行政院原子能委員會

委託研究計畫研究報告

核能電廠儀控資安評估與型態管理研究

The Research on Information Security and Configuration Management of I&C System for Nuclear Power Plants

計畫編號：992001INER004

受委託機關(構)：長庚大學

計畫主持人：陳昱仁

核研所聯絡人員：周貽新

聯絡電話：(03)2118800#5823

E-mail address：cyr@mail.cgu.edu.tw

報告日期：99 年 11 月 30 日

目　次

目　次 i

圖目次 iii

表目次 iv

中文摘要 1

Abstract 2

壹、計畫緣起與目的 3

貳、研究方法與過程 6

一、相關文獻探討 6
(一) 各國核電廠重大事故 6
(二) 核安相關網站 9
(三) 核安相關標準 11
(四) DI&C-ISG-04 適用性評估 15
二、RG 5.71 探討 21
(一) 緒論 (Introduction) 21
(二) 討論 (Discussion) 21
(三) 法規觀點 (Regulatory Position) 24
(四) 附錄 A、通用網路安全計畫樣版 (Generic Cyber Security Plan Template) 26
(五) 附錄 B、技術性安全控制 (Technical Security Controls) 38
(六) 附錄 C、操作性與管理性安全控制 (Operational and Management Security Controls) 58

參、主要發現與結論 106

一、核能電廠儀控系統資安評估項目 106
二、核能電廠儀控系統流程安全弱點分析方法設計 107
三、應用安全分析於飼水控制系統之型態管理 108
(一) 飼水控制系統簡介 108
(二) 型態管理 108
(三) 飼水控制系統型態管理安全分析 109
四、結論與效益 116

(一) 結論 116
(二) 主要效益 117
參考文獻 119

圖目次

圖 2.1：我國核能電廠近八年異常事件統計.....7
圖 2.2：我國核能機組歷年異常事件平均件數統計圖 7
圖 3.1：Level-0 安全分析圖 111
圖 3.2：Level-1 分析圖 112
圖 3.3：Level-1 安全分析圖 113
圖 3.4：Level-2 分析圖 114
圖 3.5：Level-2 安全分析圖 115

表目次

表 2.1：我國核能電廠 97 年異常事件分級統計.....6
表 2.2：各國核安事故.....8
表 2.3：核安相關網站－中華民國.....9
表 2.4：核安相關網站－世界各國.....10
表 2.5：核安相關網站－國際組織、新聞與研討會、除污與除役..11

中文摘要

近來核電廠的數位儀控網路系統紛紛採用具有開放性與標準化的產品，以增強擴充性與互通性，然而這卻導致了攻擊者可以透過標準化的工具以及增加的管道進行入侵攻擊。近年來各國資訊安全相關事件不斷發生，更突顯資訊安全的重要性。在上一年度計畫中，我們針對核電廠的儀控網路，規劃專屬的資訊安全管理制度 (Information Security Management System, ISMS)，稱之為儀控網路安全管理制度 (Instrumentation and Control Network Security Management System, ICNSMS)，我們期望這個新制度的產生，將對我國電廠或採用儀控網路的相關單位產生幫助，尤其是在資訊安全管理制度的規劃與建置方面能夠具有參考價值。

為了維護核能電廠儀控系統的整體安全，本計畫藉由研究發展中核能安全相關標準，諸如 NRC Security Rule 73.54 (10 CFR 73.54)、RG 5.71 和 NERC 關鍵基礎建設防護 (Critical Infrastructure Protection, CIP) 標準等，以訂定核能電廠儀控系統資安評估項目。依據核能電廠儀控系統流程，設計圖形化安全弱點 (Vulnerability) 分析方法。並且以龍門電廠數位儀控系統之型態管理 (Configuration Management) 為主要探討對象，應用所提之安全弱點分析方法來描述其安全弱點與威脅 (Threat) 所在以及相對應之防禦對策，以加強型態管理之安全。藉由所描述之安全弱點與威脅所在以及相對應之防禦對策，除了可供核電廠瞭解自身數位儀控系統的弱點所在，以加強型態管理之安全，對於支援原能會核電廠數位儀控系統審查管制將有所助益。

關鍵詞：數位儀控系統、資訊安全、弱點分析、型態管理

Abstract

Recently the products with openness and standardization are increasingly used in Instrumentation and Control (I&C) network systems of nuclear power plants to improve extensibility and interoperability. However, this causes the possibility that attackers can intrude and attack I&C system via common tools. In recent years, due to the information security accidents happening again and again, it mentions the importance of information security. In previous project, we aim at planning a dedicated system for the instrumentation and control network of nuclear power plants. The proposed system is called Instrumentation and Control Network Security Management System (ICNSMS). We expect that the proposed system will benefit the power plants and the officials in producing an Information Security Management System ISMS).

In order to improve the overall security of nuclear power plant I&C system, this project will study nuclear security related standards in development to decide the information security evaluation items for nuclear power plant I&C system. The referred standards include NRC Security Rule 73.54 (10 CFR 73.54), RG 5.71 and NERC CIP Standards, etc. Besides, according to the flows of nuclear power plant I&C system, we plan to design a graphical vulnerability analysis method. Furthermore, taking the configuration management of nuclear power plant I&C system as a target, we will apply the proposed vulnerability analysis method to describe the vulnerabilities, threats and countermeasures to improve the security of configuration management.

Keywords: Digital I&C System, Information Security, Vulnerability Analysis, Configuration Management

壹、計畫緣起與目的

核能安全近年來不斷有發生相關安全事故事件，在世界各地許多國家，對於核能電廠的興建與否，引發了極大的討論，其原因最重要的就是因為核能電廠的安全性受到質疑。核能電廠發電的過程是利用核分裂反應而發電，利用鈾製成的核燃料在反應爐內進行裂變，並且釋放出大量熱能，高壓下的循環冷卻水把熱能帶出，在蒸汽發生器內生成蒸汽，推動發電機旋轉。由於核燃料本身為一高放射性物質，對人類健康會產生極大影響，如果在操作過程中稍有不慎，或由於操作系統與其網路環境本身的弱點造成系統運轉失常與故障，甚至是因為不周密的安全政策造成資料的外洩，對於核能電廠發電的安全與一般民眾之健康安全，會產生嚴重的衝擊，其後果是難以設想的。為了避免 1986 年前蘇俄車諾比爾核電廠核能電廠事故的重大公安意外重演，也為了防止 2005 年日本核能電廠資料外洩事件再次發生，如何針對核能電廠發電上的安全，與資料及網路的安全性加以防範，是核能發電被接受的關鍵。

資訊科技的發展提供維護設備的高度可靠性以及正確性，能源產業紛紛為其工廠導入數位儀控 (Instrumentation and Control, I&C) 系統，如分散式控制系統 (Distributed Control System, DCS)、資料監控與擷取系統 (Supervised Control and Data Acquisition, SCADA) 與其他週邊元件等。其中分散式控制系統為一個廣泛應用於工業領域上的系統，主要負責計算、通訊、顯示與控制其它遠端的各項裝置，在設備運作過程中進行操控、資料蒐集與錯誤分析。早期的儀控系統採用非標準化的資料規格與傳輸方式，除了在擴充性上具有明顯缺點之外，也導致互通性不佳，妨礙了工廠與其工作伙伴的溝

通聯繫。近年來，儀控系統持續的追求開放性與標準化，Profibus 與 Modbus 就是兩個相當著名的標準化規格。

標準化產品提升了互通性與效率，但是標準規格的公開化，讓攻擊者可以透過符合標準的工具進行探測與攻擊，系統安全性因此容易遭受質疑。再加上為了提升網路互通效率的網際網路架構 (Internet Architecture)，開啟了工廠內部資訊向外聯繫的門戶，也增加了有心人士入侵的管道。舉個例子來說，如果核電廠來往的第三方廠商透過互連網路入侵，並且置換系統的控制作業參數，核子反應爐的運作可能受到不同嚴重程度的干擾，其後果之嚴重性可想而知。因此，在追求效率提升的同時，針對資訊安全的設計，也成為核電廠在維護整體安全目標上一個相當重要的議題。

在上一年度計畫中，我們針對核電廠的儀控網路，規劃專屬的資訊安全管理制度 (Information Security Management System, ISMS)，稱之為儀控網路安全管理制度 (Instrumentation and Control Network Security Management System, ICNSMS)，我們期望這個新制度的產生，將對我國電廠或採用儀控網路的相關單位產生幫助，尤其是在資訊安全管理制度的規劃與建置方面能夠具有參考價值。

為了維護核能電廠儀控網路的整體安全，本計畫參酌美國核能管制委員會 (Nuclear Regulatory Commission, NRC) 內之研究單位核能管制研發署 (Office of Nuclear Regulatory Research, RES) 與美國電力研究所 (Electric Power Research Institute, EPRI) 近年的研發重點－儀控系統網路安全研究 (Cyber Security Research)、儀控現代化 (I&C Modernization)，以及美國國家標準與技術局 (National Institute of Standards and Technology, NIST) 所發布的工業用資料與

監控系統安全指南。藉由研究發展中核能安全相關標準，諸如 NRC 之 10 CFR 73.54 (U.S. Nuclear Regulatory Commission Regulations: Title 10, Code of Federal Regulations, Section 73.54) “Protection of Digital Computers and Communications Systems and Networks”、法規指引 (Regulatory Guide, RG) 5.71 “Cyber Security Programs for Nuclear Facilities”、美國核能協會 (Nuclear Energy Institute, NEI) 之 NEI 08-09 “Cyber Security Plan Template” 和北美電力可靠度委員會 (North American Electric Reliability Council, NERC) 之關鍵基礎建設防護 (Critical Infrastructure Protection, CIP) 標準 “NERC Critical Infrastructure Protection (CIP) Standards” 等，以訂定核能電廠儀控系統資安評估項目。依據核能電廠儀控系統流程，設計圖形化安全弱點分析方法。並且以龍門電廠數位儀控系統之型態管理 (Configuration Management) 為主要探討對象，應用所提之安全弱點 (Vulnerability) 分析方法來描述其安全弱點與威脅 (Threat) 所在以及相對應之防禦對策，以加強型態管理之安全。藉由所描述之安全弱點與威脅所在以及相對應之防禦對策，除了可供核電廠瞭解自身數位儀控系統的弱點所在，以加強型態管理之安全，對於支援原能會核電廠數位儀控系統審查管制將有所助益。

貳、研究方法與過程

一、相關文獻探討

在本小節中，我們探討各國核安事故、核安相關網站以及核安相關標準等。

(一) 各國核電廠重大事故

國際核能事件分級制度將核能事件分成 1 至 7 個不同等級，較低的 1 至 3 級總稱為異常事件 (Incidents)，較高的 4 至 7 級則稱為核子事故 (Accidents)，若干事件如無安全的顧慮則將之歸類成 0 級（或稱未達級數）。我國 97 年各核能電廠異常事件經由上述原則分級後，結果如表 2.1，全部 13 件異常事件均係由上述第三項分級準則「深度防禦」判定其級別，屬於無任何安全顧慮的 0 級事件，顯示對民眾或環境不會有影響。

表 2.1：我國核能電廠 97 年異常事件分級統計

事件級別	廠別			總計	
	核一廠	核二廠	核三廠	件數	百分比%
0級	8	4	1	13	100
1級	0	0	0	0	0
2級	0	0	0	0	0
總計	8	4	1	13	100

97 年中核一廠共計發生 8 件異常事件；核二廠 4 件；核三廠 1 件；三座核電廠合計 13 件。以機組別比較，則以核一廠一號機發生

5 件較多，其次為核一廠二號機 3 件、核二廠一、二號機各 2 件，核三廠一號機 1 件。以近 5 年之整體趨勢看來，約略穩定於每年 2 件左右（如圖 2.1）；我國核能機組歷年異常事件平均件數統計結果如圖 2.2，近 5 年之平均值為每年每機組 1.83 件。

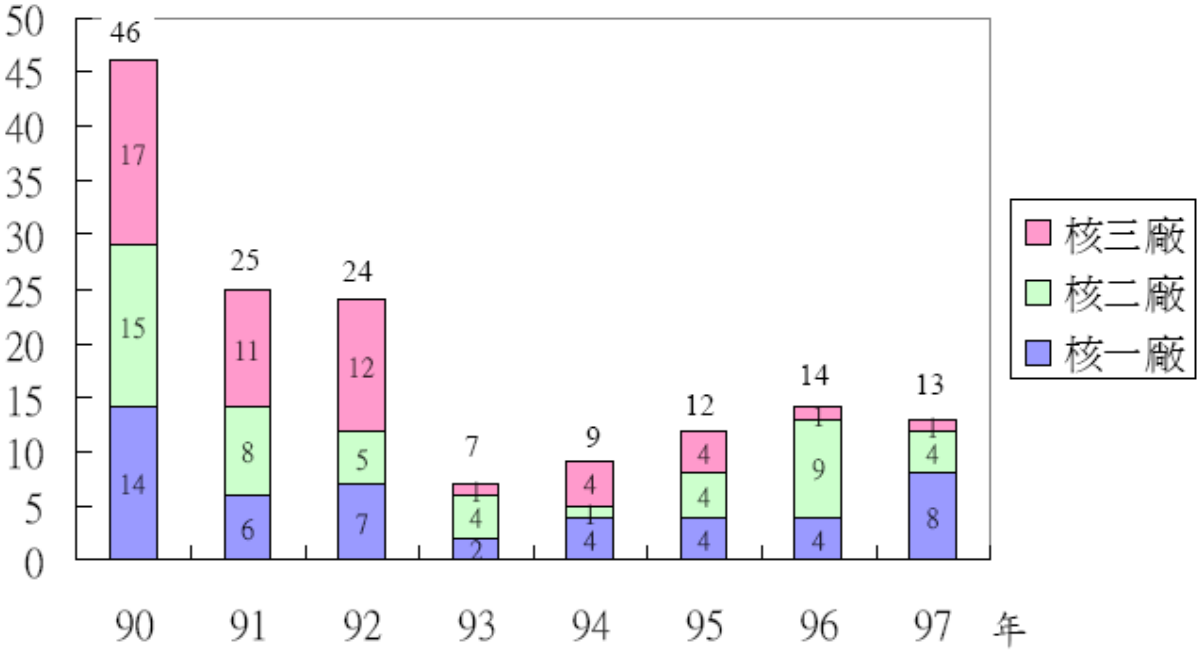

圖 2.1：我國核能電廠近八年異常事件統計

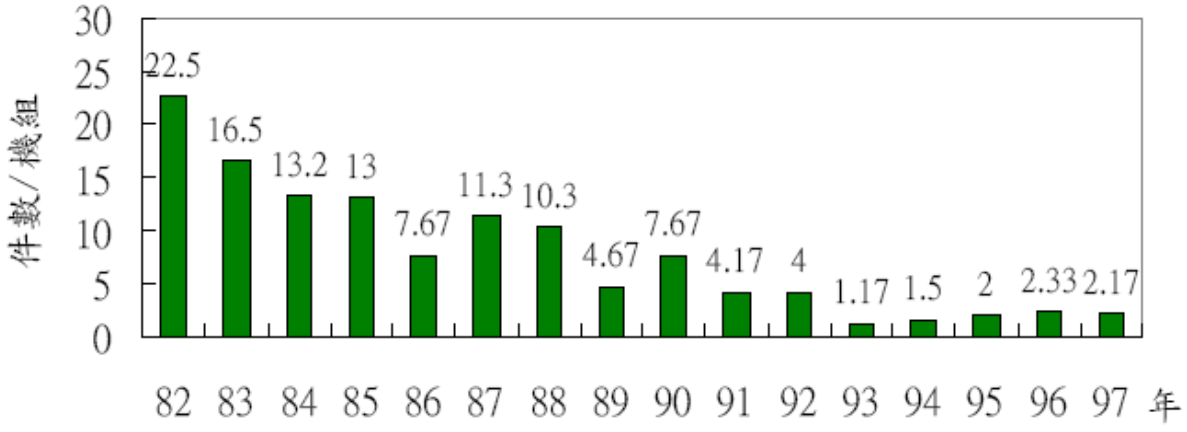

圖 2.2：我國核能機組歷年異常事件平均件數統計圖

其它各國核安事故，整理如表 2.2。

表 2.2：各國核安事故

日期	地點	概要
1979 年 3 月	美國三哩島核電廠	發生在美國賓夕法尼亞州薩斯奎哈納河三哩島核電廠的一次嚴重放射性物質泄漏事故。
1986 年 4 月	烏克蘭車諾堡核電廠	位於烏克蘭的車諾堡核電廠，發生核能工業史上最嚴重的輻射事故，輻射污染擴及白俄羅斯、俄羅斯及烏克蘭等國。
1986 年 12 月	美國 Surry 電廠	2 號機主飼水碳鋼管路發生沖腐蝕 (Erosion/Corrosion) 薄化破管造成 4 人死亡。
1992 年 2 月	立陶宛 Inalina 核電廠	發生對管理當局心懷不滿之電廠計算機中心員工，故意在電廠控制系統程式內置入邏輯炸彈 (Logic Bomb)，使控制系統功能異常；所幸控制室工程師及早發現異常狀況而未釀成事故。
1993 年 6 月	日本福島第二電廠	1993 年 6 月 15 日五次大修執行圍阻體洩漏測試，將控制棒驅動壓力系統 (HCU) 隔離時，有二支控制棒被抽出一半，一支棒位為 22，另一支棒位為 12（全入棒位為 0；全出棒位為 48）。
1996 年 1 月	美國 Crystal River 核電廠	大量海水侵入熱井，致使冷凝水與飼水系統遭到污染，在蒸汽產生器測得高濃度的氯離子、鈉離子及硫酸根。
1999 年 9 月	日本 JCO 濃縮鈾製造公司	發生鈾燃料臨界 (Criticality) 事故，造成人員受到輻射曝露，並有放射性物質外釋，導致事故現場半徑 350 公尺內之居民緊急疏散，半徑 10 公里內之居民在屋內掩蔽，本事故計有三名 JCO 工作人員受到嚴重輻射曝露（其中二名死亡）。
2000 年 4 月	日本柏崎刈羽電廠	進行第 11 次大修執行圍阻體洩漏測試，將控制棒驅動壓力系統(HCU)隔離時，有二支控制棒被抽出一半，一支棒位為 24，另一支棒位為 18(全入棒位為 0；全出棒位為 48)。
2002 年	日本福島第一核電廠	一號機被檢舉爆料，於 1992 年曾偽造圍阻體洩漏測試紀錄，在那次事件爆發後日本原子力安全保安院即勒令東京電力公司的其他 16 座核能電廠平行展開，限期停機重新執行圍阻體洩漏測試，並由原子力安全保安院人員複查後才恢復發電。

