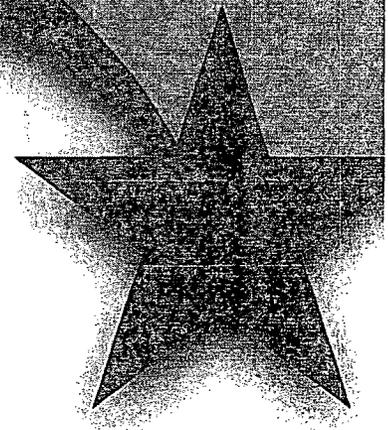


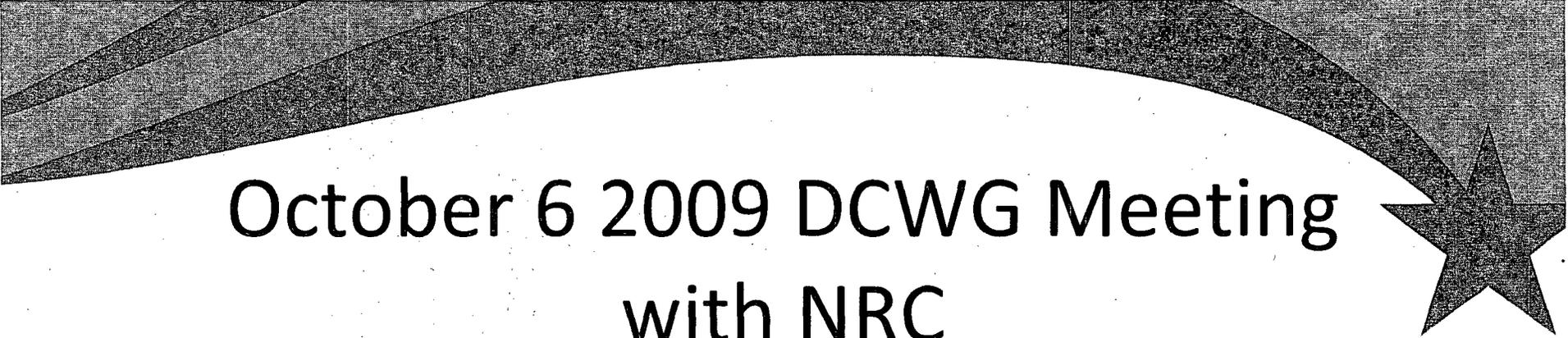


U.S. EPR Cyber Security

Pedro Salas

Licensing Technical Consultant



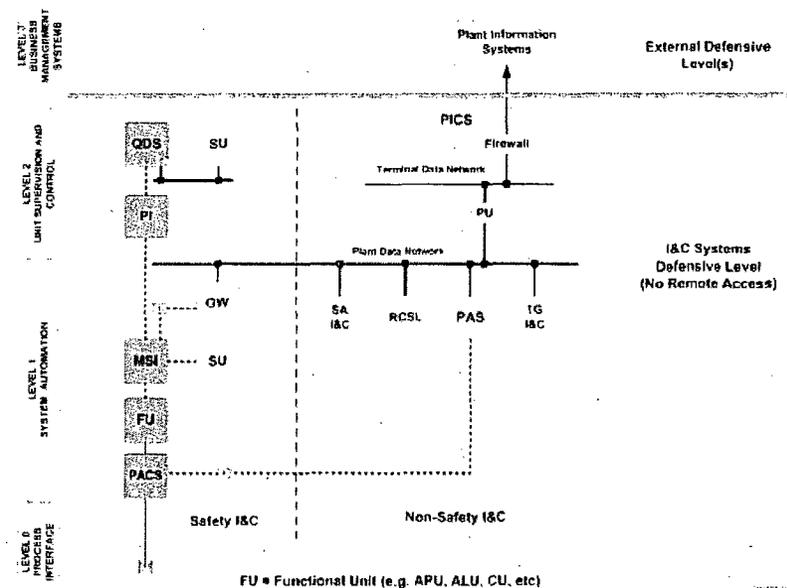


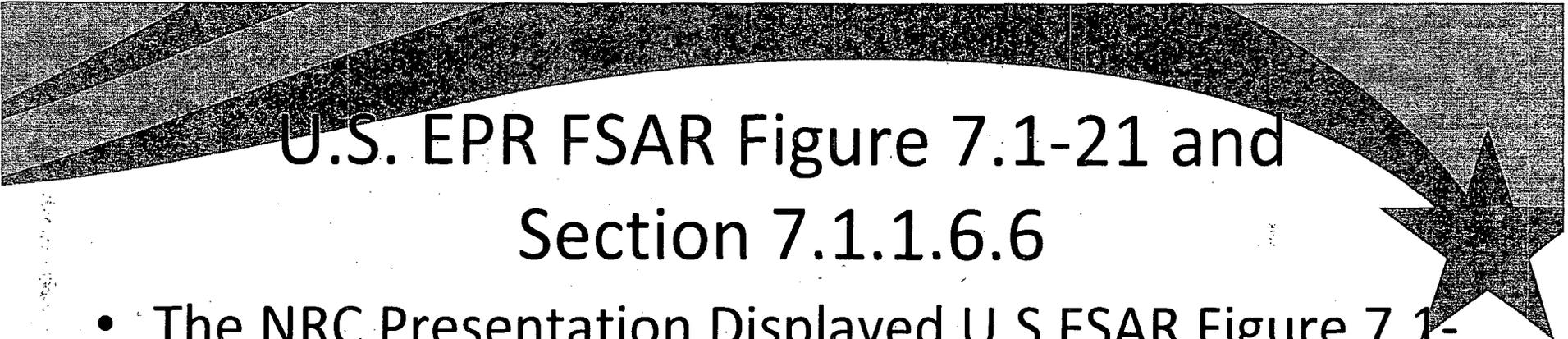
October 6 2009 DCWG Meeting with NRC

- On October 6, 2009 AREVA, UniStar and NRC Discussed Cyber Security During a DCWG Meeting
- NRC Identified Three Topics for the U.S. EPR DCWG to Consider

October 6, 2009 NRC Presentation

- *“Ensure that any non-safety equipment (including the supporting networks) communicating to safety systems (or EP, security, and support systems) is also afforded level 4 protection”*
- *“Demonstrate that cyber risks are managed for these non-safety equipment by addressing the security controls in Appendix B and Appendix C of RG 5.71”*
