

**NUCLEAR DIRECTORATE
GENERIC DESIGN ASSESSMENT – NEW CIVIL REACTOR BUILD**

**STEP 3 SECURITY ASSESSMENT OF THE WESTINGHOUSE AP1000
DIVISION 5 ASSESSMENT REPORT NO. AR 09/042-P**

HSE Nuclear Directorate
Redgrave Court
Merton Road
Bootle
Merseyside L20 7HS

EXECUTIVE SUMMARY

This report presents the findings of the security assessment of the Westinghouse AP1000 undertaken as part of Step 3 of the Health and Safety Executive's (HSE) Generic Design Assessment (GDA) process.

The Office for Civil Nuclear Security (OCNS) has a good understanding of the security philosophy applied to the Westinghouse AP1000 design. No significant issues have been identified so far that would preclude this design from being adequately secured against malicious capabilities, as identified in the UK protectively marked Nuclear Industries Malicious Capabilities Planning Assumptions document.

LIST OF ABBREVIATIONS

CBSIS	Computer Based Systems Important to Safety
GDA	Generic Design Assessment
HSE	The Health and Safety Executive
ND	The (HSE) Nuclear Directorate
NIMCA	Nuclear Industries Malicious Capabilities Planning Assumptions
NISR2003	Nuclear Industries Security Regulations 2003
OCNS	The Office for Civil Nuclear Security (Division 5 of ND)
RP	Requesting Party
WEC	Westinghouse Electric Company LLC

TABLE OF CONTENTS

1 INTRODUCTION..... 1

2 NUCLEAR DIRECTORATE’S ASSESSMENT 1

 2.1 Requesting Party’s Security Assessment..... 1

 2.2 Standards and Criteria 1

 2.3 Nuclear Directorate Assessment..... 1

3 CONCLUSIONS AND RECOMMENDATIONS 2

4 REFERENCES..... 3

1 INTRODUCTION

- 1 This report presents the findings of the security assessment of the Westinghouse AP1000 undertaken as part of Step 3 of the HSE Generic Design Assessment (GDA) in keeping with the process described in the 'Guidance Document for Generic Design Assessment Activities' dated January 2007 (Ref. 1).
- 2 The process has involved the exchange of sensitive and protectively marked information between the Office for Civil Nuclear Security (OCNS), the Requesting Parties and foreign regulatory and security agencies.

2 NUCLEAR DIRECTORATE'S ASSESSMENT

2.1 Requesting Party's Security Assessment

- 3 In late 2008, Westinghouse supplied OCNS with a protectively marked technical report describing security measures of the Westinghouse AP1000 design.

2.2 Standards and Criteria

- 4 In making their security assessment of the Westinghouse AP1000 design OCNS took into account information and standards contained in two UK protectively marked documents, the Nuclear Industries Malicious Capabilities Planning Assumptions (NIMCA) document, (which is the United Kingdom's Design Basis Threat), and the Nuclear Industries Security Regulations 2003 Technical Requirements Document.

2.3 Nuclear Directorate Assessment

- 5 After receipt of the protectively marked technical report describing security measures on the AP1000 design, OCNS carried out a detailed review of the submission to identify the areas of the generic design that require physical protection. OCNS now has a good understanding of these features and the philosophy of the design intent. The initial findings of the OCNS review indicate that the AP1000 has some robust security features that will support the OCNS requirement to have security by design in place from the onset to face the threats of the 21st century.
- 6 OCNS has extracted relevant sections of the technical report and the resulting document was forwarded to the GDA Safety Assessment Team in June 2009 for verification and validation. This was specifically with regard to the identification of Vital Areas and Computer Based Systems Important to Safety (CBSIS). OCNS now awaits the result of this verification and validation exercise, before applying OCNS's technical security requirements to determine whether further physical protection is required on the generic design.
- 7 Once the ND safety specialists have delivered their report, OCNS will engage in detailed discussions with Westinghouse to progress and conclude the development of generic conceptual security arrangements. This work will be completed by June 2011.
- 8 To date, no issues have been identified that might suggest that the Westinghouse AP1000 design is not capable of supporting the development of a robust security regime.

3 CONCLUSIONS AND RECOMMENDATIONS

- 9 OCNS has a good understanding of the security philosophy applied to the Westinghouse AP1000 design and is now awaiting validation of the relevant sections of the Westinghouse supplied technical document by ND Safety Assessors. No significant issues have been identified so far that would preclude this design from being adequately secured against malicious capabilities, as identified in the NIMCA.
- 10 It is recommended that OCNS proceed to GDA Step 4 assessment of the Westinghouse AP1000.

4 REFERENCES

- 1 *Guidance Document for Generic Design Assessment Activities.* Office for Civil Nuclear Security. Version 2 201206, January 2007.