179, p. 21].