- *“Ensure any changes to these non-safety equipment undergoes a security assessment to ensure that the security of these equipment is not impacted by the proposed changes”*

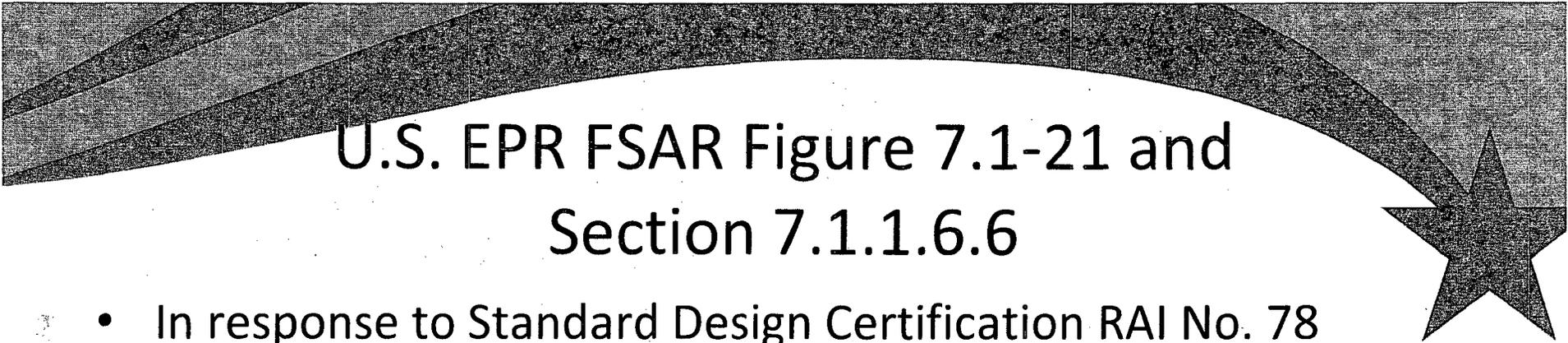




U.S. EPR FSAR Figure 7.1-21 and Section 7.1.1.6.6

- The NRC Presentation Displayed U.S FSAR Figure 7.1-21, Levels of Defense for Cyber Security
- The Figure and Section 7.1.1.6.6 were Developed and Included in the U.S. FSAR Prior to the Issuance of 10 CFR 73.54 when no Explicit NRC Cyber Requirements Existed
- As Regulatory Guide 5.71 states:

“Licensee and applicants bear sole responsibility for assessing and managing the potential for adverse effects on safety, security, and emergency preparedness...so as to provide high assurance that critical functions are adequately protected from cyber attacks.”