表 2.2：各國核安事故（續）

日期	地點	概要
2003 年 1 月	美國 Duane Arnold Energy Center 核電廠	大量化學污染物進入反應爐，使得反應爐內的硫酸根濃度為運轉限值的 15,000 倍。
2003 年 1 月	美國 Ohio 核電廠	Davis Besse 發生執行維修之施工廠商在廠內網路上自行搭接對外連結線路，以便工程師其可由廠外處所進行維修工作，結果當工程師使用家中電腦以撥接方式聯線進入電廠網路時，將家中電腦感染病毒傳入核電廠網路中，並造成核電廠之「安全參數展示系統 (Safety Parameter Display System)」故障達 6 小時。
2003 年	匈牙利 Paks 核電廠	發生被判定為 INES-2 等級的燃料破損事故。
2004 年 8 月	日本關西電力公司美濱核電廠	3 號機，因為飼水管路破裂蒸汽外洩，造成 5 名員工吸入蒸汽死亡，另有 6 名員工遭到嚴重燙傷，因為美濱電廠是壓水式設計的機組，二次側的飼水並無放射線，所以只是一般的工安事件。
2008 年 9 月	美國 AEP (American Electric Power) 電力公司 DC Cook 核電廠	1 號機之汽機發電機該機組於滿載運轉時，因主汽機所有軸承皆出現高振動警報而手動跳機，期間發電機並因氫氣外漏而引發火災，事件發生過程反應器相關設備皆正常運作，所幸無人員因此事件受傷；該事件造成汽機嚴重受損，汽機高振動之肇因為 3 支低壓汽機末級葉片斷裂（LP-2，2 支、LP-3，1 支）。

(二) 核安相關網站

核安相關網站分成中華民國、國際組織、新聞與研討會、除污與除役，以及世界各國五種分類，分類整理如表 2.3 至表 2.5。

表 2.3：核安相關網站－中華民國

中華民國	
台灣電力公司 (Taiwan Power Company, Taipower)	http://www.taipower.com.tw/
中華民國核能學會 (Chung-Hwa Nuclear Society)	http://www.chns.org/
核能資訊中心 (Nuclear Information Center)	http://www.nicenter.org.tw/
南部輻射傷害防治中心 (Radiation Accident Management Center in Southern Taiwan, RAMC)	http://ramc.kmu.edu.tw/

表 2.4：核安相關網站－世界各國

世界各國	
阿根廷 ARN (Nuclear Regulatory Authority) (核能管制局)	http://200.0.198.11/
澳大利亞 APRANSA (Australian Radiation Protection and Nuclear Safety Agency) 澳洲輻射防護及核能安全局	http://www.arpansa.gov.au/
比利時 AFCN (Agence Federale de Controle Nucleaire) (聯邦核能管制局)	http://www.fanc.fgov.be/page/homepage/1.aspx
巴西 CNEN (Brazilian National Commission for Nuclear Energy) (巴西核能委員會)	http://www.cnen.gov.br/
加拿大 (Canadian Nuclear Safety Commission) (加拿大核能安全委員會)	http://www.nuclearsafety.gc.ca/
智利 CHEN (Chilean Nuclear Energy Commission) (智利核能委員會)	http://www.cchen.cl/
捷克 SUJB (State Office for Nuclear Safety) (核能安全局)	http://www.sujb.cz/
芬蘭 STUK (Radiation and Nuclear Safety Authority) (輻射及核能安全局)	http://www.stuk.fi/english
法國 ASN (AUTORITE DE SURETE NUCLEAIRE) 核子安全主管機關	http://www.asn.gouv.fr/
德國 BMU (聯邦環境、自然資源暨核能安全部)	http://www.bmu.de/allgemein/aktuell/160.php
匈牙利 Hungarian Atomic Energy Authority (匈牙利原子能局)	http://www.haea.gov.hu/web/v2/portal.nsf/index_en
印度 Atomic Energy Regulatory board (AERB) (原子能管制局)	http://www.aerb.gov.in/
日本 原子力委員會	http://aec.jst.go.jp/
韓國 MOST (Ministry of Science & Technology) 負責核能研發及安全管制、核照之機關	http://www.most.go.kr/
立陶宛 VATESI (Lithuanian State Nuclear Safety Inspectorate) 立陶宛核能安全檢查署	http://www.vatesi.lt/
俄羅斯 Gosatomnadzor (GAN, Nuclear Safety Authority of Russia) 依據 1997 年 1 月 21 日原子能應用法，執行安全管制	http://www.gan.ru/
美國 US NRC (Nuclear Regulatory Commission) 核能管制委員會	http://www.nrc.gov/
NEI (Nuclear Energy Institute) 提供核能使用資訊	http://www.nei.org/

表 2.5：核安相關網站－國際組織、新聞與研討會、除污與除役

國際組織	
IAEA (國際原子能總署)	http://www.iaea.org/
Nuclear Energy Agency OECD (歐洲)核能總署 / 經濟合作發展組織	http://www.nea.fr/
International Nuclear Societies Council (INSC) (國際核能學會聯席會)	http://www.ne.jp/asahi/mh/u/
WENRA (西歐核安管制協會)	http://www.wenra.org/extra/pod/
新聞與研討會	
NucNet 世界核能新聞 (the World's Nuclear News Agency)	http://www.worldnuclear.org/
WNA (World Nuclear Association)	http://www.world-nuclear.org/index.htm
One Nuclear Place 核能資訊報導	http://www.1nuclearplace.com/
International Conference on Control and Management of Inadvertent Radioactive Material in Scrap Metal 2009 年 2 月 23 至 27 日於西班牙 Tarragona 舉行輻射廢金屬管制研討會	http://agora-ice.urv.es/scrap_conference2009/
除污與除役	
Nuclear Energy Agency, OECD (歐洲)核能總署 / 經濟合作發展組織	http://www.nea.fr/
CND (Co-ordination Network on Decommissioning of Nuclear Installations) 歐盟核設施除役研究計畫	http://ec-cnd.net/?Sid=cdbf56124777a4613c49e32be79f9361

(三) 核安相關標準

1. 10 CFR 73.54

10 CFR 73.54 "Protection of Digital Computers and Communications Systems and Networks"，此一聯邦法規 (Code of Federal Regulations, CFR)，提供 NRC 持照者 (Licensee) 更高的保證，避免此一標準中所規範的核能設施之數位電腦、通訊系統和網路受到網路攻擊 (Cyber Attack)。

避免網路攻擊的功能分類如下，如修改、破壞、資料或軟體的真確性或機密性的妥協、拒絕存取系統、服務或資料和影響系統運

作、網路以及相關設備。

2. RG 5.71

RG 5.71 “Cyber Security Programs for Nuclear Facilities” 為美國核能管制委員會所制定，提供核能工作人員一個可以保護數位電腦、通訊系統和網路所遵守的規定。一般性的法規要求，於 10 CFR 73.54 中列出。因為必須要有一個網路安全計畫 (Cyber Security Plan)，說明持照者如何去實施 10 CFR 73.54 並且取得更高的保證，避免自身應用系統受到網路攻擊。

網路安全計畫必須包含以下項目：

(1) 提供系統更高的安全保護。

(2) 保護系統和網路受到網路攻擊。

(3) 確認系統的保護範圍。

(4) 建立、實施和維護網路安全計畫。

(5) 公司網路安全計畫到實體的網路安全計畫。

(6) 安全的控制使用和如何保護公司資產。

(7) 縱深防禦的保護策略，有關網路攻擊的保護、偵測和系統恢復，減輕網路攻擊所帶來的衝擊。

(8) 安全意識和培訓。

(9) 當安全攻擊發生時的評估和管理，攻擊事件回應、恢復。

(10)控制使用的配置管理和內部設計控制流程。

(11)記錄和技術文件。

3. CIP

NERC Critical Infrastructure Protection (CIP) 為北美電力可靠度

委員會 (North American Electric Reliability Council, NERC) 發行之 NERC 網路安全 (Cyber Security) 的關鍵基礎建設防護 (Critical Infrastructure Protection, CIP) 標準系列：CIP-002 至 CIP-009，2009 年 12 月 16 日發行之第三版是目前（2010 年 11 月）的最新版本。

(1) CIP-002-3 重要數位資產之鑑別 (Critical Cyber Asset Identification)：支援電力系統可靠維運的重要資產，其相關之網路資產必須鑑別並撰寫於文件。

(2) CIP-003-3 安全管理控制項 (Security Management Controls)：負責的個體必須維持保護重要網路資產的最低安全管理控制項。

(3) CIP-004-3 人員與訓練 (Personnel & Training)：對於被授權進出網路或實體空間進行重要網際空間資產存取的人員，必須有適當的風險評估、訓練和安全認知。

(4) CIP-005-3 電子安全邊界 (Electronic Security Perimeter)：涵蓋重要網路資產的電子邊界及其上所有存取入口都必須有安全防護措施。

(5) CIP-006-3 重要數位資產的實體安全 (Physical Security of Critical Cyber Assets)：確保具備保護重要網路資產的實體安全方案。

(6) CIP-007-3 系統安全管理 (Systems Security Management)：負責的個體應定義方法、程序、步驟來保護重要網路資產之相關系統。

(7) CIP-008-3 事故報告與應變規劃 (Incident Reporting and Response Planning)：確保與重要網路資產相關的安全事故被鑑別、分類、處置及報告。

(8) CIP-009-3 重要數位資產的回復計畫 (Recovery Plans for Critical Cyber Assets)：確保重要網路資產具有適當的恢復計畫，且這些計畫依循業務永續與災難回復的技術與實務作法。

4. NEI

1994 年 3 月 16 日美國核能協會 (Nuclear Energy Institute, NEI) 正式成立，由美國四大核能專業法人合併而成立，包括美國核能委員會 (American Nuclear Energy Council, ANEC)（主理政府事務）、核子管理與資源委員會 (Nuclear Utility Management and Resources Council, NUMARC)（主理法規與技術事務）、美國能源覺醒委員會 (U.S. Council for Energy Awareness, USCEA)（主理能源溝通）及愛迪生電力研究所 (Edison Electric Institute, EEI)（主理出版）。其宗旨為結合核能工業界之專長與力量，積極參與美國乃至全球之核能政策訂定，期能促進核能及其技術之廣泛應用。NEI 目前有近 280 個來自美國及全球各地 15 個國家之團體會員，主要成員為美國及國際核電公司、核電廠之設計工程公司、核燃料公司、核子醫學與工業應用公司、放射性核種與製藥公司、學術研究機構、勞工團體等，為美國目前最大民間核能團體。

(1) NEI 04-04

NEI 04-04 提供了一種分級方法，基於數位資產的風險作業研究。結構化的過程是用來識別需要保護的關鍵數位資產防止網路攻擊，並考慮到後果，確定風險的敏感性。主要內容包含以下幾點：

- 角色和責任
- 政策和程序

- 訓練和提高相關意識
- 網路安全防禦對策
- 組態管理
- 減輕風險
- 事件回應和恢復
- 評估

(2) NEI 08-09

每一個核電廠需要遵守網路安全計畫 (Cyber Security Plan) 和實施時間表，而 NEI 08-09 是工業範本用於發展以及建立網路安全計畫。

(四) DI&C-ISG-04 適用性評估

DI&C-ISG-04 (Interim Staff Guidance Associated with Digital Instrumentation & Controls) 是由核能管制委員會任務工作小組 4 (Task Working Group #4) 等所制定出來的指導方針，該份文件被用來評估人員有無達到 NRC 的需求、應用數位系統設計是否與數位儀控系統設計的高度整合控制室 (Highly-Integrated Control Room, HICR) 指導方針一致，並且主要針對安全區域 (Safety Division) 之間以及安全和非安全區域 (Nonsafety Division) 的互動，對於數位儀控系統設計的 HICR 提供可接受的方法。

任務工作小組 4 定義了 HICR 是由下列四個基本的感興趣區域所組成：

1. 跨區通訊 (Interdivisional Communications)：在不同的安全區域之間或是在安全區域和非安全設備之間的通訊。

2. 命令優先權 (Command Prioritization)：當多個互相衝突的命令存在時，要送給致動器 (Actuator) 之特定命令的選擇。
3. 多區域控制與顯示工作站 (Multidivisional Control and Display Stations)：操作工作站或是顯示器的使用，這些設備與多個安全區域以及（或是）安全和非安全功能有關。
4. 數位系統網路組態 (Digital System Network Configuration)：網路或是其他數位系統的互相連接可能會影響廠房安全或是廠房安全分析假設之符合性（安全區域之間或是安全與非安全區域之間的互相連接也必須滿足針對跨區通訊的指導方針）。

底下我們將針對「跨區通訊」之 20 項審查要點以及「命令優先權」之 10 項審查要點進行是否適用於龍門電廠數位儀控網路之適用性評估，至於「多區域控制與顯示工作站」這一項目則不在討論範圍，而「數位系統網路組態」項目之相關要求則包含在前兩項項目中。

在 DI&C-ISG-04 提供了 20 項區域間訊號傳輸的準則，可用來核對系統和軟體組態。以下列出這 20 項的簡述，並評估其適用性：

1. （適用）安全通道不應該依賴來自本身安全區域之外的資訊。
2. （適用）每一個安全通道的安全功能應該要避免來自該區域外的影響，來自該區域外的資訊和訊號必須無法抑制或延遲其安全功能。
3. （適用）安全通道不應該接收任何來自其本身安全區域外的任何通訊，除非該通訊有支援或加強該安全功能的效能。
4. （適用）通訊程序本身必須由通訊處理器 (Communications Processor) 執行，此通訊處理器與執行安全功能的處理器分

開，如此一來當通訊發生錯誤或失效時就不會干擾到安全功能的執行。

5. （適用）安全功能處理器 (Safety Function Processor) 的週期時間 (Cycle Time) 應該要考量每次存取共享記憶體時，最長的可能完成時間。
6. （適用）安全功能處理器不應該執行通訊交握 (Communication Handshaking)，也不該接受任何來自自身安全區域外的中斷 (Interrupts)。
7. （適用）只有預先定義的資料集可以被接收端系統所使用；未被識別的訊息和資料應該要被接收端系統識別，並且根據事先指定的設計需求去處理，而且不允許被安全功能處理器裡的安全邏輯所使用。
8. （適用）在備援的安全區域之間或是安全與非安全區域之間進行資料交換時，不應該影響送出方、接收方或其他獨立區域的安全功能。
9. （適用）接收的訊息資料應該被儲存在共享記憶體以及與功能處理器相關的記憶體中，而且是在記憶體中事先決定的固定位置，這些記憶體位置不該被其他目的所使用。
10. （不適用）當安全區域在運作時，安全區域軟體 (Safety Division Software) 必須避免被變更，利用硬接線的 Interlock 或是經由維護與監控設備的實體斷線來避免線上 (On-line) 改變安全系統軟體。

    不適用原因：理由為龍門電廠安全網路相關設備，並不允許（線上）更新軟體，所有軟體的變動，皆必須等設備下線後，

以單機、離線之方式進行軟體之更新，待單機測試正確無誤後，才會再度上線。

11.（不適用）跨區通訊應該避免送出軟體指令給安全功能處理器，除非所有和該處理器有關的安全功能被繞過或是沒有在提供服務，而且安全功能處理器處理指令序列的過程不該被來自其區域外的任何訊息所影響。

不適用原因：理由為龍門電廠之數位儀控安全網路在任何情況下，都是不允許跨區控制的。

12.（適用）通訊錯誤不該影響所需安全性功能的運作。

13.（適用、應修改）理由為龍門電廠之數位儀控安全網路只做錯誤偵測 (Error Detection)，而不做錯誤修正 (Error Correction)，因為錯誤修正功能會增加訊息長度與處理時間。

14.（適用）極重要通訊應該要以專屬的媒體 (Dedicated Medium) 進行點對點通訊。

15.（適用）不論資料是否改變，安全功能的通訊應該是以規律間隔在固定的資料集（狀態）中通訊。

16.（適用、應修改）理由為在存活性部分，死結可以用 Watchdog 等機制來偵測，而活結部分則不知有何較有效的方法來偵測。（註：RPS 為 NUMAC 使用之通訊協定，ESFAS 為 DRS 使用之通訊協定。）

