Overview of Digital System Safety and Cyber Security

Deirdre W. Spaulding-Yeoman, DSc.

October 20, 2011

U.S.NRC
United States Nuclear Regulatory Commission
Protecting People and the Environment

Purpose

- Overview on Regulatory Guide 1.152 regarding a Secure Development and Operational Environment (SDOE)
- Overview of digital system safety and cyber security licensing and oversight

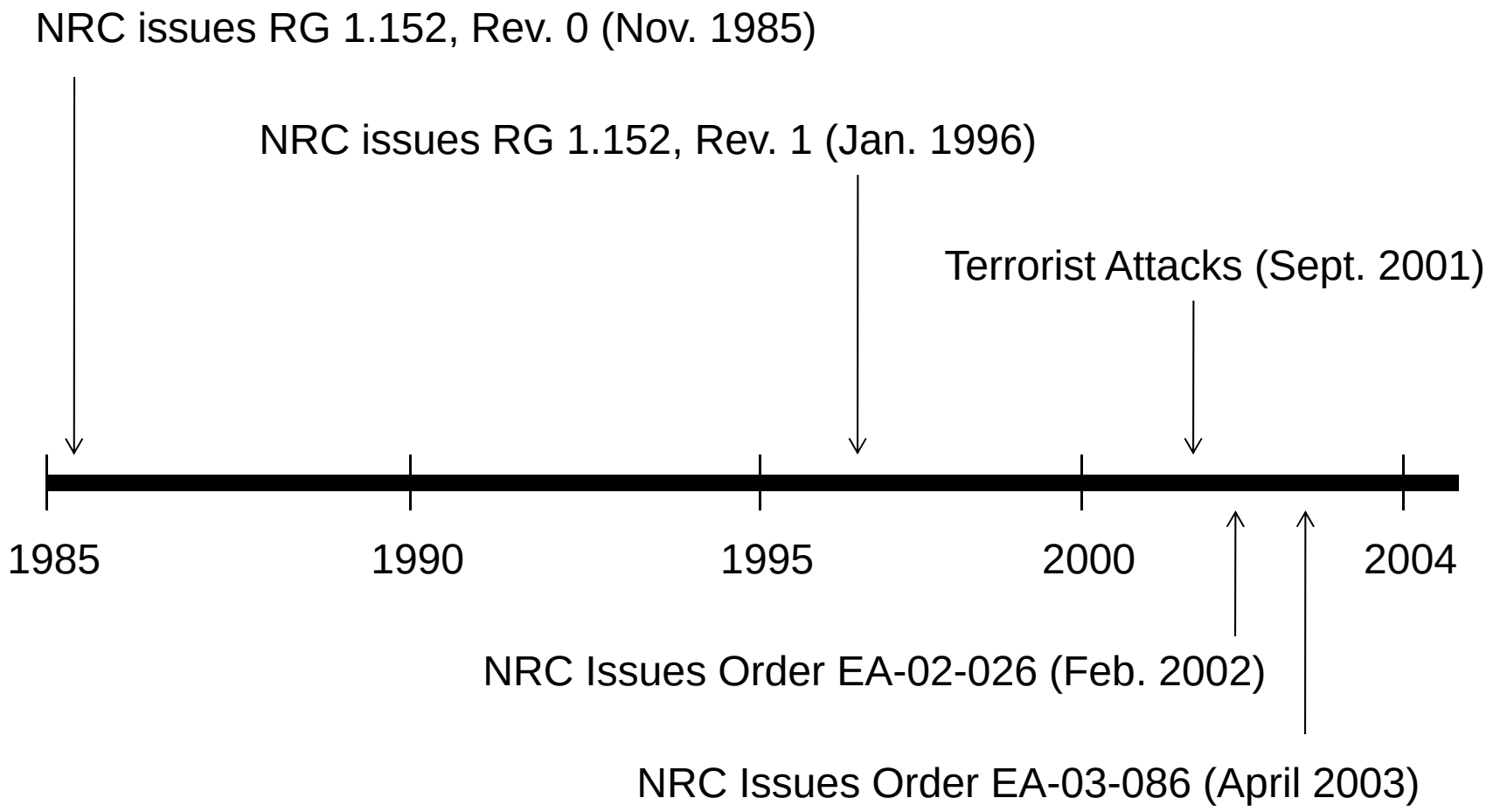
U.S.NRC
United States Nuclear Regulatory Commission
Protecting People and the Environment

