ENCLOSURE 4

Westinghouse Small Modular Reactor I&C Overview and Technical Discussion – Follow-up Presentation

(Non-Proprietary)

This is the Non-Proprietary Class 3 version of the presentation

Westinghouse Small Modular Reactor I&C Overview and Technical Discussion - Follow-up

Presented to:

Nuclear Regulatory Commission

September 24, 2013

Westinghouse

Meeting Purpose

- Further discuss two topics addressed at 08/22/2013 NRC/Westinghouse meeting
  - PMS redundancy
  - Control system segmentation
- Discuss one topic not addressed at 08/22/2013 meeting
  - Hazards analysis

WSMR Follow-up Meeting Agenda

- PMS redundancy
  - Conformance to requirements
    - Single Failure Criterion (SFC)
    - Risk based
  - Additional features to enhance reliability
  - Summary and Conclusions
- Control system architecture/segmentation
- Hazards analysis

WSMR I&C Redundancy Agenda

- Conformance to requirements
  - Single Failure Criterion (GDCs and IEEE 603)
    - During normal operation, malfunctions & testing
    - Input signals shared from protection to control
    - Component level redundancy
  - Risk objectives
- Additional features to enhance reliability

[ ] a,c

  - IDS power supply redundancy
  - Input sensor malfunction tolerance
- Summary and Conclusion

Westinghouse

Redundancy Bases

General Design Criteria (definitions) – Single failure - A single failure means an occurrence which results in the loss of capability of a component to perform its intended safety functions. Multiple failures resulting from a single occurrence are considered to be a single failure. Fluid and electric systems are considered to be designed against an assumed single failure if neither (1) a single failure of any active component (assuming passive components function properly) nor (2) a single failure of a passive component (assuming active components function properly), results in a loss of the capability of the system to perform its safety functions.

GDC 24 - Separation of protection and control systems. The protection system shall be separated from control systems to the extent that failure of any single control system component or channel, or failure or removal from service of any single protection system component or channel which is common to the control and protection systems leaves intact a system satisfying all reliability, redundancy, and independence requirements of the protection system. Interconnection of the protection and control systems shall be limited so as to assure that safety is not significantly impaired.

Redundancy Bases (continued)

- IEEE 603, Section 5.1 – Single Failure Criterion - The safety systems shall perform all safety functions required for a design basis event in the presence of: (1) any single detectable failure within the safety systems concurrent with all identifiable but non-detectable failures; (2) all failures caused by the single failure; and (3) all failures and spurious system actions that cause or are caused by the design basis event requiring the safety functions.
- Does the available redundancy support the PRA goals?
- Is additional PMS redundancy cost-effective (PRA based)

Westinghouse

WSMR PMS System Redundancy

[ ] a,c

Westinghouse

Safety System Signals Shared with Control

- IEEE 603, Section 5.1, Item (3) effectively requires a failure that would cause a design basis event to be considered in addition to a single random failure, item (1)
- Ways to address Item 3:
  - Have 4 channels (1 for Item 3, 1 for Item 1 – the single random failure, 2 to satisfy the 2/4 logic)