17.（適用）依據 “10 C.F.R. § 50.49”，在極重要通訊通道中所使用的媒體應該要符合事前正常和災害事後的環境。

18.（適用、應修改）理由為此部分與危害控制有關，應檢視相關規定後，再對此要點進行修正。

19.（適用）如果資料速率超過通訊連結或是節點能負擔的能力範圍，該系統會造成壅塞，因此所有的節點和連結應該要有足夠的能力支援所有功能。

20.（適用）安全系統回應時間的計算應該假設資料錯誤率 (Data Error Rate) 比設計基準錯誤率 (Design Basis Error Rate) 還要大，而資料錯誤率由設計和測試中所觀察到的錯誤率所提供。

優先權模組 (Priority Module) 可能是優先權裝置 (Prioritization Device) 或是軟體功能區塊 (Software Function Block)，它會接收來自多個安全和非安全的驅動命令 (Actuation Commands)，然後送出優先權最高的命令給被驅動的裝置。以下列出這 10 項的簡述，並評估其適用性：

1. （適用）優先權模組是與安全相關的裝置或是軟體功能，並且一定要符合所有在“10 CFR Part 50, Appendix A and B”的需求。
2. （適用）用於多樣化驅動器訊號 (Actuation Signals) 的優先權模組應該要跟其他數位系統互相獨立，並且不受其他數位系統的狀態和條件所影響。
3. （適用）安全相關的命令必須總是有最高的優先權而且能覆蓋其他命令。如果該命令是來自安全相關通道 (Safety-related Channel)，但只有取消安全狀態或不直接支援安全功能，則該命令擁有較低的優先權，可能會被其他命令所覆蓋。
4. （適用）優先權模組可能控制一個或是多個元件，如果優先權模組控制一個以上元件，則這些命令應用於每一個被驅動的元件。

5. （適用）每個優先權模組的獨立通訊應該要如同這份文件中的跨區通訊 (Interdivisional Communications) 所述相同。
6. （適用）優先權模組中用來設計、測試和維護的軟體應該要遵守所有在 “Regulatory Guide 1.152” 中的應用準則。
7. （適用）任何在優先權模組中用來支援安全功能的軟體程式，皆屬於安全相關軟體。
8. （適用、應修改）理由為要進行所有輸入值的完整測試在實際執行上會有困難，一方面是如何定義所有的輸入值，一方面是如何證明所有可能的輸入值皆已列入測試。
9. （適用）優先權模組的自動化測試不應該禁止模組的安全功能。如果自動化測試軟體失敗使得安全功能無效，則可能會導致常見的失敗 (Common-cause Failure)。
10. （適用）優先權模組必須確保定義在 “IEEE Standard 603” 的防護動作都有被完成，也就是避免被來自該模組所處安全區域外的命令、條件和錯誤所中斷。

經由考量龍門電廠數位儀控網路之架構，以及檢視 DI&C-ISG-04 之規範，在「跨區通訊」之 20 項審查要點中，有 15 項被評估為「適用」，有 2 項被評估為「不適用」，有 3 項被評估為「應修改」；而在「命令優先權」之 10 項審查要點中，有 9 項被評估為「適用」，有 1 項被評估為「應修改」，並沒有被評估為「不適用」的項目。這些適用與修改後之準則，可提供龍門電廠制定數位儀控系統 HICR 指導方針之參考。

二、RG 5.71 探討

在本小節中，我們針對法規指引 RG 5.71 進行研讀，並簡介說明如下。

(一) 緒論 (Introduction)

10 CFR 73.54 (Title 10, of the Code of Federal Regulations, Section 73.54)「數位電腦及通訊系統網路的保護」(Protection of Digital Computer and Communication Systems and Networks) 要求美國核能管制委員會 (Nuclear Regulatory Commission, NRC) 持照者，提供數位電腦及通訊系統網路合適的保護，並且包含 10 CFR 73.1「目標與範圍」的基礎設計威脅 (Design-basis Threat, DBT)。

10 CFR 73.54(a)(1)要求持照廠商保護數位電腦及通訊系統網路，避免被 10 CFR 73.54(a)(2)中所識別出來的攻擊威脅，10 CFR 73.54(a)(2)所識別出來的威脅分別為下列四種：

- 安全相關及重要的安全功能
- 安全功能
- 緊急準備功能，包含異地通訊
- 支援可能因洩漏而對安全或緊急準備造成影響的系統及設備

(二) 討論 (Discussion)

核能電廠持照廠商的實體保護計畫必須遵守在 10 CFR 73.55 中所描述的績效目標及需求，而 10 CFR 73.55(b)(8)要求持照者必須根據 10 CFR 73.54 來建立、維持及實行網路安全計畫。持照者被要求透過實體保護計畫以及安全組織的建立和維護，來保護在 10 CFR 73.54(a)(1)所識別的系統。而這個安全組織的目標是對於包含特殊

核能原料的活動提供下列兩點高度保證：

- 不會有害於一般防護與安全性 (Security)。
- 不會對大眾健康及安全 (Safety) 構成不合理的風險。

為了因應2001年所發生的911事件執法和情報機構所提供的資訊，NRC 在 2002 年發布 NRC Order EA-02-026「核能電廠的臨時保護措施及安全補償方法」，提出當時的環境威脅，並且要求持照者提出網路安全的弱點。接著 2003 年 NRC 發布 EA-03-086「放射性破壞的設計基礎威脅」，補充 10 CFR 73.1 對核能電廠所描述的設計基礎威脅，其中有些部分需要持照者提供額外的網路攻擊特性。

此外，由於核電廠數位科技的使用增加，所以需要識別潛在網路安全相關議題，因此 NRC 發布 NUREG/CR-6847「美國核能電廠自我評估網路安全的方法」，使用此法令及在開發時的觀察，NEI 發展出 NEI 04-04「動力反應器的網路安全計畫」，提供核能電廠反應器持照者開發及維護網路安全計畫。雖然 NUREG/CR-6847 提供持照者有用的資訊以開發臨時網路安全計畫，但是未提供一套遵守 10 CFR 73.54 需求的方法，反觀在 10 CFR 73.54 範圍內的系統，RG 5.71 透過使用 NIST SP 800-53 第三版「對聯邦資訊系統的安全控制措施建議」，提供全面性的方法來遵守 10 CFR 73.54 的網路安全。RG 1.152 提供設計、開發及保護方法的實行給採用數位儀控安全應用的核能電廠持照者的保護機制，其修訂第二版的 2.1-2.9 是用來作為執照變更、設計憑證或營運執照的依據，而這所提出在安全系統內的方法實行方面並沒有涵蓋到 IEEE Standard 7-4.3.2-2003。任何數位安全系統的新增、修改或者是新的反應器安全系統的任何執照，皆要透過執照變更要求、設計憑證或 COL 的審核，假設持照者

選擇透過使用設計特徵來提出 10 CFR 73.54，之後詳述打算滿足 10 CFR 73.54 規範的安全系統的任何設計特徵，則必須要提出部分的執照變更需求、設計認證申請或營運執照來做審核及批准。在一些個案中，NRC 將只審查這些與系統安全功能相關的特徵，來確保安全系統的可靠度並不受納入這些安全特徵所影響。

2007 年 NRC 發布 BTP 7-14 的修訂第五版「以數位電腦為基礎的儀表和控制系統在評論上的指導」，提供對於核能電廠評估軟體生命週期流程結合安全相關的數位儀控系統的查核準則，也提出一個可接受軟體管理計畫應有的特徵。

10 CFR 73.55(b)中，委員會建立對於核能電廠反應器設備的實體防禦計畫的要求，包含對於偵測、評估、阻斷和消除有效放射性破壞的設計基礎威脅的績效準則。

NIST SP 800-53 修訂第三版「對於聯邦的資訊系統所推薦的安全控制」及 NIST SP 800-82「工業控制系統指南」，這兩個是基於容易理解的網路威脅、風險及弱點，再加上同樣是易懂的因應對策和保護技術。而 NIST 針對在工業控制系統環境中的使用，包括資訊系統/工業控制系統的結合以開創考慮這些安全控制的應用需求的一般工業控制系統環境。

RG 5.71 將前面所提到的安全控制分為三類：技術、操作及環境。NRC 透過修改 NIST SP 800-82 所提出的「高度影響」的安全控制來發展 RG5.71 以提供遵守 10 CFR 73.54 的方法。RG 5.71 描述一個提供防禦性策略的管理措施，包含根據 SP 800-53 及 800-82 所提出的架構及安全機制，也涵蓋一些標準組織機構的發現，包括國際自動化學會、IEEE、NIST 及美國國土安全部 (DHS) 的準則。RG

5.71 提供框架以幫助識別出免受網路攻擊的數位資產，這些被識別出來的資產又被稱為關鍵數位資產 (Critical Digital Asset, CDA)，持照者應該透過應用這份法規指引所提到之防禦架構和各項安全控制項目來找出 CDA 潛在的安全風險。RG 5.71 的目標是在協調提出 CDA 的潛在風險的安全控制，以提供讓持照者能建立、維護及成功地將安全控制整合至安全計畫的彈性方法。

(三) 法規觀點 (Regulatory Position)

第 C.1 節提供與網路安全相關的管理需求；第 C.2 節介紹計畫元素，對遵守 10 CFR 73.54 規範的安全開發計畫提供方法，這份安全計畫描述方法及管理程序以保證這計畫相關記錄以及實行的政策和程序，而計畫的修改必須按照 10 CFR 50.54(p)處理，在實行前持照者必須提交減少計畫效能的改變給 NRC 批准。

安全計畫必須描述下列要素：

- 持照者如何對電腦通訊系統及網路遠離網路攻擊提供高度保證，包括 10 CFR 73.1 中描述的設計基礎威脅
- 持照者如何保護電腦系統及網路遠離網路攻擊，這些攻擊可能會有下列影響：
  - 資料的機密性及真確性
  - 系統服務的可取用性
  - 系統及相關的設備運作
- 識別範圍內關鍵數位資產的方法
- 持照者如何建立、實行及維護它的安全計畫
- 持照者如何將網路安全計畫納入實體安全計畫中
- 所使用的安全控制及他們如何保護 10 CFR 73.54(b)(1)識別出來

的資產

- 深度防禦措施以及這些措施如何用來保護、偵測、回應以及復原網路攻擊
- 被設計來減輕網路攻擊負面影響之網路安全計畫元素
- 如何設計網路安全計畫以確保從 10 CFR 73.54(b)(1)中所識別出來被保護的資產功能並沒有受到網路攻擊而有不良影響
- 網路安全意識及訓練計畫如何提供在必要的訓練以執行所賦予的職責
- 持照者所使用去評估及管理網路安全風險的步驟
- 用在組態管理及設計控制步驟的控制以確保：
  - 工廠資產的修改和新設備的增加不會對網路安全造成負面影響
  - 網路安全議題透過系統設計的生命週期來提出
  - RG 1.152 第二版修訂版對於安全系統設計及開發流程提供額外的指導
- 特別的地點條件 (Site-specific Conditions) 如何影響網路安全計畫的實行
- 對於網路攻擊的事件回應及復原方法，包括描述持照者如何達到：
  - 維持對網路攻擊的即時偵測及回復能力
  - 降低網路攻擊的後果
  - 修補被利用的弱點
  - 修復被網路攻擊的系統、網路和設備
- 具體的網路安全政策及流程

- 如何根據包含週期性需求的 10 CFR 73.55(m)，將網路安全計畫評論為實體安全計畫的元件
- 持照者如何管理所有記錄和支援技術文件，以滿足 10 CFR 73.54(h)所提出的安全需求

(四) 附錄 A、通用網路安全計畫樣版 (Generic Cyber Security Plan Template)

A.1 簡介

描述對於 10 CFR 73.54 的需求如何被實施來保護數位電腦、通訊系統與網路以防止在 10 CFR 73.1 中所描述之網路攻擊。

如同 10 CFR 73.54(e)和 10 CFR 73.55(c)(6)所要求，持照者/申請者需要建立、實施與維護網路安全計畫。本計畫的實施並沒有減輕持照者/申請者對於 NRC 其餘規則的責任。

（註：本報告第貳章第二節中皆以「本計畫」來稱呼「本網路安全計畫」。）

A.2 網路安全計畫

A.2.1 範圍與目標

範圍：對於關鍵數位資產的安全與緊急準備 (SSEP) 功能。

目標：實施與文件化下列行為，以保護系統與 SSEP 功能免於數位攻擊的關連性。

- RG 5.71 第 3.3 節說明－安全控制。
- RG 5.71 第 4 章說明－網路安全計畫。

A.2.2 以績效為基礎的需求

如同 10 CFR 73.55(a)(1)所要求，持照者必須經由被委員會批准的實體安全計畫、訓練與資格計畫、保障措施持續計畫與網路安全計畫，以實施此小節的要求。

如同 10 CFR 73.54(b)(3)所定義，網路安全為實體安全計畫的一部分。

A.3 網路安全計畫實施

符合 10 CFR 73.54(b)(2) 與 10 CFR 73.55(b)(8)的要求，建立與實施防禦策略：

- 與 RG 5.71 第 3.1.5 節所描述之防禦模型一致
- 包括 RG 5.71 第 3.1、3.2、3.3 節所描述之安全控制

維持計畫，如同 RG 5.71 第 4 章所描述。

可取得每一項 CDA 之安全控制文件，以供檢查。對於網路安全計畫的修改描述於 10 CFR 50.54(p)，提交修改給 NRC 以供審查。報告任何於電廠中的數位攻擊或意外給 NRC，如同 10 CFR 73.71 與 10 CFR Part 73 之 Appendix G 所要求。

A.3.1 分析數位電腦系統

A.3.1.1 安全評估與授權

申請者/持照者須年度發展與檢查更新項目如下：

- 須有一正式文件化安全計畫、評估與授權政策。
- 須有一正式文件化程序以促進網路安全計畫與安全評估的實施。

A.3.1.2 網路安全小組

網路安全小組 (Cyber Security Team, CST) 由各種廣泛的知識人員組成：

- 資訊與數位系統技術。
- 核能設施運作、工程與安全。
- 實體安全與緊急準備。

CST 的責任與角色包含下列：

- 執行或監督數位安全管理程序的每一個步驟。
- 對於所有的關鍵觀察記錄進行文件化，分析與搜尋於評估程序，使之能夠在應用於安全控制時使用。
- 重新評估與假設於近期內的數位安全威脅；潛在的弱點與攻擊；有效的數位安全控制與防禦策略、減緩攻擊法與對於員工的數位安全宣傳跟訓練；CDA 與數位安全控制於系統生命週期中。
- 於檢查時確認資訊並重新審查，透過綜合且全面的 CDA 與連接數位資產與數位安全控制有關係之項目、包含全面檢查實體與電子驗證行為。
- 確認與實施潛在新的數位安全控制。
- 準備文件化與監督實施於 RG 5.71 附錄 B 與 C 中提供之網路安全控制，對於未實施的特定 RG 5.71 附錄 B 中提供之網路安全控制項目建立基礎之文件說明，或是對於 RG 5.71 附錄 B 中提供之網路安全控制實施替代方案的項目建立基礎之文件說明。
- 確保所有評估文件，包含記錄與協助資訊，根據 10 CFR 73.55(q)

與保留指定的記錄之要求於本計畫第 5 章中說明。

A.3.1.3 識別關鍵數位資產

識別 CDA 與 CST：

- 透過 SSEP 功能：電廠系統、設備、通訊系統與網路、協助系統。
- 透過關鍵系統 (Critical System, CS)：初步結果進行分析、相關性與路徑之分析。
- 識別與文件化於 CS 特有功能有直接、協助或間接角色之 CDA。

對每一個 CS 進行檢查，申請者/持照者需要文件化下列內容：

- 對於各系統資產或網路識別為 CDA 的描述。
- 識別各 CS 中的 CDA。
- 簡單描述 CDA 所提供的功能。
- 安全功能需求或特定項目包含：安全組態、安裝與 CDA 運作的效率、維護於安全特性與功能。

A.3.1.4 審查與驗證測試

持照者/申請者的 CST 對每一個 CDA 進行審查與驗證活動：

- 直接或間接的連接路徑。
- 基礎設施的相互依存關係。
- 防禦措施的應用：防禦模組、安全控制、防禦測量。

CST 透過下列來全面審查上述行為：

- 對於每一個 CDA 的連接與組態進行實體檢驗。
- 檢驗組態與檢驗通訊路徑中的安全控制的有效性。

- 檢測實體安全建立以保護每一個 CDA 與通訊路徑。
- 檢測 CS 與 CDA 的之間的相互依存關係，並信任之。
- 檢測基礎系統、備用的電力、環境控制與滅火設備之相互依存關係。
- 檢測系統、網路、通訊系統與網路於電廠中可用，包含潛在的攻擊路徑。
- 解決 CDA 與 CS 之資訊與組態描述之識別於審查時或其他數位安全沒有相關的 CDA。

A.3.1.5 深度防禦對策

持照者/申請者實施、文件化與維護深度防禦策略，以維持 CDA 受到數位攻擊的偵測、回應與復原能力。

防禦策略根據底下項目：

- 安全控制（本計畫第 3.1 節）。
- 防禦模組（RG 5.71 第 3.2 節）。
- 深度防禦（RG 5.71 附錄 C 第 6 節）。
- 詳細的防禦架構（RG 5.71 附錄 C 第 7 節）。
- 維護網路安全計畫（RG 5.71 附錄 A 第 4 節）。