Topics

- History of digital system safety and cyber security
- Overview of the current cyber security program and digital system safety review
- Regulatory Guide 1.152
- Regulatory developments regarding cyber security

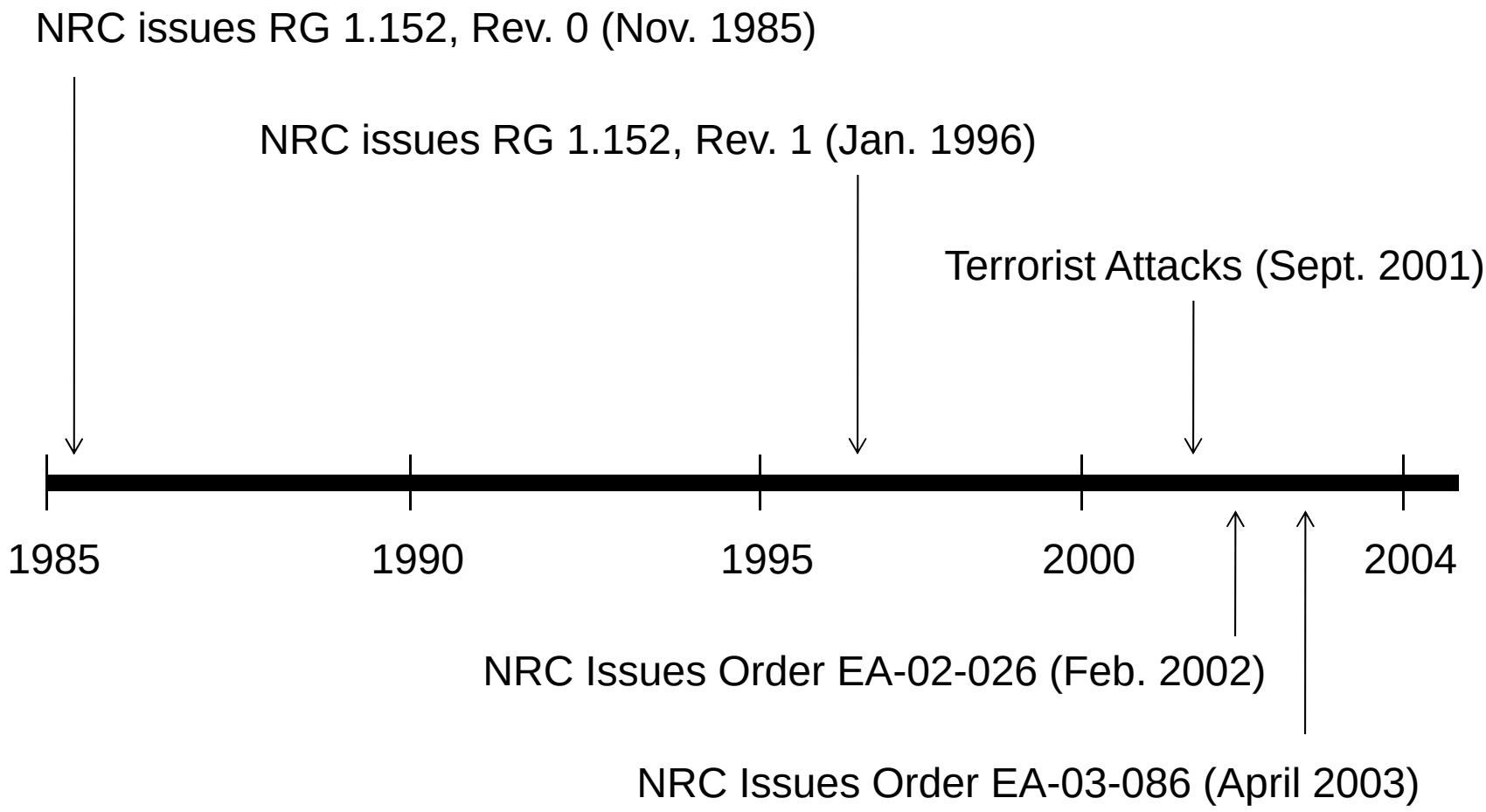
U.S.NRC
United States Nuclear Regulatory Commission
Protecting People and the Environment