[ ] a,c

  - Provide separate protection and control channels
  - Others not currently used

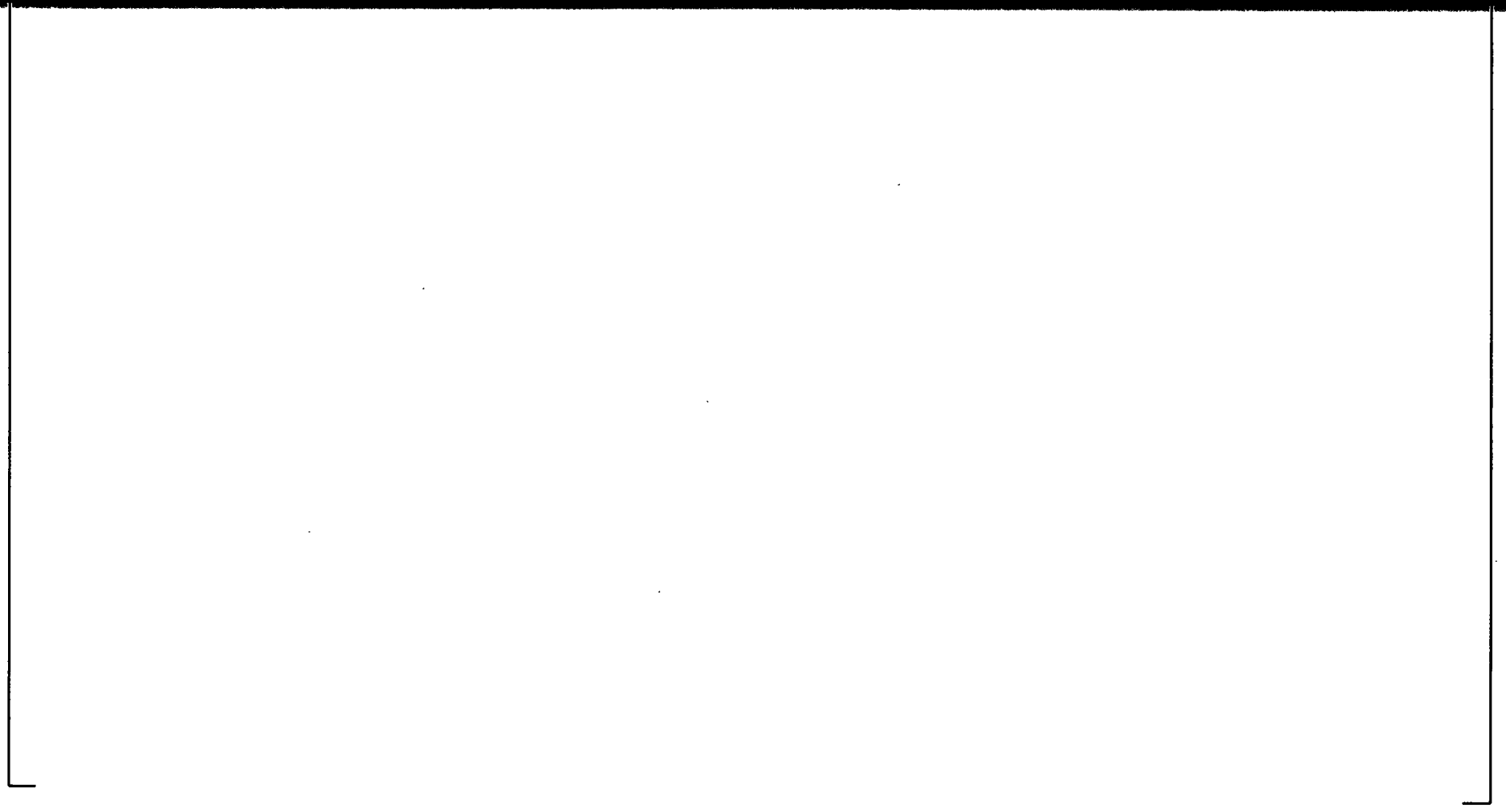
Westinghouse

- The PMS architecture ensures that safety functions will not be prevented by the SFC sub-criteria.
  - a) Any single detectable failure within the safety systems concurrent with all identifiable but non-detectable failures.
  - b) All failures caused by the single failure.
  - c) All failures and spurious system actions that cause or are caused by the design basis event requiring the safety functions.