A.3.1.6 安全控制的應用

持照者/申請者建立深度防禦策略，透過實施與文件化下列程序：

- 防禦策略（RG 5.71 第 3.2 節）。
- 實體與管理性的安全控制。
- 運作與管理控制（RG 5.71 附錄 C）與驗證 CDA 的有效性。

- 技術控制（RG 5.71 附錄 B）。

遵守技術安全控制：持照者/申請者使用本計畫第 3.1.4 節所描述於此計畫中的資訊收集，以進行一或多個行為如下述：

- 對於所有安全控制的實施描述於附錄 B 中。
- 對於無法被實施的安全控制，須實施替代的控制措施。
- 非實施的安全控制描述於附錄 B 中。

當控制措施會對於 SSEP 功能有不利影響時，持照者/申請者不能應用的安全控制，須使用替代的控制措施。

持照者/申請者施行下列：有效的分析（本計畫第 4.1.2 節）、弱點評估與掃描（本計畫第 4.1.3 節）。

A.3.2 結合網路安全計畫至實體保護計畫中

實體安全計畫的第二十三章引用廠區的網路安全計畫，根據 10 CFR 73.54(b)(3)、10 CFR 73.55(a)(1)和 10 CFR 73.55(c)(6))。

考量到發展與識別目標過程中的數位攻擊描述於實體安全計畫與 10 CFR 73.55(f)(2)。

持照者/申請者結合管理實體與數位安全如下：

- 建立一個統一的安全組織，包含數位與實體安全，並且從一般運作中獨立出來。
- 文件化實體與數位安全之相互依存關係。
- 發展政策與程序以整合統一管理實體與數位安全控制措施。
- 納入統一的政策與程序，以保護 CDA 免於攻擊。
- 協調實體或數位安全服務、訓練、裝置與設備。

- 協調實體與網路安全降為與訓練的相互依存關係。
- 結合與協調事件反應能力與實體、數位安全的意外事件。
- 訓練高級管理人員。
- 定期訓練整體組織的安全知識。

A.3.3 政策與實施程序

持照者/申請者發展政策與實施程序以滿足安全控制目標，描述於 RG 5.71 附錄 B 與 C 中。

負責實施與監督此計畫之人員要向核電廠主管、核電廠運作主管、核電廠運作副總經理或副總經理回報。

持照者/申請者程序與建立特定的責任，描述於 RG 5.71 附錄 C 第 10.10 節中。

A.4 維護網路安全計畫

說明維護關鍵數位資產的必要安全規定，讓 CDA 於 SSEP 方面能夠有充分的保護。

- 本計畫第 4.1 節說明持續監測與評估、安全控制的建立、實施，確保有達成維護資訊資產的目標。
- 本計畫第 4.2 節說明對於新增、刪除、修改的規則。
- 本計畫第 4.3 節說明網路安全計畫的審查。

A.4.1 持續監測與評估

持照者/申請者採用與 RG 5.71 附錄 C 相符的控制方法，可使用自動化工具協助，以即時管理對於 CDA 的數位安全，持續監測程序包括下列：

- 適當的使用自動化的協助工具，並達成對 CDA 的即時安全管理，確保在每個 CDA 中都有確實實施安全控制。
- 確保 Rogue Asset（可能對其他資產造成危害的或是產生弱點的資產）沒有與基礎建設相互連接。
- 在 RG 5.71 附錄 B 與 C 提出定期評估與有效的安全控制，並且定期進行安全審查程序，這些程序項目與達成關鍵數位資產管理組態變革相互支援。
- 需要定期更新資訊安全計畫。

這些程序元素相互協助，以對於改變 CDA 的管理組態變革，持續監測需要更新至網路安全計畫中。

A.4.1.1 定期評估安全控制

至少每年要進行關鍵數位資產的安全評估，確保資產的強度、彈性與效率，如同 RG 5.71 附錄 B 與 C 的描述。

A.4.1.2 效能分析

網路安全小組 (Cyber Security Team, CST) 確保安全程序與安全控制有確實被實施與運作，持續提升對 CDA 受到資訊攻擊的保護，其中也包含設計基準威脅 (DBT) 審查安全程序

- 增加網路安全計畫的效率與表現。
- 管理與評估風險。
- 加強實施安全控制的效用。
- 確認新的安全控制是否為保護 CDA 所需要的。
- 驗證已存在的安全控制與程序先後順序，並有效的保護 CDA 免

於數位攻擊。

- 促進糾正那些被發現含有缺陷的安全方案。

CST 要審查維護的記錄，確保 CDA 具有製造商所建議的安全功能。

A.4.1.3 弱點評估與掃描

掃描次數不能少於 RG 5.71 附錄 B、C 所規定的每季一次，並且需使用最新的弱點掃描技術，促進互動性的工具與自動弱點管理程序；對脆弱性評估進行分析，記錄掃描報告與位址。

掃描行為不能對 SSEP 產生不良的影響，且於進行掃描時要有備援方案（如提供一個可取代性的系統或是關鍵資產去掃描）。

A.4.2 改變控制措施

在進行更改的時候要確保安全機制仍然有效，並且任何可能有被攻擊的弱點與路徑都要被保護。

A.4.2.1 組態管理

組態管理的控制措施描述於 RG 5.71 附錄 C 第 11 節。

維持資訊安全的目標在 10 CFR 43.54(a)(1)中描述。

於 CDA 的生命週期中的運轉於維持步驟中，持照者/申請者確保能夠透過組態管理程序來掌控改變的動作，來避免系統額外的弱點或風險。這些程序同時也確認對於每一個 RG 5.71 附錄 B 與 C 中提的安全控制時間性與應用效率。

A.4.2.2 環境變化對於安全影響的分析

持照者/申請者的 CST 需要評估、文件化與納入安全衝擊分析對於 CDA 或系統之間的安全性，需要更新與文件化項目如下：

- 確保 CDA 的位置與（直接或間接）連結的資產。
- 連結路徑（直接或間接）。
- 基礎設施的互相依存關係。
- 應用的防禦策略。
- 整個廠區的實體與虛擬安全政策與防範對於 CDA 的攻擊，同時也要考量再受到攻擊後要如何反應與恢復。

持照者/申請者管理 CDA 於 SSEP 功能中的數位安全，透過持續評估威脅與弱點於應用在每個安全控制提供上（如 RG 5.71 附錄 B 與 C 於生命周期中每一個步驟所述）。另外，持照者/申請者需要建立與文件化對於篩選、評估與舒緩威脅與弱點之通知，此通知來自於可信來源。

A.4.2.3 安全重新評估與授權

當 CDA 有修改時，持照者/申請者需要公布、審查與更新下列事項：

- 一個正式、文件化的安全評估授權政策。
- 一個正式、文件化的程序，以便實施安全重新評估、授權政策與相關的控制措施。

A.4.2.4 更新網路安全的做法

當 CDA 或環境有變更時，持照者/申請者的 CST 需要審查、更

新與修改電廠的數位安全政策、程序、訓練、數位安全控制、對於網路架構的詳細描述（包含邏輯層與實體層）、安全設備資訊與任何其他與安全程序或安全控制有關的狀態（如 RG 5.71 附錄 B、C）資訊包含如下：

- 電廠與組織範圍資訊之政策、程序與近期演練的數位安全項目。
- 詳細的網路架構與圖形。
- 對於安全設備與 CDA 的組態資訊。
- 新的電廠或是組織範圍的資訊安全防禦策略，或是安全控制措施需要被制定，與政策、程序、行為與技術相關的部屬。
- 廠區的實體與控制安全程序。
- 對於供應商與承包商的數位安全需求。
- 已識別的潛在攻擊路徑。
- 近期的數位安全調查文件。
- 確定基礎設施能夠在系統故障或可能影響正常運作的時候還能持續維持系統的安全功能。

A.4.2.5 修改或新增關鍵資訊資產時的審查和驗證測試

持照者的 CST 在對於 CDA 使用程序的修改或新增的審查結果與確認測試，實施與文件化在本計畫第 3.1.4 節中描述。

A.4.2.6 修改或新增時要應用的安全控制機制

當新的 CDA 引入到環境中：

- 部署 CDA 到適合的層級。
- 確認適用的技術控制。
- 確認目標與管理控制。

變更或修改 CDA：

- 分析安全影響。
- 確認安全控制措施。
- 確認目標與管理控制。

A.4.3 網路安全計畫審查

要依照 10 CFR 73.55(m)的要求，至少每 24 個月要審查一次，遵循原則如下：

- 實施後一開始要 12 個月內審查一次。
- 如果進行會影響到安全的變更也需要在 12 個月內審查一次。
- 當廠房分析、評估或其他效能指標有需要時。
- 審查人員必須獨立於負責計畫實施與管理的人員。

持照者需要將這些報告以可稽核的格式保存，且要可以審核，並且將計畫審查的發現輸入至修正行動計畫 (Corrective Action Program) 中。

A.5 文件控制和記錄保留與處理

所需的文件必須符合 10 CFR 73.54 與 10 CFR 73.55 的要求。

安全攻擊或其他安全相關事件的歷史記錄需要被保留。

這些記錄至少要保留三年直到被取代，除非另有規定。

(五) 附錄 B、技術性安全控制 (Technical Security Controls)

B.1 存取控制 (Access Control)

B.1.1 存取控制政策與程序 (Access Control Policy and Procedures)

持有執照者或申請人必須要每年審查和更新關鍵數位資產 (CDA) 的存取控制政策，要定義好目的、範圍以及角色，並且要開發正式文件化的程序。

存取控制政策的說明如下：

- 存取控制的權利 (Right)（個人和程序可以存取哪些資源）和權限 (Privilege)（這些個人和程序可以對這些資源做甚麼）。
- 關鍵數位資產的管理（建立、啟動、修改、審查、取消或者移除帳戶等等動作）。
- 保護資料庫的密碼金鑰來防止未授權的存取。
- 要每年對 CDA 進行審查，或者當人員職責與系統功能的配置有改變時，需要馬上審查。
- 職責區分（透過分配存取授權的方式）。

B.1.2 帳戶管理 (Account Management)

持有執照者或申請人必須要負責以下：

- 審查 CDA 帳戶要與存取控制列表提供的行動一致，並且要啟動所要求的動作。
- 要求存取控制的權利是基於工作的職務，並且當工作職能有改變時，就必須在進行審查的動作。
- 採用自動的機制來支援 CDA 帳戶管理的功能，像是關閉非活動的帳戶、建立和維護帳戶建立、刪除和修改的審查記錄等。

B.1.3 存取執行 (Access Enforcement)

持有執照者或申請人必須要負責以下：

- 授權人員存取權限功能與安全有關的訊息要符合既定的政策和程序。
- 定義和文件化與 CDA 有關的權限職務。
- 對關鍵權限職務和建立任何使用者的存取權限要求要有雙重授權。
- 當存取執行無法使用時，要有替代方案來執行安全存取控制。

B.1.4 資訊流的執行 (Information Flow Enforcement)

持有執照者或申請人必須要負責以下：

- 維護好文件，這些文件是說明在 CDA 和安全邊界設備所要求的授權等級會有哪些允許或不允許的資訊流。
- 實施即時的能力來偵測、阻止、防止和回應非合法或未授權的資訊流。
- 實施動態資訊流控制政策，允許或禁止那些不斷變化的情況或一些操作上的考量。

B.1.5 功能區分 (Separation of Functions)

持有執照者或申請人必須要負責以下：

- 建立和文件化部門的責任和職務，並且要排除利益上的衝突。
- 透過分配存取授權的方式來執行 CDA 的功能區分。
- 當 CDA 沒辦法支援不同權限時，要實施替代控制方案並且要符合正當的情況。

B.1.6 最小權限 (Least Privilege)

持有執照者或申請人必須要負責以下：

- 分配給使用者所需要的特別任務要有最嚴格的權利和權限設定。
- 當 CDA 沒辦法支援不同權限時，要實施替代控制方案並且要符合正當的情況。

B.1.7 不成功的登入嘗試 (Unsuccessful Login Attempts)

持有執照者或申請人必須要確保以下：

- 安全控制的實施要限制一個使用者的無效存取的次數，一個特定時間的登入失敗次數可能會因為 CDA 的不同而改變。
- 如果一個 CDA 因為對效能、安全或可靠性產生不良影響而導致無法執行帳戶，就應該要採用替代政策，例如可以即時記錄不成功的登入嘗試，或即時發出警報。

B.1.8 系統使用通知 (System Use Notification)

持有執照者或申請人必須要確保以下：

- 系統使用通知主要會顯示以下這些訊息，使用者正在存取一個受到限制的系統、系統會使用監測和記錄並且會接受審查、未經授權使用 CDA 是禁止的，並且會受到刑事和民事的處罰、CDA 的使用是同意進行監測和記錄的。
- CDA 系統使用通知訊息會提供隱私和安全公告。

B.1.9 前一次登入通知 (Previous Logon Notification)

持有執照者或申請人必須要負責以下：

- 成功登入之後，CDA 應該要顯示從上一次成功登入之後的最後登入的時間和日期以及不成功的登入嘗試次數。
- 要求所有的使用者要回報給網路安全管理者有哪些任何可疑的活動。

B.1.10 會談鎖定 (Session Lock)

設定 CDA 做到以下功能：

- 在三十分鐘未動作後，自動啟動會談鎖定。
- 為使用者提供可以直接啟動會談鎖定機制的能力。
- 維持一個 CDA 的會談鎖定直到使用者使用身分識別和驗證程序重新建立存取。

B.1.11 存取控制的監督和審查 (Supervision and Review—Access Control)

持有執照者或申請人必須要負責以下：

- 記錄、監督和審查關於使用者執行的存取控制的活動。
- 採用自動機制在 CDA 中，以支援和幫助審查使用者的活動。

B.1.12 未經過識別或驗證的可允許執行動作 (Permitted Actions without Identification or Authentication)

持有執照者或申請人必須要負責以下：

- 在正常或緊急而且未經識別或驗證的情況下，要確認和記錄特定使用者可以對 CDA 可以執行的動作。

- 只有在必要完成任務目標的情況下，才允許未經識別和驗證的情況下採取行動，當然要以不影響安全和緊急應變功能，並且要符合核能管制委員會的條例。

B.1.13 自動標記 (Automated Marking)

持有執照者或申請人必須要負責確保 CDA 的軟硬拷貝輸出要採用標準的命名方式來識別任何特殊的傳送、處理或者分佈指示等等，例如安全相關訊息。

B.1.14 自動標籤 (Automated Labeling)

持有執照者或申請人在儲存、處理以及傳輸的方面要標籤軟硬拷貝的輸出。

B.1.15 網路存取控制 (Network Access Control)

持有執照者或申請人要使用緩和技術來確保 CDA 的安全，可能是經由媒體存取控制鎖定、實體或電氣的隔離、加密或者監測等等。

B.1.16 開放與不安全協定的限制 ("Open/Insecure" Protocol Restrictions)

持有執照者或申請人必須要負責以下：

- 當協定缺乏安全控制時，要從一個未經授權的存取中實施額外的預防措施來保護網路和線路通信協定。
- 從啟動命令來終止這個協定，會改變 CDA 從安全的狀態變為不太安全的狀態。

B.1.17 無線存取限制 (Wireless Access Restrictions)

持有執照者或申請人必須要負責以下：

- 禁止在與 CDA 有安全和重要功能有關的地方使用無線技術。
- 要記錄、授權、監督和控制 CDA 的無線存取，確保無線存取的限制是與 RG 5.71 所描述的防禦策略是一致的。

B.1.18 不安全和惡意的連結 (Insecure and Rogue Connections)

當改變和修改 CDA 時，持有執照者或申請人要驗證在 CDA 的部屬過程，而驗證的頻率為一個月至少一次。

B.1.19 可攜式和移動式設備的存取控制 (Access Control for Portable and Mobile Devices)

持有執照者或申請人必須要負責以下：

- 建立和文件化使用的限制並且實施可攜式和移動式設備的指導方針。
- 執行和記錄移動式設備的安全性和完整性是維持在一個水平並且符合 CDA 所支援的。

B.1.20 專有協定的可視性 (Proprietary Protocol Visibility)

持有執照者或申請人要確保，當專有協定的建立缺乏可視性時，例如系統無法偵測到攻擊，就要實施替代控制或保護政策來保護 CDA 避免遭到網路攻擊和基礎設計威脅。

B.1.21 第三方產品和控制 (Third Party Products and Controls)

持有執照者或申請人要確保第三方產品和控制在以下情況：

- 因為廠商許可和服務協議，第三方安全解決方案是不被允許的。
- 如果第三方應用程序的安裝沒有經過廠商的核准，服務支援會發生損失。

B.1.22 外部系統的使用 (Use of External Systems)

持有執照者或申請人必須要負責以下：

- 確保外部系統不能被更高層級所存取。
- 禁止使用者從外部系統來存取 CDA 或處理、儲存、傳送組織控制的資訊。

B.1.23 可公開存取的內容 (Publicly Accessible Content)

持有執照者或申請人必須要負責以下：

- 授權指定的個人訊息要發佈到系統上，是要公開存取的。
- 確保那些可能會導致安全緊急應變功能產生不良影響或可能會協助攻擊者進行攻擊的訊息，不能被公開發佈。

B.2 稽核和可歸責性 (Audit and Accountability)

B.2.1 稽核和可歸責性的政策與程序 (Audit and Accountability Policy and Procedures)