Timeline



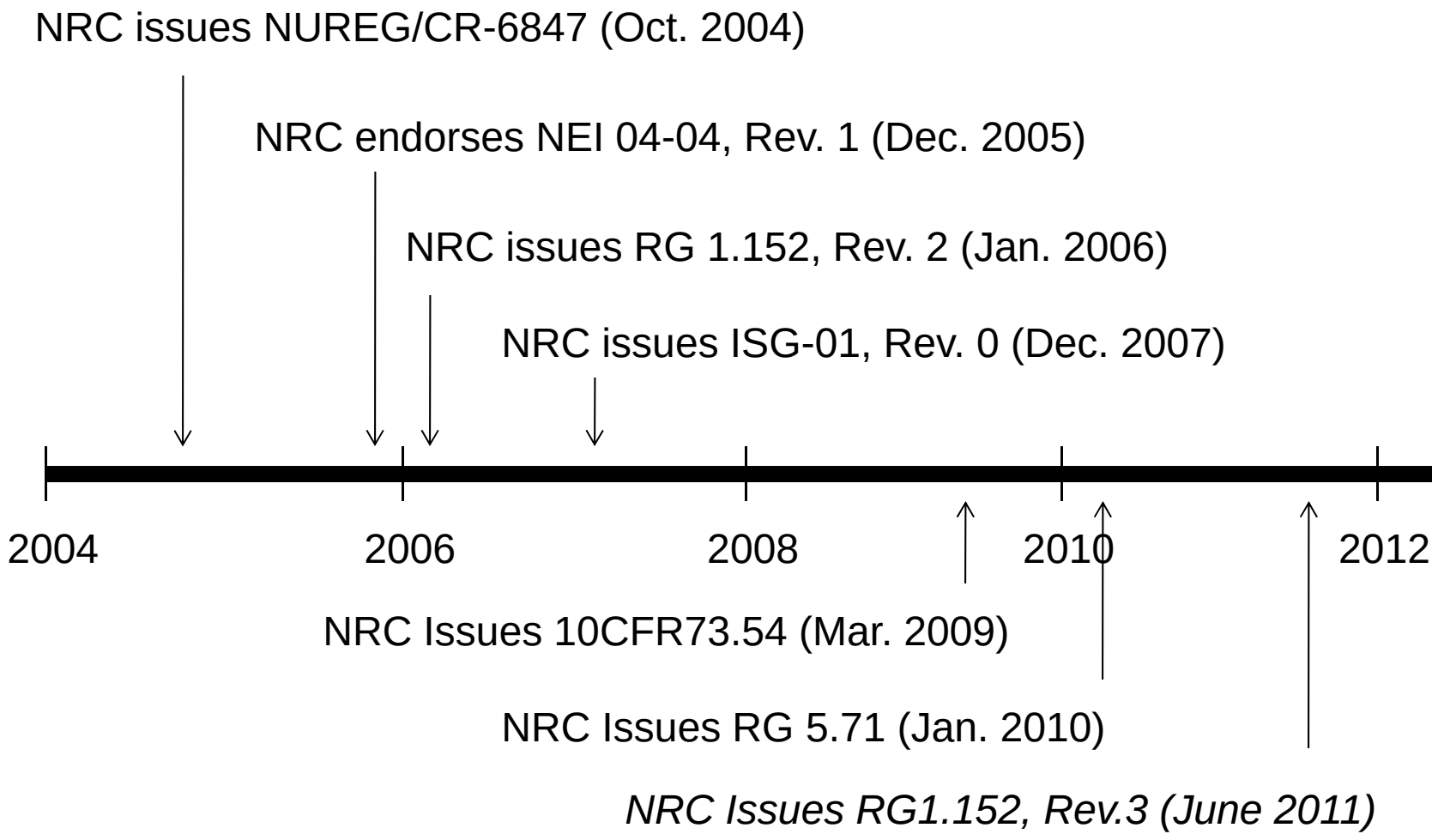
U.S.NRC
United States Nuclear Regulatory Commission
Protecting People and the Environment