U.S. EPR FSAR Figure 7.1-21 and Section 7.1.1.6.6

- In response to Standard Design Certification RAI No. 78 (14.03.05-03), AREVA NP created a new combined License Information Item (13.6-4) incorporating a new requirement for an operational program:

“A COL applicant that references the U.S. EPR design certification will provide a cyber security plan consistent with 10 CFR 73.54”

- The COLA Cyber Security Plan Program Description will Establish the Required Features for Compliance with 10 CFR 73.54 and Regulatory Guide 5.71
- U.S. EPR FSAR Section 7.1.1.6.6 and Figure 7.1-21 Are Unnecessary and Will be Removed

U.S. EPR Cyber Security Classification



- Conceptual Cyber Security Classification Diagram Depicts the Cyber Security Levels
- Cyber security levels are Different From U.S. EPR Automation Levels

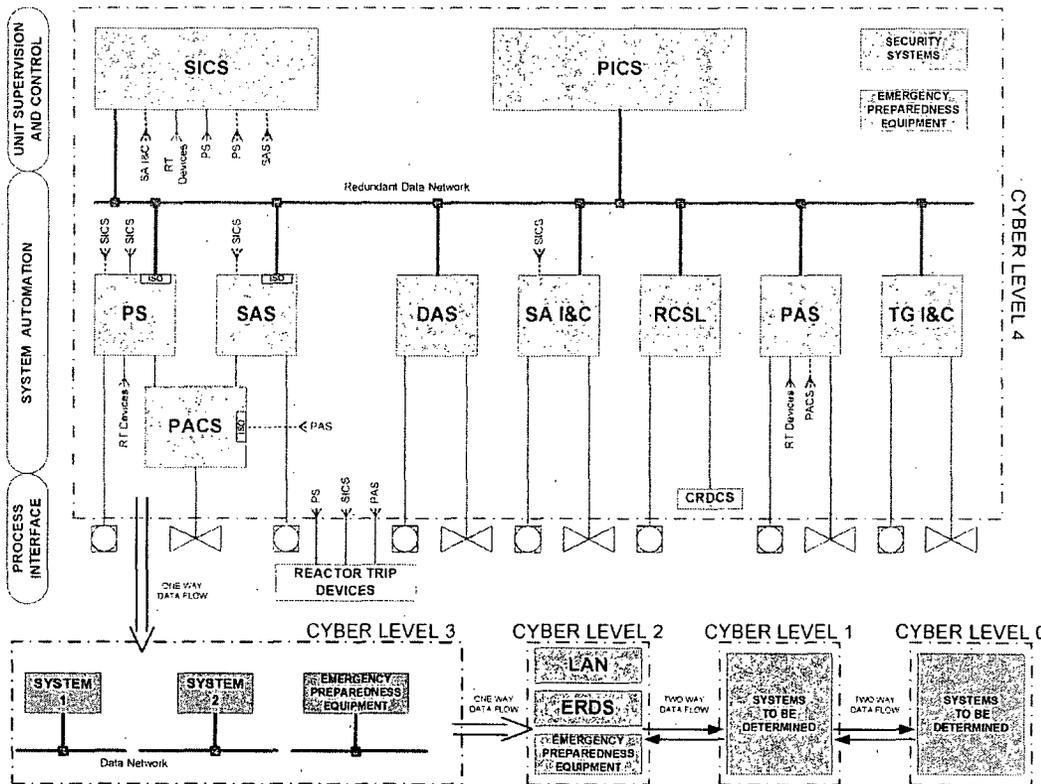
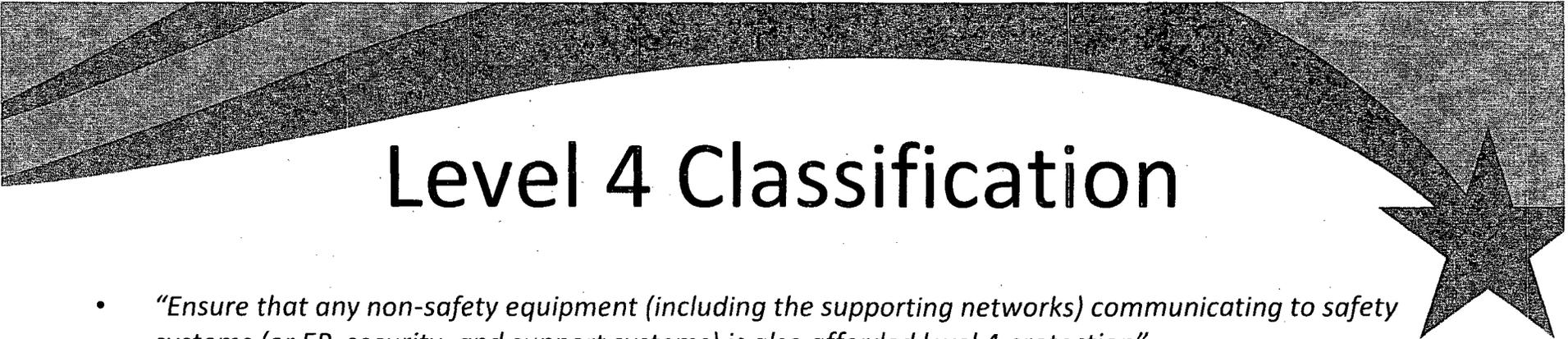