持有執照者或申請人必須要每年稽核和更新稽核和可歸責性的政策，要定義好目的、範圍以及角色，並且要開發正式文件化的程序。

B.2.2 可稽核的事件 (Auditable Events)

持有執照者或申請人必須要負責以下：

- 與 CDA 有相關的事件的安全緊急應變功能需要被稽核。
- 要定義可稽核的事件的列表以及每個事件的稽核頻率。
- 要定期審查和更新可稽核的事件。
- 要以 RG 5.71 附錄 A 第 4.1.2 節為基礎，調整 CDA 中被稽核的事件的威脅訊息和效益分析。

B.2.3 稽核記錄的內容 (Content of Audit Records)

持有執照者或申請人必須要負責以下：

- 確保 CDA 所產生的稽核記錄要包含足夠的訊息，像是事件發生的時間、地點以及原因等等。
- 確保 CDA 可以提供額外更詳細的稽核記錄，像是稽核事件的類型、地點或主題等等。

B.2.4 稽核的儲存容量 (Audit Storage Capacity)

持有執照者或申請人分配稽核記錄的儲存容量，要滿足 NRC 的要求並且要配置好稽核來減少類似超過容量的情形發生。

B.2.5 稽核處理失敗的回應 (Response to Audit Processing Failures)

持有執照者或申請人必須要確保以下：

- 如果一個 CDA 或安全邊界設備之稽核處理失敗的話，就會發生：
  - ■ 發送給指定人員的事件處理警報的稽核處理會失敗。

- 稽核失敗會被當成是 CDA 或安全邊界設備的故障，而申請人要根據技術規範來採取行動。

- CDA 的稽核失敗應該要採取下列行動：
  - 關閉 CDA。
  - 停止產生稽核記錄。

B.2.6 稽核的審查、分析和報告 (Audit Review, Analysis, and Reporting)

持有執照者或申請人必須要負責以下：

- 要對那些標記為不正常的活動，進行審查和分析 CDA 的稽核記錄，一個月至少一次。
- 當有一個威脅或風險改變時，要以申請人或 NRC 所訂定安全緊急應變功能所信任的訊息為基礎，調整 CDA 稽核的審查、分析和報告。
- 在 CDA 採用自動機制來對惡意活動的調查和回應進行整合稽核審查、分析和報告。

B.2.7 稽核簡化和報告產生 (Audit Reduction and Report Generation)

持有執照者或申請人必須設定和部署 CDA 做到下列功能：

- 提供 CDA 稽核簡化和報告產生的能力。
- 提供對可選擇標準的事件有自動處理稽核記錄的能力。

B.2.8 時戳 (Time Stamps)

持有執照者或申請人從一個專用的資源來同步 CDA 的時間，

用來保護與 CDA 處於相同或更高層級的資源，像是現有的安全網路、直接或透過 SNTP 採用 CDA 以及管理信任金鑰的過程，當時間同步沒辦法使用在 CDA 時，要有替代控制方案來管理潛在的網路安全風險。

B.2.9 稽核資訊的保護 (Protection of Audit Information)

持有執照者或申請人必須要負責以下：

- 從未經授權的存取、修改和刪除的方式要符合 CDA 的來源，來保護稽核資訊和稽核工具。
- 確保所有的稽核資訊的保護是與該設備來源處於同一個層級。

B.2.10 不可否認性 (Nonrepudiation)

持有執照者或申請人要保護 CDA 和稽核記錄，來避免一個人進行了某些特別動作來否認他們過錯的情形發生。

B.2.11 稽核記錄的保存 (Audit Record Retention)

持有執照者或申請人要保留稽核記錄並要符合記錄保存所要求的存取授權方案，才可以提供安全事件的事後調查支援。

B.2.12 稽核的產生 (Audit Generation)

持有執照者或申請人的安全架構要提供以下：

- 對 CDA 可稽核事件要有審查記錄產生的能力。
- 對 CDA 已經選定的可稽核事件清單中要有產生稽核記錄的能力以及從不同 CDA 的元件中可以匯集稽核記錄的能力。

B.3 關鍵數位資產及通訊的保護 (Critical Digital Asset and Communications Protection)

B.3.1 關鍵數位資產及通訊的保護政策與程序 (Critical Digital Asset and Communications Protection Policy and Procedures)

CDA 系統和通訊的保護政策要文件化，包含處理的目的、範圍、角色、責任等等；程序要文件化以促進 CDA 系統和通訊的保護政策以及和 CDA 系統與通訊相關保護安全控制措施的實施。

B.3.2 應用程序分區和安全功能的獨立 (Application Partitioning and Security Function Isolation)

- 配置關鍵數位資產系統，以區分用戶的功能和關鍵數位資產管理的功能。
- 配置關鍵數位資產系統，從非安全性功能中區隔出安全性功能，如軟體、硬體、韌體存取的完整性。

B.3.3 共享資源 (Shared Resources)

配置 CDA 系統，以防止未經授權的資訊藉由共享系統資源來傳輸，並使用獨立的網路設備，以建立和維持第 3 層和第 4 層和其他所有層級彼此的邏輯分離。

B.3.4 阻斷服務的保護 (Denial of Service Protection)

- 配置 CDA 系統，來抵抗或減少 DoS 攻擊所造成的影響。
- 配置 CDA 系統，以限制使用者發動 DoS 攻擊的能力。

B.3.5 資源優先權 (Resource Priority)

持有執照者或申請人配置 CDA，藉由優先程度來限制資源的使用，防止優先程度低的流程被優先程度高的流程給延遲或是干擾。

B.3.6 傳輸完整性 (Transmission Integrity)

- 配置 CDA，以保護資訊傳輸的完整性。
- 使用加密機制，以確認資訊在傳輸及接收的過程中是否有改變，除非有其他替代的實體保護措施。
- 實施監測，以偵測出中間人 (Man-in-the-Middle, MITM) 攻擊和位址解析協定中毒 (Address Resolution Protocol (ARP) Poisoning)。

B.3.7 傳輸機密性 (Transmission Confidentiality)

- 配置 CDA，以保護資訊傳輸的機密性。
- 使用加密機制，以防止資訊在傳輸和接收當中未經授權而揭露，除非有其他替代的實體保護措施。

B.3.8 可信任的路徑 (Trusted Path)

持有執照者或申請人要配置 CDA，在用戶和 CDA 的安全功能之間使用可信任的通訊路徑，至少要包括身分驗證和重新驗證。

B.3.9 加密金鑰建立和管理 (Cryptographic Key Establishment and Management)

當加密技術是必要的而且在 CDA 內採用，持有執照者或申請人可以使用自動化的機制來管理加密金鑰，且該自動化機制可同時

支援手動程序。

B.3.10 密碼學使用 (Use of Cryptography)

持有執照者或申請人要配置 CDA 來實施加密機制，該機制要符合聯邦資訊處理標準 (Federal Information Processing Standards, FIPS) 140-2 加密模組安全需求 (Security Requirements for Cryptographic Modules)。

B.3.11 未授權遠端啟動服務 (Unauthorized Remote Activation of Services)

- 配置 CDA 以禁止遠端啟動協同運算機制，並提供本地使用者明確的指示。
- 配置 CDA 提供攝影機和麥克風實體斷線的方法，該方法需操作簡易，除非是為了安全目的用來控制和監測 CDA 的技術。

B.3.12 安全參數的傳輸 (Transmission of Security Parameters)

持有執照者或申請人配置 CDA 並把資訊相關的安全參數在 CDA 之間進行交換。

B.3.13 公開金鑰基礎建設憑證 (Public Key Infrastructure Certificates)

持有執照者或申請人根據憑證政策來發布或取得公開金鑰憑證，且該憑證政策必須是發執照者所認可的。

B.3.14 行動碼 (Mobile Code)

對於惡意使用行動碼技術可能對 CDA 造成的損害，建立使用限制和實施方針；並授權、監測和控制 CDA 內行動碼的使用。

B.3.15 安全名稱／位址解析服務（來源可靠性）(Secure Name/Address Resolution Service (Authoritative/Trusted Source))

- 配置系統，該系統提供名稱／位址解析的服務，在回應解析查詢上提供資料來源的可靠性。
- 配置系統，該系統對 CDA 提供名稱／位址解析，當操作分散式、階層式命名空間時，提供方法來表示子空間的安全狀態，如果子空間支援安全的解析服務，就能夠驗證父空間與子空間之間的信任關係。

B.3.16 安全名稱／位址解析服務（快取解析器）(Secure Name/Address Resolution Service (Recursive or Caching Resolver))

- 配置系統，該系統對 CDA 提供名稱／位址解析的服務，以執行資料來源的認證和資料完整性驗證。
- 配置 CDA，在收到資料時，它們執行資料來源驗證和資料完整性驗證，以回應 CDA 是否明確要求要這個服務。

B.3.17 建構和提供名稱／位址解析服務 (Architecture and Provisioning for Name/Address Resolution Service)

持有執照者或申請人配置系統，該系統對邏輯組織提供名稱／位址解析服務，以提供容錯和隔離的服務（即實施角色分離）。

B.3.18 會談可驗證性 (Session Authenticity)

持有執照者或申請人配置 CDA 來保護通訊會談的可驗證性。

B.3.19 輕便的節點 (Thin Nodes)

持有執照者或申請人配置 CDA 和控制台來使用正在處理的元件，使其功能和資料的儲存可以最小化。

B.3.20 靜止資訊的機密性 (Confidentiality of Information at Rest)

持有執照者或申請人配置 CDA，以保護靜止資訊的機密性。

B.3.21 異質性／多樣性 (Heterogeneity/Diversity)

持有執照者或申請人使用多種技術來實作 CDA。

B.3.22 故障於已知狀態 (Fail in Known State)

若 CDA 故障於已知狀態，確保 SSEP 的功能不會因為 CDA 故障而受到影響，並防止 CDA 或者其元件在故障事件中損失其機密性、完整性和可用性。

B.4 識別和驗證（Identification and Authentication）

B.4.1 識別和驗證的政策及程序 （Identification and Authentication Policies and Procedures）

將識別政策和驗證政策文件化，該文件包含處理的目的、範圍、角色、責任和管理承諾，並且識別出潛在的網路用戶、主機、應用程式、服務和資源。另外程序也要文件化，以利於政策及相關控制措施的實施。並將這些文件發展、宣傳、（每年度）審查和更新。

在管理使用者的識別碼和 CDA 的驗證碼時，該政策在識別及驗證用戶上提供了一些指導方針。

B.4.2 使用者識別和驗證（User Identification and Authentication)

- 實施身分鑑別和驗證的技術，以識別和驗證使用者與 CDA 之間的互動行為，並確保 CDA、設備的安全邊界、操作環境的實體控制以及個人與 CDA 的互動，都是具有唯一的識別和驗證，使用者所進行的活動也都是要經過驗證和識別的。
- 確保身分驗證的技術是使用多因子 (Multifactor) 驗證，用來保護處理程度。
- 當 CDA 不能支援使用者身分識別和驗證時的對策時，實施替代的控制措施並且記錄使用替代控制措施的理由。
- 實施安全區域的驗證，如果該地方沒有使用區域形式的驗證，記錄和說明沒有實施安全區域驗證的理由。

B.4.3 密碼要求（Password Requirements）

持執照者或申請人確保在使用密碼時要平衡密碼的安全性和操作上的方便性、密碼要具有長度和複雜性的要求、定期更改密碼、主要密碼的副本要存放在有限制存取的安全地點、有權利去更改主要密碼 (Master Password) 的人員必需要是授權過的人員。

B.4.4 人機介面不支援身分驗證的安全（Nonauthenticated Human Machine Interaction Security）

- 確保在 CDA 人機界面 (Human Machine Interaction, HMI) 不支援身分驗證的情況下，要有適當的實體安全控制，可以對操作

者進行授權和識別並對操作者進行監控，使得操作者的行為可以被稽核和記錄。

- 對 NHMI (Nonauthenticated Human Machine Interactions) 做控制存取時，可以在不妨礙人機界面下且同時保持 NHMI 的安全並且只限於授權人員可以存取 NHMI。
- 驗證 SSEP 功能不會受到驗證、會談鎖定或是會談結束的控制措施而造成不利的影響。
- 在 NHMI 上實施稽核，確保授權人員或是有資格的人員記錄和監測所有的操作活動，並且維護歷史記錄。

B.4.5 設備識別和驗證（Device Identification and Authentication）

在設備要建立與 CDA 的連線之前，實施並且記錄識別和驗證的設備所使用的技術，以及在 CDA 不能支援設備的識別和驗證情況下，實施替代的控制措施並且記錄使用替代控制措施的理由。

B.4.6 識別碼管理（Identifier Management）

- 唯一識別每一位使用者。
- 檢驗每位使用者的識別碼。
- 從組織官員取得授權以發給使用者識別碼。
- 核發使用者識別碼給計畫參與人員。
- 如果使用者識別碼在最多三十天內都沒有使用，則使其失效。
- 將使用者識別碼歸檔，並與存取授權程式的記錄保存一致。

B.4.7 驗證碼管理（Authenticator Management）

- 定義初始驗證碼的內容，如定義密碼的長度和組成、令牌、金

鑰和其他形式的驗證碼。

- 在初始驗證碼分配時，建立管理程序；如驗證碼遺失、洩漏或損壞和撤銷驗證碼等管理程序。
- CDA 安裝完成後，變更預設的驗證碼並且定期每年變更。

B.4.8 驗證碼回饋（Authenticator Feedback）

確保 CDA 在驗證的過程中模糊了驗證資訊的回饋，以避免資訊被利用或是未經授權的使用，以及確保 CDA 和 CDA 的回饋不會提供資訊給未經授權的用戶。

B.4.9 加密模組驗證（Cryptographic Module Authentication）

確保 CDA 是根據 FIPS 140-2 加密模組安全需求來驗證該加密模組。

B.5 系統強化 (System Hardening)

B.5.1 移除不需要的服務和程式 (Removal of Unnecessary Services and Programs)

- 持有執照者和申請人要文件化所有與 CDA 有關聯需要的應用程序、公用設施、系統服務、配置文件、資料庫和其他軟體等等。
- 持有執照者和申請人要維護 CDA 的服務需求清單，這個清單要包括有正常或緊急行動所需要的通訊埠 (Port) 和服務需求，這個清單還必須要描述為何每個服務是必要的操作，只有哪些服務和程式的必要操作是允許的。
- 持有執照者和申請人要文件化作業系統和軟體的更新，讓 CDA

可以允許追蹤和驗證沒有額外的服務是被重新安裝或者重新啟用。

- 被移除或取消功能的軟體元件在加入 CDA 的生產環境之前不需要進行操作和維護。

B.5.2 主機入侵偵測系統 (Host Intrusion Detection System)

持有執照者和申請人要建立、實施和文件化以下要求：

- 配置主機入侵偵測系統要包括屬性，例如靜態文件的名稱、動態文件的格式、系統和使用者的帳號、未經授權執行的代碼、主機的使用率、權限和程序來使系統具有偵測網路攻擊的能力，以及包括設計基礎威脅。
- 當安全議題被識別來保持已建立層級的系統安全性，執行規則更新和主機入侵偵測系統的程式修補 (Patch)。
- 持有執照者和申請人要保證主機入侵偵測系統配置文件的安全，以確保只有授權人員才可以進行存取。

B.5.3 檔案系統和作業系統權限的更改 (Changes to File System and Operating System Permissions)

持有執照者和申請人要建立、實施和文件化以下要求：

- 配置 CDA 的最小權限、資料、命令、檔案和帳戶存取。
- 配置系統服務來執行最小權限等級，可能為服務和文件的配置。
- 要文件化變更或停用的檔案和功能。
- 經過修改或升級之後，要驗證最基本的權限和安全設定是沒有被改變的。

B.5.4 硬體組態 (Hardware Configuration)

持有執照者和申請人要建立、實施和文件化以下要求：

- 關閉那些透過軟體或實體中斷，不需要網路和無線通訊的 Port，以及可移動式的媒體裝置或提供工程屏障。
- 要使用密碼保護 BIOS 來避免未經授權的更改。
- 適當的使用網路設備來限制從特定位置的存取。
- 如果設備的組態被軟體或文件來關閉，可以允許系統管理員重新啟用該設備。
- 設備組態的更換要經過驗證，必須等於或優於原本的設備。

B.5.5 作業系統、應用程式以及第三方軟體的更新安裝 (Installing Operating Systems, Applications, and Third-Party Software Updates)

持有執照者和申請人要建立、實施和文件化以下要求：

- Patch 管理程序、更新流程以及個人安裝的責任等。
- 會影響 CDA 的弱點的通知要被實施，以 4 小時內收到的弱點訊息為主。
- 通知與網路安全相關 Patch 的授權人員。
- 在實施前的更新或變通辦法要被授權。

持有執照者和申請人要建立，實施和測試以下：

- 在安裝生產系統以及所有與安全影響有關的更新之前，非生產系統或設備接收到網路更新必須要先經過測試以及驗證。
- 持有執照者和申請人要確保非生產系統和設備能夠準確的複製到 CDA 的生產當中。

(六) 附錄 C、操作性與管理性安全控制 (Operational and Management Security Controls)

C.1 媒體保護 (Media Protection)

C.1.1 媒體保護政策及程序 (Media Protection Policy and Procedures)