Timeline



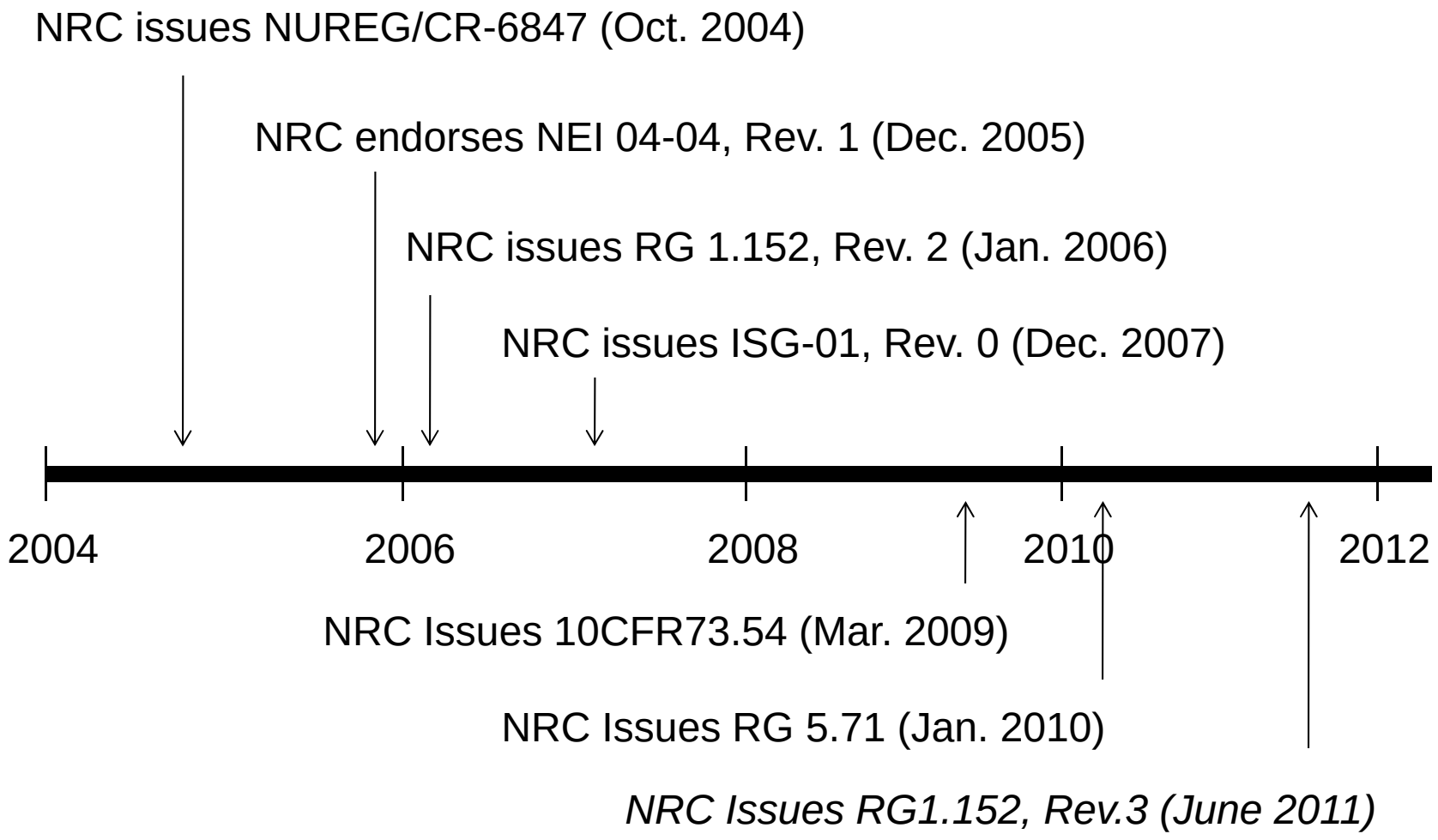
U.S.NRC
United States Nuclear Regulatory Commission
Protecting People and the Environment