Figure 1: U.S. EPR I&C Conceptual Diagram - Cyber Security Levels (DRAFT-PRELIMINARY)

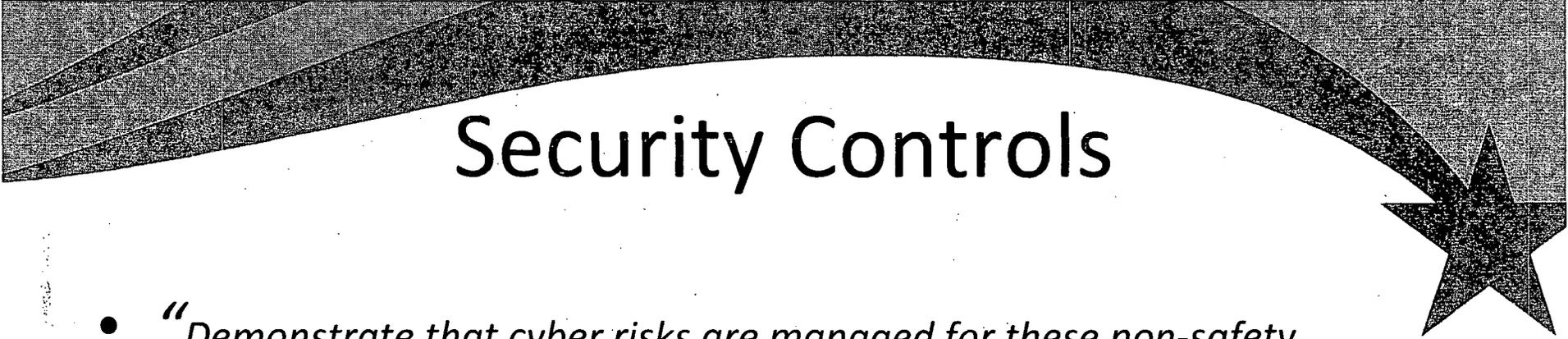
01/18/10 REVISION

Level 4 Classification



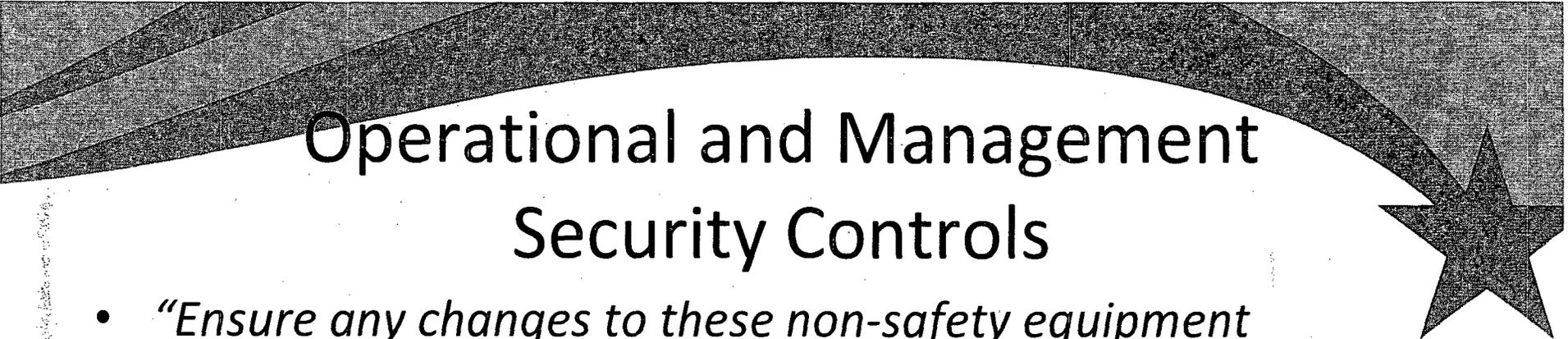
- *“Ensure that any non-safety equipment (including the supporting networks) communicating to safety systems (or EP, security, and support systems) is also afforded level 4 protection”*
 - The U.S. EPR non-safety systems within the scope of 10 CFR 73.54 are afforded level 4 protection
 - Only identified exception is Emergency Planning Due to Design Necessities
 - Regulatory Guide 5.71. Section c.3.2.1- Security Defensive Architecture, is silent on the classification level for Emergency Planning:
 - “CDAs associated with safety, important to safety and security functions, as well as support systems and equipment which, if compromised, would adversely impact safety, important to safety and security functions, are allocated to Level 4 and are protected from all lower levels”*
 - Some of the equipment supporting emergency preparedness functions--such as offsite communications equipment necessary to maintain two way communications with outside organizations such as Federal, State and Local authorities—must be able to communicate with lower cyber security level equipment maintained by those outside groups
 - Such data flow with outside organizations dictates that some of the equipment be placed in cyber security level 0-2
 - Remaining EP equipment will be placed in cyber security levels 3-4