持有執照者和申請人開發、傳播以及每年定期檢閱及更新下列兩點：

- 在[地點/持照者/申請者]實體中提出目的、範圍、角色、責任、管理實行 (Management Commitment) 及協調之正式且文件化的媒體保護政策，並且與每個資訊目錄一致，及確認任何能夠提供資訊以幫助攻擊者的媒體，將之被標明為最低限度以識別媒體的敏感性質。
- 正式且文件化的程序，包含定義目的、範圍、角色、責任以及媒體接收、儲存、處理、清潔、移除、在利用和處理範圍內的管理實行，藉此提供高度保證，阻止未經授權的資訊揭露透過網路攻擊影響核能設施的 SSEP 功能，以幫助媒體保護政策和所有相關媒體保護控制措施的實行。

C.1.2 媒體存取 (Media Access)

持有執照者和申請人文件化和限制對關鍵數位資產媒體的存取，只接受被授權者的存取。關鍵數位資產媒體包括數位媒體及非數位媒體。

持有執照者和申請人 對每個具備儲存資訊能力之行動計算及通訊設備進行安全資訊的存取限制，只允許被授權者的存取。

持有執照者和申請人採用自動化機制限制對媒體儲存範圍的存取，以及查核存取嘗試並允許存取。

C.1.3 媒體標記 (Media Labeling/Marking)

持有執照者和申請人根據資訊分類標記可移動的關鍵數位資產媒體和關鍵數位資產輸出，指出分配限制和注意事項的處理。包含影音放映設備之外部媒體輸出，根據識別出來的一套特殊傳播、處理或分散指示，適用於使用人類可讀取和媒體標記的標準命名慣例之系統輸出。

C.1.4 媒體儲存 (Media Storage)

持有執照者和申請人安全地保護和儲存關鍵數位資產媒體，以達到與資料敏感相符的層級。

C.1.5 媒體轉換 (Media Transport)

持有執照者和申請人用與資料敏感性相符合的傳輸方法，保護和儲存關鍵數位資產媒體。

持有執照者和申請人在控制區域外的傳輸期間，保護和控制關鍵數位資產媒體，限制相關的媒體傳輸活動，只允許被授權者的傳輸。

持有執照者和申請人在控制區域外的傳輸期間，使用持有執照者和申請人所定義的安全方法保護數位及非數位媒體。

持有執照者和申請人使用其所定義系統所記錄的關鍵數位資產媒體，將其相關傳輸活動文件化。

在關鍵數位資產媒體傳輸期間，持有執照者和申請人在關鍵數

位資產媒體傳輸時間使用認可的監督人 (Identified Custodian)。

C.1.6 媒體清潔與處理 (Media Sanitation and Disposal)

持有執照者和申請人再次利用前，遵照 NIST SP 800-88 的指引清潔關鍵數位資產媒體。透過阻止設計基礎威脅(DBT)對手再建造的方式來破壞資訊。

持有執照者和申請人識別需要清潔的關鍵數位資產媒體，及過程中使用適當的技術和程序、再次利用前清潔識別的關鍵數位資產媒體，並實行這控制措施讓媒體清潔是連貫的。持有執照者和申請人追蹤、文件化及確認媒體清潔和處理動作，並且每年檢測已清潔的資料以確認設備和步驟正確運行。

C.2 人員安全 (Personnel Security)

C.2.1 人員安全政策與程序 (Personnel Security Policy and Procedures)

持有執照者和申請人的審查員允許在沒有人護送的情況下授權進入某些單位，如要有進入權限、額外的知識 (Extensive Knowledge)、對於 CDA 的管理控制或通訊系統，在進入之前可能會對 CDA 的安全、緊急應變措施產生不利，此項根據 10 CFR 73.56 人員進入核電廠的進入授權。

C.2.2 人員離職或轉換 (Personnel Termination or Transfer)

持有執照者和申請人終止或轉移其職務時，根據 RG5.71 附錄 C-3 頁且建立於 10CFR73.56 下:進入授權程序須執行以下操作：

- 終止所有 CDA 與系統的存取（權限）。

- 進行離職（離開職位）面談。
- 通知相關人員身分變更與終止事項。
- 檢查所有與安全相關的組織財產。
- 保留終止職位前對於組織資訊與 CDA 的存取控制資訊。

C.3 系統及資訊真確性 (System and Information Integrity)

C.3.1 系統及資訊真確性政策與程序 (System and Information Integrity Policy and Procedures)

持有執照者和申請人開發、傳播以及每年定期審查及更新下列事項：

- 一個正式且文件化的系統和在持有執照者和申請人的實體及一致性裡，提出目的、範圍、角色、責任、管理實行和協調的資訊真確性。
- 正式且文件化的步驟以幫助關鍵數位資產的實行、資訊真確性政策和相關之系統及資訊真確性的控制措施。

持有執照者和申請人的系統和資訊真確性程序包含下列屬性：

- 偵測在建立防禦層級範圍和在安全層級內發生惡意/可疑的存取控制或網路異常。
- 使用合適的安全通訊機制以適時進行偵測與警告人員，且能夠免於被網路監控到的惡意或可疑活動。
- 隔離且包含惡意活動。
- 消除惡意活動。
- 集中網路安全事件的記錄檔以支援事件關連。
- 針對安全機制管理提供安全監控。

- 提供給所有的安全相關設備時間同步資訊。
- 對於監控網路(或系統/關鍵數位資產)的實體和吻合或超過的邏輯安全提供高度保證，並且不同於被監控的系統/關鍵數位資產或網路。

C.3.2 缺陷修復 (Flaw Remediation)

持有執照者和申請人為了下列目的建立、實行及文件化程序：

- 識別安全警告和弱點評估過程。
- 傳達弱點資訊。
- 盡快修正使用組態管理過程的缺陷。
- 修正關鍵數位資產的安全缺陷。
- 執行關鍵數位資產的弱點掃描和評估，以證實缺陷在關鍵數位資產運作前已被消除。

在實行修正以前，持有執照者和申請人文件化和測試與缺陷修補的軟體更新，以決定在關鍵數位資產的效用與潛在的副作用。持有執照者和申請人在缺陷修補軟體的修正行動計畫抓取缺陷修補資訊。

C.3.3 惡意碼保護 (Malicious Code Protection)

持有執照者和申請人在安全範圍設備的進入及離開點建立、配置及文件化即時惡意碼保護機制，用來偵測及消除惡意碼之網路上的關鍵數位資產、工作站、伺服器及行動計算設備因下列而產生：

- 系統、關鍵數位資產、可移動媒體或其他通訊方法之間的資料通訊。

- 利用關鍵數位資產弱點。

每當符合持有執照者和申請人的組態管理政策和流程，持有執照者和申請人文件化和更新惡意碼保護機制新版本的可用性。

持有執照者和申請人文件化和配置惡意碼保護機制以確保下列事項：

- 每週完成安全範圍之設備、關鍵數位資產、工作站、伺服器及行動計算設備的掃描，以及當下載、開啟或是執行檔案時的即時掃描。
- 消毒及隔離受感染的文件。

持有執照者和申請人從多個供應商深度防禦策略的一部分文件化及採用惡意碼保護軟體產品，並且提出在惡意碼偵測及消除過程所收到的錯誤，和由此產生對關鍵數位資產可用性的潛在影響。

持有執照者和申請人集中管理惡意碼保護機制以完成下列事項：

- 關鍵數位資產避免使用者繞過惡意碼保護的能力。
- 只有在被授權的使用者指定時，關鍵數位資產才能更新惡意碼保護機制。

持有執照者和申請人不允許使用者將未經授權的可移動媒體傳入關鍵數位資產。

持有執照者和申請人禁止所有非必要的關鍵數位資產作業的媒體介面。

持有執照者和申請人文件化和實行惡意碼保護機制，以識別包

含惡意碼資料，及當關鍵數位資產面臨資料未明確被安全政策允許的相對回應。

C.3.4 監控工具及技術 (Monitoring Tools and Techniques)

持有執照者和申請人負責下列事項：

- 監控關鍵數位資產的事件。
- 監控關鍵數位資產的攻擊。
- 監控和阻擋未經授權的連結。
- 依照資訊保留需求留存事件記錄。
- 識別關鍵數位資產未經授權的使用。
- 監測設備部屬以對下列能力提供關鍵數位資產的能見度：
  - 收集資訊來偵測攻擊、未授權的行為和存取以及授權存取。
  - 追蹤持有執照者和申請人的特定傳輸型態。

持有執照者和申請人無論何時都要提高監測活動的層次。

持有執照者和申請人或美國核能管制委員會決定有對地點的 SSEP 風險增加的指示。

持有執照者和申請人文件化、聯繫及配置個人入侵偵測工具至使用共同協定的廠區入侵偵測系統。

持有執照者和申請人測試在與 NEI 03-12 第 20.1 節所定義的時間框架相符的網路入侵偵測和預防。

持有執照者和申請人文件化和採用自動化工具以協助事件即時分析。

持有執照者和申請人文件化和採用自動化工具以整合入侵偵測工具至存取控制及流量控制機制，以迅速回應。

持有執照者和申請人對異常及未經授權的活動和狀況監控、記錄以及文件化往返的通訊。當揭露或潛在揭露的指示發生時，監控能力要及時提供警告。

持有執照者和申請人防止使用者規避入侵偵測和預防能力。

持有執照者和申請人通知及文件化可疑事件的回應人員和對 SSEP 功能採用最低的破壞性行動，以調查和終止可疑事件。

持有執照者和申請人文件化及保護從偵測監控工具獲得的資訊以避免未經授權的存取、修改及刪除。

持有執照者和申請人使用足夠的網路安全人員以隨機測試和文件化入侵監控工具。

持有執照者和申請人對確保加密流量與可見的監控工具進行文件化及規範。

持有執照者和申請人分析及文件化在關鍵數位資產範圍外的通往外面的通訊流量。

持有執照者和申請人確認及文件化監控工具及技術的使用不會影響關鍵數位資產的功能性效能 (Functional Performance)。

C.3.5 安全警報與通告 (Security Alerts and Advisories)

持有執照者和申請人要負責下列事項：

- 從可信的外部組織即時接收安全警告、公告、建議和指示。
- 針對與關鍵數位資產的安全控制，實行安全指示獨立地評估和決定需求、嚴重性、方法和時間框架（RG 5.71 附錄 A 的 3.1 節）。
- 在建立的時間框架內：
  - 當有需要時產生和文件化內部安全警告、建議及指示。
  - 對活動的指定人員傳播、文件化安全警示、建議和指示及追

蹤他們的狀態及完成度。

- 根據建立的時間框架實行和文件化安全指示，或實行替代安全措施。
- 根據[配置管理程序]實施和文件化任何必要的減緩措施。
- 當有需要時可在[地點]採用自動或其他機制以讓安全警報和建議資訊。

C.3.6 安全功能驗證 (Security Functionality Verification)

持有執照者和申請人確認及文件化關鍵數位資產安全功能的正確操作。

可能發生在開始、重新啟動、收到有適當權力的使用者命令、[每週]和發現異常的時候。

當技術可行時，關鍵數位資產提供錯誤安全測試的提示，且由持有執照者和申請人文件化這些個案。

當技術可行時，關鍵數位資產提供自動支援給分散式安全測試管理和持有執照者和申請人文件化測試結果。

持有執照者和申請人文件化關鍵數位資產不能支援分散式安全測試管理自動化機制使用的情況，採用替代控制措施的理由。非自動化機制及程序測試包含下列所使用的安全功能：

- 有資格的人。
- 根據 10 CFR 73.56 值得信任且可靠的人。
- 測試流程及結果。
- 關鍵數位資產的實體存取限制。
- 監控及記錄關鍵數位資產的實體存取（對入侵的即時偵測和回應）。

- 查核和驗證措施。

C.3.7 軟體和資訊真確性 (Software and Information Integrity)

持有執照者和申請人負責下列事項：

- 偵測及文件化對軟體及資訊未經授權的變更。
- 在技術可行的情況下，採用硬體存取控制以防止未經授權的軟體變更。
- [每季]遵照 NEI 03-12 或是 NRC 規範需求，透過執行正規的真確性、操作和與製造商或供應商建議相符的功能性掃描，以進行再評估及文件化軟體及資訊的真確性、操作和功能。
- 在驗證真確性期間，技術可行則採用及文件化自動工具，以在發現差異時提供通知給指定的人。
- 採用和文件化集中管理的真確性驗證工具。
- 要求對於系統元件實體竄改事件封包或封條的使用。
- 當使用竄改事件封包，要求定期檢查。
- 進行文件化與確保使用真確性驗證應用程式不會對關鍵數位資產的操作效能產生不利的影響，並且在真確性驗證應用程式不能使用時採用替代控制措施。

C.3.8 資訊輸入限制 (Information Input Restrictions)

持有執照者和申請人負責下列事項：

- 限制關鍵數位資產輸入資訊來源只能是被授權的能力。
- 自動確認資訊的正確性、完整性、合法性及驗證性，盡可能靠近原點。將確認關鍵數位資產輸入的有效語法規則文件化，以確認輸入與格式和內容的指定定義符合。輸入通過解譯器

(Interpreters) 會預先篩選以防止內容被無意翻譯成命令。

C.3.9 錯誤處理 (Error Handling)

持有執照者和申請人對關鍵數位資產文件化及實行控制措施以確保下列事項：

- 識別錯誤情況。
- 錯誤訊息的產生，對未揭露潛在傷害性資訊卻可能遭對手利用的修改動作提供必要資訊。
- 錯誤訊息只能透過被授權者揭露。
- 避免敏感訊息包含在錯誤的記錄檔或相關管裡訊息內。

C.3.10 資訊輸出處理與保留 (Information Output Handling and Retention)

持有執照者和申請人保留從關鍵數位資產的輸出，以確保敏感資訊只被授權的人員揭露及處理。

C.3.11 預期錯誤回應 (Anticipated Failure Response)

持有執照者和申請人透過與技術規範相符、預防的維護計畫、維護規則計畫、安全計畫、緊急計畫或修正行動計畫以保護關鍵數位資產的可用性。

如果這些方案不適用，關鍵數位資產的可用性透過下列方法提供：

- 當有需要時，元件的替代、改變主動機制及元件的 standby roles
- 計算元件在特定操作環境錯誤的平均時間
- 擁有足夠的必要備份元件庫存

C.4 維護 (Maintenance)

C.4.1 系統維護政策與程序 (System Maintenance Policy and Procedures)

持有執照者和申請人開發、傳播及每年審查下列事項：

- 提出目標、範圍、角色、責任、管理承諾、在持有執照者和申請人實體中的協調、與關鍵數位資產相關的維護措施，和遵守的正式且文件化關鍵數位資產維護政策。
- 正式且文件化程序使關鍵數位資產維護政策和相關維護控制措施便利實行。
- 覆蓋在所有安全範圍內資產的系統維護政策及程序，包含下列事項：
  - 所有者控制的區域:一個在工廠安全區域外的工廠的最遠保護區域範圍。
  - 保護區域:在被實體障礙包含的核能設備範圍內及存取被控制的區域
  - 重要區域：包含任何設備、系統、材料、錯誤、破壞、能透過暴露於輻射下直接或間接破壞大眾健康和安全的釋放。重要區域可能也會包含需要設備或系統。
  - 公共存取區域：在廠區實體控制以外的區域。

C.4.2 維護工具 (Maintenance Tools)

持有執照者和申請人負責下列事項：

- 同意、監控及文件化關鍵數位資產維護工具的使用。
- 對維護人員帶進來的設備之維護工具有明顯不適當的修改，進

行檢查和文件化。

- 在關鍵數位資產使用的媒體或移動設備前，確認及文件化所有媒體及移動設備，包含針對惡意碼的關鍵數位資產、系統和測試程式或軟體。
- 控制、防止及文件化經由下列其中之一的未經授權移動之維護設備：
  - 確認設備上沒有包含持有執照者和申請人的資訊,並且在重新導入設備前確認設備真確性。
  - 消毒或破壞設備。
  - 保留設施內的設備。
  - 取得來自官方的批准，明確地授權設施設備的移動。
- 採用[自動的/手動的]機制限制，只有授權人員能夠使用維護工具，並且只在關鍵數位資產或支援設備無法支援自動機制時採用手動機制。

C.4.3 人員進行維修和測試活動 (Personnel Performing Maintenance and Testing Activities)

持有執照者和申請人負責下列事項：

- 維持及文件化現有的授權維護人員名單，需要與其存取授權計畫和內部減緩計畫相符。
- 實行及文件化[自動機制或非自動機制]以偵測命令被未經授權的人使用或執行，或者指定及文件化持有執照者和申請人人員與關鍵數位資產互動有必要的存取授權和監督陪同人員的知識。

C.5 實體與環境保護 (Physical and Environmental Protection)

C.5.1 實體與環境保護政策與程序 (Physical and Environmental Protection Policies and Procedures)

對在[地點]保護區域外的關鍵數位資產，持有執照者和申請人開發、實行及每年審查及更新下列事項：

- 正式、文件化的實體和環境保護政策並且提出下列事項：
  - 與保護關鍵數位資產有關的實體安全計畫目標。
  - 採用組織的人員及第三方承包商的實體安全計畫範圍。
  - 實體安全計畫的角色、責任及管理歸責性結構，以確保與持有執照者和申請人安全政策及其他規章承諾相符。
- 正式、文件化的流程，以讓實體及環境保護政策和相關實體及操作環境保護安全控制便利實行。

C.5.2 第三方／陪同者的存取 (Third Party/Escorted Access)