Timeline



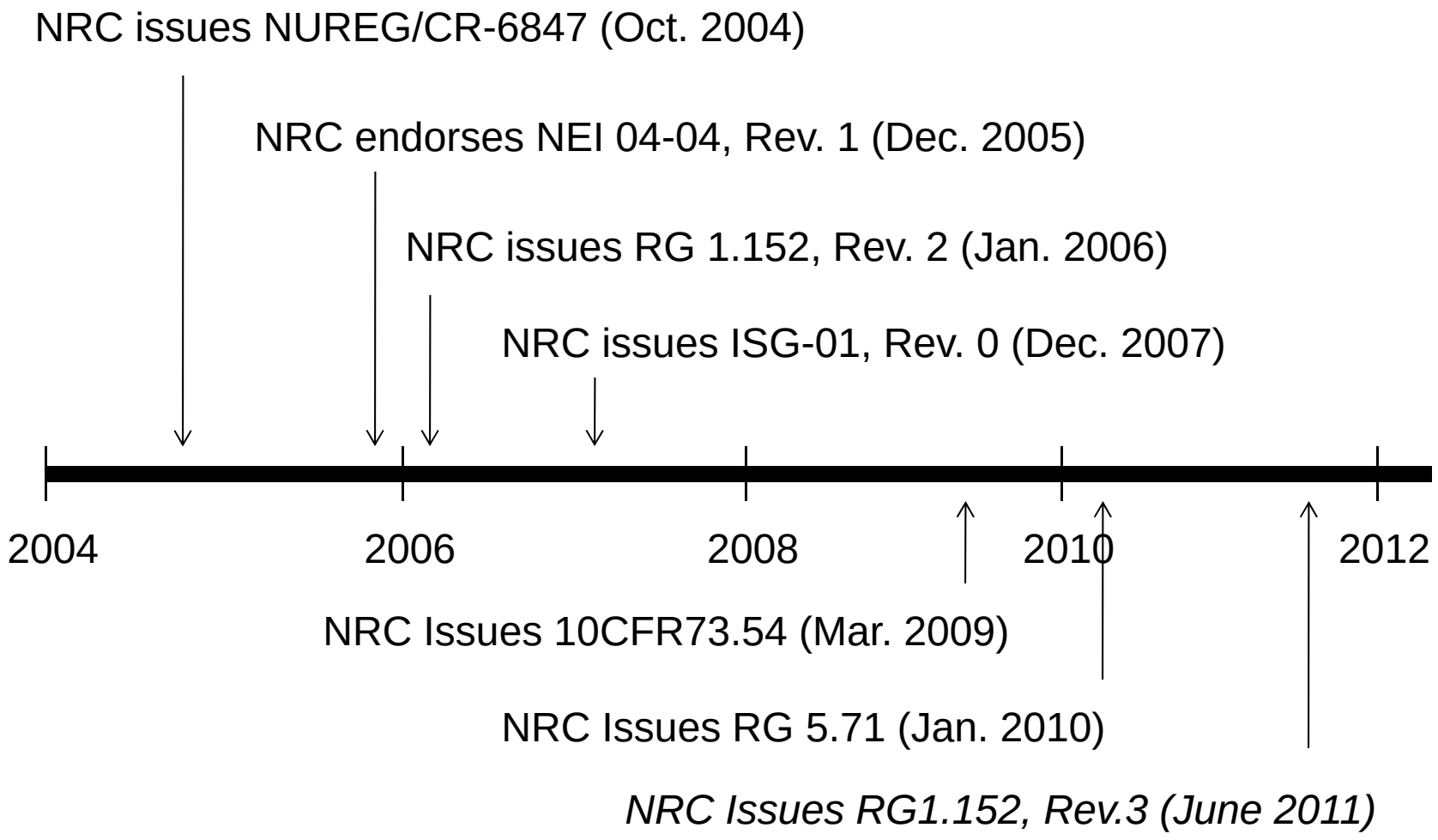
U.S.NRC
United States Nuclear Regulatory Commission
Protecting People and the Environment

Timeline



U.S.NRC
United States Nuclear Regulatory Commission
Protecting People and the Environment