[ ] a,c

Component Level Redundancy

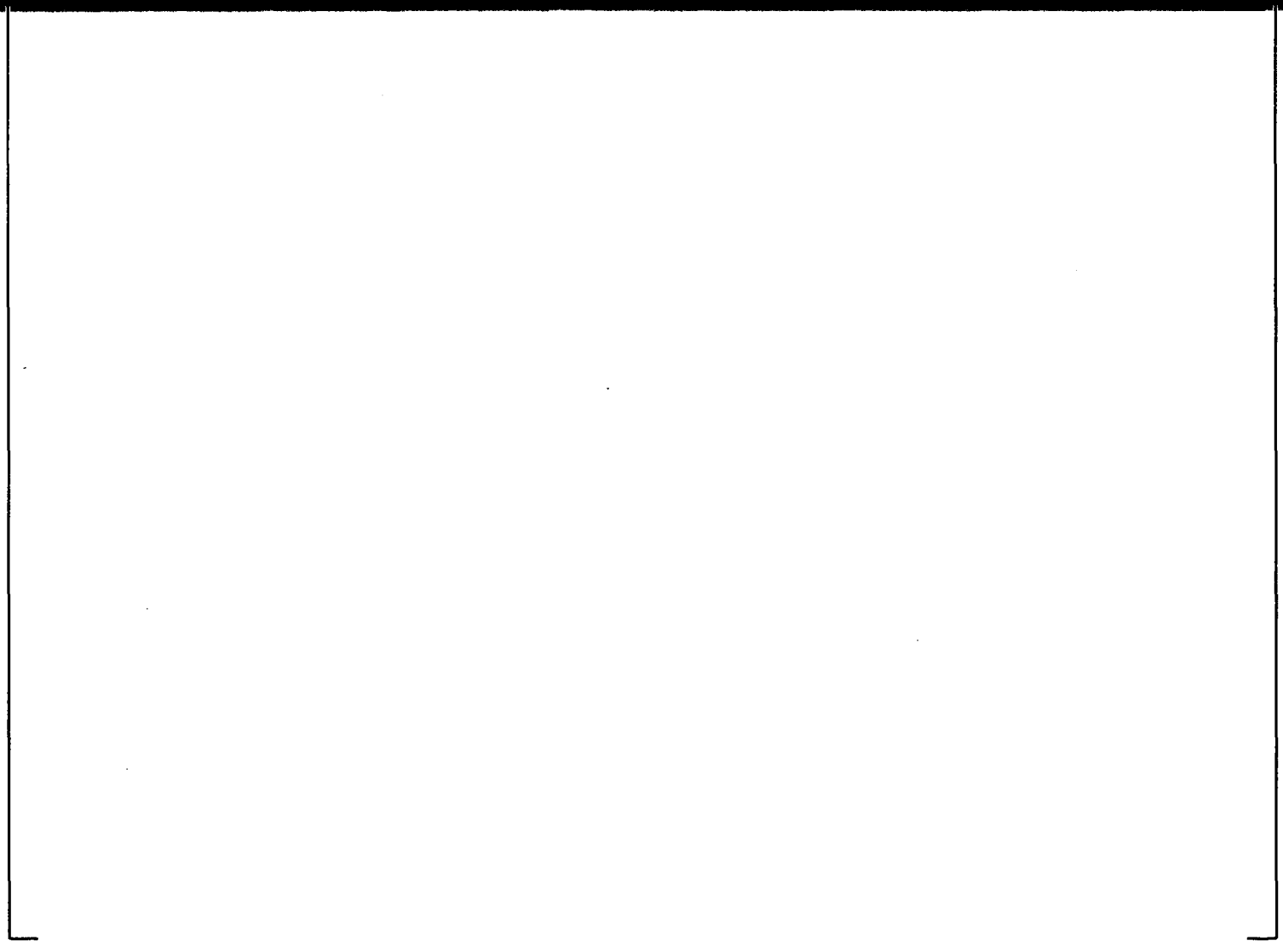
[ ] a,c



PRA Sensitivity Study Insights

[ ] a,c

Additional Features Improving WSMR Reliability

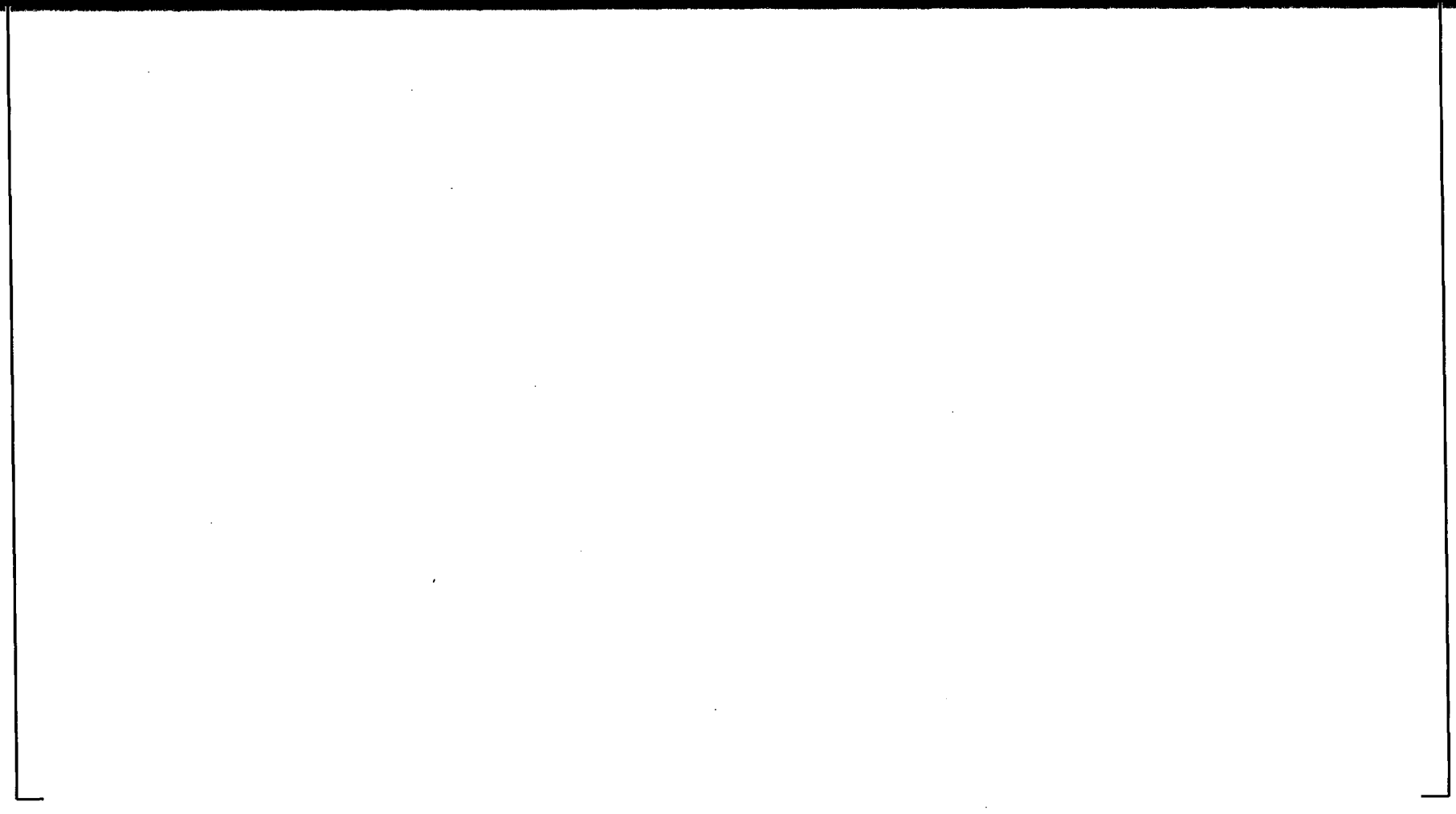


Component Control Path Redundancy

[ ] a,c

Inadvertent Actuation Prevention

a,c



IDS Power Supply Redundancy

[ ]a,c

IDS Power Supply Redundancy- IDS UPS

[ ] a,c

IDS Power Supply Redundancy-IDS – Battery

[a,c]

Input Sensor Malfunction Tolerance

[ ]a,c

DAS Redundancy

[ ]a,c

Summary and Conclusions

With One PMS Division Inoperable

[ ]a,c

Additional Features to Enhance Reliability

[ ]a,c

Loss of More than One PMS Division

- Two or more PMS division failures treated as CCF and addressed by DAS
- DAS inadvertent ADS actuation will be minimized

Protection System Comparison

[a,c]

(1) Some functions are only 3-way or 2-way redundant

Conclusions

For the SMR Protection and Safety Monitoring System

- The I&C architecture complies with all redundancy requirements including the Single Failure Criterion (normal operation, malfunctions and test)

[ ] a,c

- Many design features enhance reliability beyond the requirements of meet the single failure criterion
  - Ensure reliable actuation when required
  - Minimize the potential for inadvertent actuation

Westinghouse

Control System Architecture/Segmentation

SMR Control System Architecture

[ ]a,c

Control System Segmentation

[ ] a,c

Hazards Analysis

AP1000® Hazards Analysis

- FMEA of AP1000® Protection and Safety Monitoring System, (WCAP-16438-P)
- Software Hazards Analysis of AP1000® Protection and Safety Monitoring System, WCAP-16592-P
- Traditional hazards analysis methods
- Process for performing analyses well understood
- Plan is to follow same approach for SMR project

Westinghouse

Wrap Up

Questions?

Thank You!

Westinghouse