持有執照者和申請人負責下列事項：

- 篩選、執行及文件化第三方人員的安全控制，並且監控服務提供者的行為及承諾。
- 在取得相關合約及協議文件中明確包含人員安全控制。

C.5.3 實體與環境保護 (Physical and Environmental Protection)

持有執照者和申請人保護及文件化關鍵數位資產的實體存取。採用實體安全控制以限制對關鍵數位資產的存取，及防止可能會影響關鍵數位資產於操作環境進行正確操作之效能下降。

C.5.4 實體存取授權 (Physical Access Authorizations)

持有執照者和申請人負責下列事項：

- 開發及維護被授權存取設備之人員名單，並發給授權憑證。
- 包含關鍵數位資產和安全範圍系統。
- 在組織內指定官員審查及批准上述存取名單，及授權證書與存取授權計畫相符。

C.5.5 實體存取控制 (Physical Access Control)

持有執照者和申請人負責下列事項：

- 在同意對這些區域存取前，控制所有進入及離開 CDA 所在區域之實體存取點，以及確認個人存取授權。
- 批准個人存取特權及執行與關鍵數位資產改變相關的實體和邏輯存取限制。
- 透過使用電子設備和軟體控制邏輯存取。
- 產生、保留和審查記錄相關的存取限制。
- 確保只有擁有資格及授權的人才能存取關鍵數位資產。
- 控制關鍵數位資產的實體存取，獨立於設備的實體存取控制。

C.5.6 傳輸媒體的存取控制 (Access Control for Transmission Medium)

持有執照者和申請人控制及文件化關鍵數位資產通訊路徑的實體存取。

C.5.7 顯示媒體的存取控制 (Access Control for Display Medium)

持有執照者和申請人控制及文件化對於也許會幫助敵人顯示資

訊之關鍵數位資產的實體存取，並且防止未經授權的人觀察顯示輸出。

C.5.8 監測實體存取 (Monitoring Physical Access)

持有執照者和申請人負責下列事項：

- 監控及文件化關鍵數位資產的實體存取及安全範圍，以偵測及回應實體安全事件。
- 審查實體存取日誌。
- 協調審查結果及與持有執照者和申請人調查的事件回應人員。
- 監控即時實體入侵警告及監督設備。
- 採用自動機制以評估及識別潛在入侵並啟動適當的回應動作。
- 提供足夠的照明給存取監控設備。

C.5.9 訪客存取控制記錄 (Visitor Control Access Records)

持有執照者和申請人負責下列事項：

- 控制及文件化訪客對關鍵數位資產的實體存取，透過識別及確認擁有優先進入人員的存取授權。
- 陪同訪客及監控訪客活動以防止對 SSEP 功能負面的影響。

C.6 防禦策略 (Defensive Strategy)

實施和記錄其防禦策略,識別每個安全層級裡相關的保護控制。

實施和記錄一個防禦模型，它可以識別資料傳輸以及相關通訊協定的邏輯邊界。該模型定義了層級和個別的 CDA 之間可允許連接的等級。防禦策略的要素要合併到 CDA。使用與風險相關的安全控制，以執行符合的設計規格和操作要求的功能。這個方法可以用

來阻止可能的攻擊方法並且提供足夠的保護。深度防禦策略使用實體安全計畫的元素；緊急應變計畫；以及管理、操作和技術的控制。CDA 使用安全控制，以限制層級之間的資料流，如此可以保護 CDA 不會受到來自另一個不安全層級的網路攻擊。安全控制和深度防禦策略是用來偵測、減緩、減輕和回復網路的攻擊。

網路安全防禦模型使用一系列增強防禦等級的網路架構來佈署。該模型利用了實體安全計畫實施的實體和行政安全控制。實體障礙，如上鎖的門、上鎖的櫃子或是實體位置的保護區或是重要區也可以用來減少風險。

本計畫附錄 A 第 3.2 節記錄了關於[持執照者/申請者]防禦策略的具體資訊。

C.7 深度防禦 (Defense-in-Depth)

實施並且記錄防禦策略，如下：

- 分配網路安全保護最高層級（即第 4 級）給 CDA，進行保安以及安全的功能並且保護 CDA 不受到低防禦層級的影響，
- 防止對最高防禦層級的 CDA 進行遠端存取，
- 防止安全等級之間位址的欺騙，
- 資料流只能是單向的，從第 4 層流到第 3 層以及從第 3 層流到第 2 層，
- 禁止從低安全等級的數位資產向高安全等級的數位資產進行通訊，
- 第 4 層的 CDA 之間的雙向通訊只能在安全層級 4 裡進行，
- 任何非安全系統對安全系統的通訊如果是雙向的，也要給予和安全系統一樣等級的保護，

- 在安全級別之間的邊界提供入侵防禦和偵測的能力，
- 確保在深度防禦的層級只能使用雙向的通訊，即不同層級之間資料流只有通過設備來執行各等級之間的安全策略以及偵測、預防、延遲、減緩和回復低安全等級的網路攻擊，
- 從低安全層級移動資料、軟體、韌體和設備到高安全層級，使用文件化的驗證流程或程序，安裝或連接這些流程和程序的設備在資料代碼、資訊或設備上，以確保個人資料、軟體、韌體或設備免於受到已知惡意代碼、木馬病毒、蠕蟲和其他的被動式攻擊。

實施和記錄高安全等級和低安全等級之間的安全邊界控制設備，包括下列內容：

- 在實體和邏輯上保護和強化了 CDA，以防止未經授權的存取或操縱，
- 根據 RG 5.71 的附錄 B，使用安全的管理通訊和加密，
- 提供日誌和警報的功能，
- 提供入侵偵測和防禦的功能，
- 偵測並且防止惡意軟體在邊界之間移動，
- 要比觀測邊界之間通訊所使用的協定其狀態做的還要更多，例如透過堡壘主機或是應用程式代理。

CDA 提供保安、安全或控制功能並且分配到第 4 層級的保護。CDA 提供資料取得的功能，並分配在第 3 層級以上的保護。該防禦模型定義了資料的傳輸。

C.8 事件回應 (Incident Response)

應用於衡量系統、CDA、網路保護裝置的阻斷、拒絕與偵測網路攻擊之必要性，且與持有執照者和申請人的防禦策略並行。

持有執照者和申請人建立、實施與文件化安全控制，來進行拒絕、阻斷、偵測有害威脅與 CDA 可能會遭受到網路攻擊影響之狀況。安全控制用於防制假設性的威脅上。持有執照者和申請人建立、實施與文件化方法常用於[廠區/申請者]的事件回應人員反應事件與加強網路安全事件（適合的法規施行）或是 NRC。

持有執照者和申請人的改善行為程序評估、追蹤、管理提供了改善行為與網路攻擊的文件化。

持有執照者和申請人 管理回覆對於網路事件的即時身分驗證及偵測與網路攻擊回報程序。當對於網路攻擊有合理的懷疑時，進行回應指示通知行動管理負責人、廠區安全負責人、管理核能資訊科技、網路安全事件回報小組與其他緊急回應行為。

持有執照者和申請人的直接抑制動作程序。這些測量至少包含以下幾個必須動作：

- 協助管理操作可行的決策。
- 如果可以的話,在行動管理負責人的允許下隔離受影響的 CDA。
- 確認環繞或連接 CDA、網路與輔助系統沒有受到汙染與退化。

根除識別出來的攻擊或是有危險的路徑。持有執照者和申請人使用損壞回復程序來修補、清除、Reimage 或取代 CDA。持有執照者和申請人管理程序直接衡量必要性以減緩網路攻擊的影響。

包含但不只限於恢復行為，回復功能測試、安全功能與需求測試、修復運轉的地區、確認可運轉與恢復到服務動作。被網路攻擊

的系統、網路或設備影響將直接由持有執照者和申請人的程序回復到正常運轉。持有執照者和申請人需進行事件分析並且符合修正行動計畫。

持有執照者和申請人將網路攻擊直接由持有執照者和申請人的程序報告給 NRC，此項與 RG 5.71 附錄 C 中的要求—「報告維護事項」一致。更詳細的描述於第 C.8.6 節和 10 CFR Part 73 Appendix G。

C.8.1 事件回應政策與程序 (Incident Response Policy and Procedures)

持有執照者和申請人發展、散播並每年定期審查與更新事項如下：

- 一個制式化、文件化事件回報政策來說明意圖、範圍、規則、責任、管理承諾、持有執照者和申請人實體之間的協調與服從。
- 制式化、文件化程序來使得事件回覆政策與建立程序相關事件回報控制更加便利，建立的程序如下：
  - 通知員工與操作員；
  - 當非預期的事項或可能導致網路攻擊錯誤狀態發生時進行決策；
  - 在網路攻擊事件發生可能導致先前的行為中斷或 CDA 終止，使用修正行動計畫來進行分析確認入口設備有進行關閉弱點；
  - 建立損壞回復計畫，使之能夠在網路攻擊下明確的許可快速回復，包含系統備份用於快速的重建 CDA。
- 回復計畫需要演習以確保其生效與人員充分了解，使之能夠符合[損壞回復計畫、業務持續與緊急計畫]，而於練習訓練中或實

際發生事件可能會對於課程學習進行修改。

持有執照者和申請人包含股東對於事件回覆政策、程序與計畫之發展，包含下列數項：

- 實體安全
- 網路安全小組
- 運作
- 工程
- 資訊科技
- 人力資源
- 系統支援廠商
- 管理
- 合法

C.8.2 事件回應訓練 (Incident Response Training)

持有執照者和申請人需對下列事項負責：

- 從訓練回報規則訓練人員，並且尊重對於 CDA 的責任，並提供進修[最少每年一次]。
- 將事件模擬狀況納入事件回應訓練，使得人員在事件發生的危急關頭能更加的有效率。
- 將事件回覆訓練動作文件化並且確認有資格訓練的人員。

C.8.3 事件回應測試與訓練 (Incident Response Testing and Drills)

持有執照者和申請人需對下列事項負責：

- 測驗並進行對於 CDA 的事件回應能力[至少每年一次]。

- 使用持有執照者和申請人定義測試、訓練或包含兩者來更新事件回應能力來保持其有效。
- 將測試與訓練結果文件化。
- 提供事件回應測驗與訓練程序。
- 利用自動化機器來徹底並有效率的測驗或訓練事件回覆能力
- 公告並且文件化宣布或是未宣布測驗與訓練。

C.8.4 事件控管 (Incident Handling)

持有執照者和申請人需對下列事項負責：

- 實施並文件化一個正在進行的對於安全事件的事件處理能力，包含準備、偵測與分析，並抑止、根除與回覆將它列入已經存在的事件處理程序清單。
- 正在進行的事件處理動作於事件回覆程序與按照程序實行併入課程學習
- 將完整的網路安全事件回覆小組 (CSIRT) 列表。
- 在非計畫的事件狀態發生如，減少需要網路安全人員數量，在兩小時內，利用其他訓練、在場有資格的人員或連絡下班的人員進行輔助。
- 提供有技術能力與有權力的小組來有效率的回覆潛在的網路安全事件。
- 制定並且文件化程序與控制，當雇用小組後發現或確認潛在或實際的網路安全攻擊。
- 對下列進行文件化與確認回覆：
  - 辨認網路安全事件的組成因素
  - 辨認威脅層級與事件分類

- 描述對於被用來執行在每一個組成部分的事件回覆與恢復程序 (Incident Response & Recovery (IR&R) Process)。
- 描述個別的假設層級或是事件與攻擊的類別，如於分析攻擊時的攻擊路徑，指示與潛在或計畫的舒緩方法。
- 辨別可能會協助辨識與抑制網路攻擊的防禦策略。
- 描述 CSIRT 事件通知程序。
- 描述事件文件化需求。
- 建立用於本地、偏遠 CSIRT 成員與外部代理之間的協同與安全通訊方式
- 描述回覆擴大需求。

持有執照者和申請人的 CSIRT 由下列個人的知識與經驗組成：

- 資訊與數位系統科技：此項目涵蓋到網路安全、軟體發展與應用、電腦系統管理與電腦網路等範圍。特別是數位系統結合於電廠需要相關知識，包含電子儀器、控制系統與其他電廠業務系統。於電廠作業區域，包含能夠程序化的邏輯控制器 (Logic Controller)、控制系統與分散式控制系統。於業務區域，包含電腦系統與包含資訊的資料庫，用來設計、運轉與維護 CDA。於網路區域，於工廠與公司範圍網路皆需要知識。一個有經驗且有高度技術的網路安全員工成員應於上述區域中皆有經驗。
- 核電廠設備運轉、引擎與安全：這些包括於全部的設備運轉與廠區技術規格等知識。 員工描述這些技術區域將能夠追溯弱點或一系列的弱點，這些弱點會透過工廠子系統或系統影響 CDA（或連接的數位資產）外部，所以廠區全部的安全影響、安全與緊急準備 (SSEP) 皆是可以評估的。

- 實體與運轉安全: 這些包括於工廠實體與運轉的安全程式含較深度的知識，除了上述的需求之外，特別於深度的網路安全技術是需要進行電子測試確認與選擇性的掃描行為。
- 持有執照者和申請人於這些區域可能沒有就地的人員訓練與經驗，如果這些技術並沒有辦法執行，可以考慮使用企業級的網路安全人員、獨立的網路安全組織或其他必須確認這些經驗的資源。

除此之外，下列規則包含 CSIRT 的基本需求項目也需加入（與事件相關）:

- 電廠安全（實體）
- 老舊電廠管理
- 企業公共關係 (Corporate Public Relations)
- 企業法規 (Corporate Legal)

事件資料蒐集包含下列：

- 事件標題
- 事件資料
- 可靠的報告
- 事件的種類
- 進入點
- 犯人 (Perpetrator)
- 系統類型、硬體與軟體影響
- 簡述影響
- 對組織的影響

- 偵測與防範再次發生
- 回覆

C.8.5 事件監測 (Incident Monitoring)

持有執照者和申請人基本上使用自動設備追蹤並文件化安全事件，用來協助追蹤安全事件蒐集與分析事件資訊。

C.8.6 事件報告 (Incident Reporting)

RG 5.69 “Guidance for the Application of the Radiological Sabotage Design Basis Threat in the Design, Development and Implementation of a Physical Security Protection Program that Meets 10 CFR 73.55 Requirements” 提供網路攻擊與網路安全攻擊的類型指引，包含對於美國 NRC 的報告。

於網路安全攻擊或網路事件的調查與恢復期間，檢討決策的報告性是必須的。目前有數個規則報告緊急與非緊急事件給 NRC，報告中不僅只能有網路安全報告標準。NRC 已制定 DG-5019 “Reporting of Safeguards Events”，但截至目前並沒有結果或公告。

C.8.7 事件回覆與援助 (Incident Response Assistance)

持有執照者和申請人提供有能力與訓練事件回覆人員，能夠全年無休、廿四小時提供報告的建議或幫助 CDA 的使用者與網路安全事件報告，此協助資源對構成持有執照者和申請人的事件回覆能力是必須的。

持有執照者和申請人使用機器來加強對於事件回覆所需的資訊與協助之能力。

C.8.8 網路事件回應計畫 (Cyber Incident Response Plan)

持有執照者和申請人發展一個事件回應計畫包含：

- 描述網路事件回覆能力的結構與組織。
- 提供高階途徑來找出網路事件回覆能力如何符合整個組織。
- 定義可報告的網路事件與 Regulatory Position C.8.6 符合。
- 提供公制於測量組織網路事件回報能力。
- 定義資源與管理協助之需求，對於有效的維護與更加成熟的事件回覆能力。
- 需由網路安全程式提供者批准審核。

持有執照者和申請人分配事件回覆計畫的副本於廠區人員，包含事件回覆人員，審查事件回報計畫[每年]，重新審查事件回報計畫於地址變更或於計畫實施、執行、測試過程中遇到問題，並傳達事件回覆計畫的改變給廠區人員包含事件回覆人員。

C.9 SSEP 程序於意外發生時的持續計畫 (Contingency Planning/Continuity of Safety, Security, and Emergency Preparedness Functions)

C.9.1 意外處理計畫政策與程序 (Contingency Planning Policy and Procedures)

持有執照者和申請人發展、散佈、年度審查與更新事項如下：

- 一個制式、文件化的意外計畫政策說明意圖、範圍、規則、責任、管理承諾、持有執照者和申請人實體之間的協調與服從。
- 制式化、文件化程序來使得緊急計畫政策更加便於施行並與緊

急計畫控制結合。

當持有執照者和申請人重新審查指出需要更新時，持有執照者和申請人更新緊急計畫政策與程序於其他程式的必要與相關政策。

持有執照者和申請人緊急計畫包含下列：

- 需要事件或狀態有持續變化且嚴重時回覆，使恢復計畫進行。
- 依據手冊運作 CDA 程序與外部電子連線切割直到安全狀況恢復。
- 規定與回覆者的責任。
- 備份的過程與程序，與資料的安全儲存。
- 完整與現代化的邏輯圖表來描述網路連結。
- 近期的組態資訊與組件。
- 授權 CDA 的網路或實體存取的員工清單(根據標題、功能)。
- 緊急狀況連絡的通訊程序與人員清單(根據標題、功能)。
- 對替代的組件需求進行文件化。

C.9.2 意外處理計畫 (Contingency Plan)