Security Controls



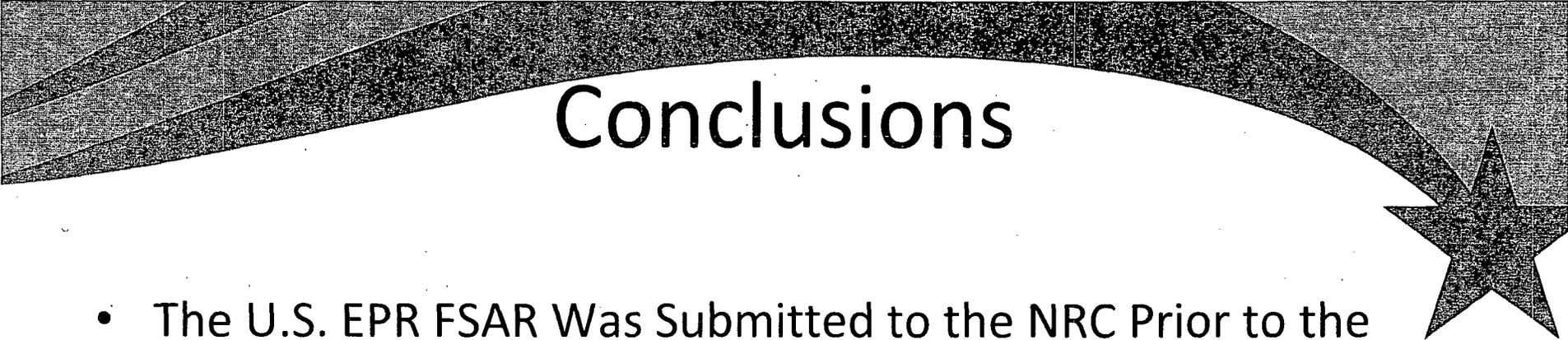
- *“Demonstrate that cyber risks are managed for these non-safety equipment by addressing the security controls in Appendix B and Appendix C of RG 5.71”*
 - Response to Standard Design Certification RAI No. 78 (14.03.05-03), AREVA NP created a new combined License Information Item (13.6-4) incorporating a new operational program: “A COL applicant that references the U.S. EPR design certification will provide a cyber security plan consistent with 10 CFR 73.54”
 - R-COLA Cyber Security Plan being developed by UniStar will require evaluation of the security controls in Appendix B and Appendix C of RG 5.71
 - R-COLA Cyber Security Plan is being developed based on RG 5.71

Operational and Management Security Controls



- *“Ensure any changes to these non-safety equipment undergoes a security assessment to ensure that the security of these equipment is not impacted by the proposed changes”*
 - The new combined License Information Item (13.6-4) incorporating a new operational program to provide a cyber security plan consistent with 10 CFR 73.54 addresses this concern
 - The Operational and Management Security Controls in the Cyber Security Plan will be based on RG 5.71 Appendix C and will provide an NRC approved method for controlling changes to the non-safety equipment

Conclusions

A decorative banner at the top of the slide features a dark, textured background with a curved, light-colored path that ends in a large, five-pointed star on the right side.

- The U.S. EPR FSAR Was Submitted to the NRC Prior to the Promulgation of New Cyber Security Requirements and Will be Adjusted In the Next Revision
- Non-safety Equipment Within the Scope of 10CFR 73.54 will be Classified as Cyber Level 4 – Except Emergency Planning Equipment that Requires Two Way Communications
- Cyber Risks will be Managed Consistent with Regulatory Guide 5.71
- Changes to Non-safety Systems will be Assessed for Cyber Risks With the Operational and Management Security Controls Outlined in the Cyber Security Plan Which Will be Based on Regulatory Guide 5.71