Timeline



U.S.NRC
United States Nuclear Regulatory Commission
Protecting People and the Environment

Cyber Security Framework

- 10 CFR 73.54
  - Program focused
  - Performance-Based

- Cyber Security Licensing Process
  - Cyber Security Plans
    - One of Four Security Plans
  - Templates
    - Appendix A of RG 5.71 and NEI 08-09, Revision 6
    - Minimizes Licensing Review Period

U.S.NRC
United States Nuclear Regulatory Commission
Protecting People and the Environment

Cyber Security Framework

- Use of Chapter 13.6.6 NUREG 0800 Cyber Security SRP
  - Deviations or Alternate Methods Submitted by Licensees / Applicants Undergo In-Depth Review Against SRP and RG 5.71
- Cyber Security Licensing Reviews
  - Operating Reactors
  - New Reactor Applicants

U.S.NRC
United States Nuclear Regulatory Commission
Protecting People and the Environment

Cyber Security Framework

- Recent Policy Developments
  - Scope of Systems
- Planned Updates to RG 5.71 and SRP 13.6.6
- NEI-08-09, Revision 6
- Cyber Security Oversight / Inspection

U.S.NRC
United States Nuclear Regulatory Commission
Protecting People and the Environment

Digital System Safety Framework

- Goal: Ensure digital safety system reliability, availability, and integrity for non-malicious events.
- Part 73 review – determines adequacy of cyber security protection.
- Part 50/52 review – ensures protective feature does not impact safety.
- RG 1.152, Revision 3, supports these concepts.

U.S.NRC
United States Nuclear Regulatory Commission
Protecting People and the Environment

Digital System Safety Framework

- RG 1.152 was revised to:
  - Eliminate reference to cyber-security
  - Eliminate direction to evaluate systems against intentional malicious actions or attacks
- RG 1.152 is clarifying its focus on:
  - Controls to prevent inadvertent access to systems
  - Protection against undesirable behavior of connected systems
  - Protection of the development environment from inclusion of undocumented and unwanted code

U.S.NRC
United States Nuclear Regulatory Commission
Protecting People and the Environment

Technical Aspects of Digital System Security

- Design practices addressing non-malicious events could be used for malicious events
- Little technical change in the RG 1.152 regulatory positions
- Licensees and vendors are addressing cyber security up-front in the development stage

U.S.NRC
United States Nuclear Regulatory Commission
Protecting People and the Environment

Summary

- NRC's framework for addressing digital system security has evolved over the years
- Digital systems should have sufficient reliability, availability, and integrity in the face of non-malicious events
- Technical overlap in addressing malicious and non-malicious events
- RG 1.152 modifications are necessary to maintain consistency with the NRC's cyber security position
- NRC has a robust framework to address digital system safety and security

U.S.NRC
United States Nuclear Regulatory Commission
Protecting People and the Environment

Background Slides

U.S.NRC
United States Nuclear Regulatory Commission
Protecting People and the Environment

IEEE 603-1991

- Clause 5.6.3 (5.6 Independence) Between Safety Systems and Other Systems. The safety system design shall be such that credible failures in and consequential actions by other system, as documented in 4.8 of the design basis, shall not prevent the safety systems from meeting the requirements of this standard.
  - Clause 4.8 Design basis shall document conditions having the potential for functional degradation and for which provisions shall be incorporated to retain the capability for performing the safety functions (e.g., operator error, failure in nonsafety-related systems)
  - Clause 5.6.3.1(1) Interconnected Equipment Classification. Equipment used for safety and non-safety . . . Isolation devices used to effect a safety system boundary shall be classified as part of the safety system.
  - Clause 5.6.3.1(2) Interconnected Equipment Isolation. No credible failure on the non-safety side of an isolation device . . . A failure in the isolation device shall be evaluated in the same manner as a failure of other equipment in a safety system.

U.S.NRC
United States Nuclear Regulatory Commission
Protecting People and the Environment

IEEE 603-1991

- Clause 5.9 Control of Access. The design shall permit the administrative control of access to safety system equipment. These administrative controls shall be supported by provisions within the safety systems, by provision in the generating station design, or by a combination thereof.