持有執照者和申請人需對下列事項負責：

- 透過發展與公布規則、責任、指派連接資訊項目與對於 CDA 影響之決定的相關行為，在妥協、分裂或失敗與回復 CDA 後，實施網路意外安全計畫來維持 SSEP 功能。
- 持有執照者和申請人組織對於相關計畫、需求的責任來調整意外計畫發展。
- 於危機狀態發生時，維持必要的資源與能力來確定必要的資訊程序、電信與支援環境。

- 於危機狀態發生時，將必要的資源文件化，以確保資訊程序、電信、支援環境的必要能力。
- 當 CDA 的程序遺失或與運轉設備的通訊失敗之狀態發生時，部屬 CDA，CDA 將進行預先決定之動作。

C.9.3 意外處理計畫測試 (Contingency Plan Testing)

持有執照者和申請人有責任進行下列行為：

- 測試、練習與文件化意外計畫[至少每年]來確認仍然可以有效與組織執行計畫的意願。
- 審查意外計畫測試與練習結果，了解適當的改正行為。
- 調整持有執照者和申請人各單位於相關計畫的責任之意外計畫測試或練習。
- 測試、練習與文件化意外計畫於緊急或備份地點，來使得緊急人員能夠熟悉這些設備與能用的資源，評估單位能力來協助緊急事件處理。
- 透過提供更多涵蓋完整意外問題，選擇更多實際的測試與練習劇本與環境，使用自動化機器來徹底與有效率的測試與練習意外計畫。
- 將恢復與補足 CDA 於意外計畫之測試。
- 當緊急計畫無法測試或練習時，建立與文件化替代的控制措施，因為對於 SSEP 或信任區域與 CDA 有潛在或是重大的不利影響。
- 使用階段性與非階段性的系統維護行為，包含回覆給 CDA 組成與系統故障，如測試或練習意外計畫的機會。

C.9.4 意外處理計畫訓練 (Contingency Plan Training)

持有執照者和申請人需對下列事項負責：

- 從訓練意外規則訓練人員，並且尊重對於 CDA 的責任，並提供進修[最少每年一次]，或與持有執照者和申請人整體的意外程序一致，無論時間長短。
- 維持訓練程序，並將個人訓練記錄文件化。
- 包含人員對於熟悉設備、CDA 與能使用的資源進行熟悉之訓練演習，並評估單位能力來協助意外處理。
- 透過提供更多涵蓋完整意外問題，來使用自動化機器來徹底與有效率的測試與演習意外計畫。
- 進行實際測試與演習劇本與環境，更有效的對 CDA 進行壓力測試。

C.9.5 異地備援 (Alternate Storage Site and Location for Backups)

持有執照者和申請人辨別與文件化替代儲存地點並加入必要的協定來允許 CDA 的資料備份，資料備份與備份資料於替代儲存地點的傳輸速率要能夠維持持有執照者和申請人的恢復時間之目標與恢復計畫目標。

持有執照者和申請人需對下列事項負責：

- 確認替代儲存的地理位置要與主要的儲存地點分散，避免遇到同樣的破壞影。響。
- 確認替代儲存地點能夠便於恢復作業。
- 辨別與文件化對於替代儲存位置之潛在遭受存取問題，當較廣泛區域的破壞與分裂時要能夠實施明確的改善行為。

C.9.6 CDA 備份 (CDA Backups)

持有執照者和申請人需對下列事項負責：

- 管理使用者階級或系統階級資訊的備份。
- 確認 CDA 由 CDA 指定之時間區間或由事件觸動來進行備份。
- 於儲存位置保護備份資料。
- 測試與文件化備份資料[每月]來確認媒體可靠性與資訊真確性。
- 將備份資訊於修復 CDA 功能加入意外計畫測試中。
- 當受到未授權的修改時保護系統備份資訊。
- 儲存於分散設備或與防火設備中，與作業軟體不同步的作業系統與其他關鍵 CDA 軟體之備份拷貝。
- 建立與文件化必須恢復的 CDA 資料之時間表，與關鍵資料與組態受到修改時的頻率。

C.9.7 回復與變更 (Recovery and Reconstitution)

持有執照者和申請人使用機器與協助程序，於分裂或故障後，允許 CDA 能夠恢復與改組到已知的安全狀態，並且只能允許授權人員。持有執照者和申請人在回到一般作業之前進行恢復測試，以確保 CDA 有正確執行。

C.10 意識與訓練 (Awareness and Training)

C.10.1 資訊安全意識與訓練 (Cyber Security Awareness and Training)

持有執照者和申請人建立，實施與文件化對於持照者/申請者人員與承包商進行必要的訓練需求，對於程序需求的實施，履行其受指派職責與責任。

持有執照者和申請人單位要訓練到適合的網路安全知識等級，以對他們所被指派的責任提供高度保證，使這些單位能夠在工作上有完整的表現。

C.10.2 意識訓練 (Awareness Training)

持有執照者和申請人的網路安全意識訓練是設計來加強各單位對於網路威脅與弱點的敏感度，以及其對於必須被保護資料與資訊的認知。政策層面的意識訓練提供員工與承包商對於了解安全政策的能力，使得程序能夠有效的執行。單位使用者必須了解他們對於忠誠於適當的政策與標準的責任。

持有執照者和申請人對於下列幾點建立、實施與文件化需求：

- 訓練程序提供設備人員基本的網路安全意識訓練。 進修或持續的訓練提供新的威脅與技術訊息。
- 張貼公告、提供安全訊息項目、發送電子信箱公告、通知與登入螢幕顯示的訊息，能提供網路安全意識。
- 訓練包含實際的練習以模擬實際的網路事件、恢復計畫、回報計畫與敵人 (Adversary) 攻擊。

持有執照者和申請人制定與文件化基礎的網路安全訓練內容如下：

- 指定規則與責任
- 認定防禦策略的特定需求
- CDA 對於有權存取的人員

持有執照者和申請人建立、實施、文件化對於訓練的需求提供

如下：

- 對於持有執照者和申請人人員與承包商的網路安全意識訓練說明如下：
  - 對於網路安全程序的特定位置目標、管理期待、系統化的職權 (Programmatic Authority,)、規則與責任、政策、程序與不服從造成結果
  - 一般攻擊方法、包含社交工程技術與適合或不適合的網路安全練習。
  - 攻擊指示如下：
    - 不正常的大量網路傳輸
    - 磁碟空間不足使得可用的空間嚴重減少
    - 異常高的 CPU 使用率
    - 新的帳戶產生
    - 企圖或實際使用對於管理權限的帳號
    - 鎖定的帳戶
    - 當非該用戶工作時，其帳號卻為使用中的狀態
    - 清除記錄文件
    - 對不尋常的大量事件進行完整的記錄。
    - 防毒或入侵偵測警報
    - 防毒軟體或其他安全控制無法使用
    - 意外的修補異動
    - 機器連接到外部 IP 位址
    - 對於系統資訊的需求（社交工程企圖）
    - 組態設定意外的更改

- ◆ 系統意外關機
- ◆ 不正常的控制裝置行動
- ◆ 損失控制裝置的訊號
- ◆ 於安全區域內不正常的設備
- ◆ 組織連線到報告者對可疑的行為、意外與弱點或網路安全政策、程序或練習

- ■ 對於為何存取與控制方法的說明為必須。
- ■ 測量使用者可以用以減少風險
- ■ 如果控制方法並沒有完整包含對於組織的影響。

C.10.3 技術訓練 (Technical Training)

持有執照者和申請人建立、實施與文件化對於人員表現、確認或管理行為之訓練程序，與程序範圍，來確保適當的熟練度 (Proficiency) 有達到與維持。持有執照者和申請人單位對於網路安全責任與相關程序 (Programs, Processes, Procedures) 或包含對於 CDA 設計修改與維持，將會到技術訓練。

持有執照者和申請人建立、實施與文件化進行需求如下：

- 提供單位網路安全相關的技術訓練:
  - ■ 於授權存取 CDA 或履行指定的責任之前
  - ■ 當有政策或需求程序改變與計畫修改需求時
  - ■ 每年度或是持有執照者和申請人所定義的時間（只能更短），減輕風險與確保人員之維持能力
- 提供網路安全相關技術訓練與適當的網路安全概念給一些人員，這些人員的角色與責任參與了設計、安裝、運作、維護或管理 CDA 跟與其相關之網路，指出下列事項：

- 特定的網路安全知識與工程程序、練習與技術，包含實施方法與設計需求，且應用到其工作中可能會遭遇到的資產。
- 網路弱點、對於 CDA 的潛在後果與成功性高的網路攻擊網等一般資訊，與網路安全風險減少方法。

持有執照者和申請人提供系統管理、網路安全專家、系統擁有者、網路管理員與其他對於系統階層軟體有存取權限的人員，有安全相關技術訓練來確保他們對於受指派的責任之履行。

C.10.4 特定的網路安全訓練 (Specialized Cyber Security Training)

持有執照者和申請人單位有計畫性或程序性的網路安全權力，與必要的知識與技巧來達成對於網路安全能力的要求，網路安全專家接受專業網路安全訓練來設計、實施與管理網路有效的網路安全策略。

持有執照者和申請人對於指派安全專業與專家之進階單位訓練，建立、實施與文件化之需求，包含網路安全規則與網路安全、事件回覆與實行之責任，並管理深度防禦保護策略。進階的訓練項目包含下列：

- 達成與維持對於最新的必要技術與知識於資料安全、作業系統安全、應用安全、網路安全、安全控制、入侵分析、是建管理與回覆、數位證明、能力測試與廠區系統功能性與運轉之核心能力。
- 對於工具、加強 CDA 跟網路的實體與邏輯技術之能力，以減少可能受到網路攻擊的弱點。
- 提供對於其他員工成員的網路安全指引、協助與訓練。

- 對於程序與特定系統網路安全計畫與練習進行審查。
- 評估 CDA、網路與資產以遵從網路安全政策。
- 設計、取得、安裝、運作、維持或管理安全控制。

C.10.5 跨功能網路安全小組 (Cross-Functional Cyber Security Team)

持有執照者和申請人制定、實施與文件化一個跨功能 (Cross-Functional) 網路安全小組 (CST)。

持有執照者和申請人制定、實施與文件化一個程序來分享 CST 成員之間經驗與各領域知識。

持有執照者和申請人的 CST 包含於最小或單一的組織資訊技術員工、單一儀器與控制系統引擎、單一控制系統之運轉、一個主要的網路安全專家，與一個管理階層的人員。

持有執照者和申請人的網路安全主要專家的經驗包含網路架構與設計、安全程序與訓練，與安全基礎設施設計與運轉。

持有執照者和申請人的 CST 也包含控制系統廠商或有需要的系統整合人員。

持有執照者和申請人的 CST 報告對直接針對組織架構如何與相關人員。

C.10.6 狀況意識 (Situation Awareness)

持有執照者和申請人安全訓練描述受到控制的實體程序，而相關的 CDA 與安全控制亦同。

C.10.7 回饋 (Feedback)

持有執照者和申請人對於人員或承包商建立、實施與文件化回報程序，讓網路安全程序與列出以辨識的訓練缺陷能夠更加完善。

C.10.8 安全訓練記錄 (Security Training Records)

持有執照者和申請人文件化與監測單位的網路安全訓練。

C.10.9 聯繫安全小組與組織 (Contacts with Security Groups and Associations)

持有執照者和申請人維持與被選擇的安全團隊之接觸，以保持最新受到建議的安全訓練、技術與科技之資訊，並分享近期與安全相關的資訊，包含威脅、弱點與事件。

C.10.10 角色與責任 (Roles and Responsibilities)

持有執照者和申請人產生、文件化與提供下列職位（角色）與符合資格的人員：

- 角色：網路安全發起者
- 需求：重要位置人員管理
- 責任：
  - 全體責任與對於安全程序之責任。
  - 提供發展、實施與網路安全程序之元素所需的資源。

- 角色：網路安全計畫管理者
- 責任：
  - 提供對於工廠網路安全運作之監管。

- 與網路安全位置議題相關的功能，如單點聯接。
- 提供對於核能電廠網路安全相關議題之監管與管理。
- 根據需要，初始化與協調 CSIRT 功能。
- 於網路安全事件發生期間，根據需要，與 NRC 協調。
- 監控與批准對於網路安全計畫的發展與實施。
- 確保與批准對於網路安全教育、意識與訓練程序之發展與運作。
- 監視與批准網路安全政策與程序之發展與實施。

- 角色：網路安全專家
- 需求：
  - 保護 CDA 以免網路威脅。
  - 了解網路安全牽涉於電廠網路、控制系統、安全系統、作業系統、硬體平台、廠區特定應用與伺服器等環繞整體之架構，與依賴於申請的協議之上。
  - 完成對於數位電廠系統之網路安全評估。
  - 管理安全稽核、網路掃描與必要時對於 CDA 進行滲透測試。
  - 管理網路安全調查，包含 CDA 之洩漏。
  - 於網路安全調查期間保護所蒐集到的證據，以防止證據資訊遺失。
  - 在網路安全區域，維持專家技術與知識等級。

- 角色：網路安全事件回應小組
- 需求：
  - 人員具有網路鑑識知識

- 與事件回應計畫相符的功能

- 責任：
  - 當需要保護 CDA 免於洩漏與協助事件回復被洩漏的系統時，進行初步的緊急行動。
  - 控制與減輕事件，包括重要或其他支援系統與恢復被洩漏的 CDA。

C.11 組態管理 (Configuration Management)

C.11.1 組態管理 (Configuration Management)

持有執照者和申請人建立、實行及文件化關鍵數位資產組態管理安全控制，與此計畫第 4.2.1 節所描述的流程相符。

C.11.2 組態管理政策與程序 (Configuration Management Policy and Procedures)

持有執照者和申請人開發、傳播、每年審查及更新正式且文件化的組態管理政策和實行提出目標、範圍、角色、責任、管理承諾、[在持有執照者和申請人實體間協調]、與組態管理控制相關和承諾。

持有執照者和申請人文件化它的組態管理政策作為[地點]組態管理計畫的一部分，並且包含硬體組態、軟體組態和存取權限。文件化及根據這些政策存取硬體或軟體的改變並且實行程序。

結構化的組態管理流程評估及控制對關鍵數位資產的變更，以確保關鍵數位資產維持安全。在任何變更實行以前，持有執照者和申請人確認不會引進新的弱點。

C.11.3 基本組態 (Baseline Configuration)

持有執照者和申請人開發、文件化及維護現有關鍵數位資產的基本組態，及包含介面特徵、安全需求和資訊通訊。由於部分組態管理流程，持有執照者和申請人採用[手動的/自動的]機制以維護每個關鍵數位資產最新、完整、準確和可用的基本組態。

持有執照者和申請人文件化最新的基本組態及每季查核組態。基本組態包含現有所有元件名單、周邊組態、現有軟體發行版本和機器元件轉換設備。持有執照者和申請人對每個關鍵數位資產維護組態變更進行日誌記錄，包含實施變更的人名、變更日期、變更目的及任何在程序所觀察到的變化。

持有執照者和申請人文件化及維護開發和測試環境的基本組態，是從操作/生產基本組態分開管理。

持有執照者和申請人採用「拒絕全部，允許例外」的授權政策以識別及授權在持有執照者和申請人關鍵數位資產所允許的軟體。在實行授權變更後，持有執照者和申請人確認安全特徵功能依然適當且有足夠的網路安全層級維護。

被授權進行修改關鍵數位資產組態的人員，應受到適當的訓練及擁有執行修正的資格。持有執照者和申請人對修改定義最小實體及邏輯存取。另外，持有執照者和申請人採用電子方法監控關鍵數位資產的存取以確保只有使用被授權的系統與服務。此外，文件化使用替代安全控制場合的理由，而這個場合是無法電子監控，包含下列事項：

- 實體限制存取。
- 監控及記錄實體存取，使得可以即時對入侵做偵測及回應。

- 採用稽核及確認方法。
- 根據 10 CFR 73.56，確保被授權者是值得信任並且可靠。
- 確保被授權者是在建立工作管理控制下操作。
- 進行維修後測試以確認已正確變更。

持有執照者和申請人遵守實體安全計畫進行審查日誌記錄[一季至少一次]。

C.11.4 組態變更控制 (Configuration Change Control)

持有執照者和申請人負責下列事項：

- 授權及文件化關鍵數位資產的變更。
- 保留及審查關鍵數位資產組態變更記錄，和查核與關鍵數位資產組態變更的相關活動，並且採用[手動的/自動的]機制進行下列事項：
  - 文件化關鍵數位資產的變更。
  - 通知指定的批准機關。
  - 阻止變更的實行直到收到及文件化指定的批准機關。

C.11.5 變更與環境的安全影響分析 (Security Impact Analysis of Changes and Environment)

持有執照者和申請人的 CST 在對關鍵數位資產作變更前執行安全影響評估，符合[RG 5.71 附錄 A 的 4.2.2 節]以管理變更的網路風險。CST 評估、文件化及合併在任何定義安全相互依存關係的安全影響分析。

持有執照者和申請人在變更批准流程的一部分執行及文件化安

全影響評估。

C.11.6 變更存取限制 (Access Restrictions for Change)

持有執照者和申請人定義、文件化、批准及執行與關鍵數位資產相關變更的實體及邏輯存取限制，以及產生、保留及查核每季記錄，並且當有跡象時顯示也許有未經授權的變更發生。

持有執照者和申請人實行它的組態變更計畫以提出發現的誤差。

持有執照者和申請人採用自動化機制偵測未經授權的變更、執行授權限制及支持往後執法活動的查核。

持有執照者和申請人文件化替代安全控制的理由和細節，在關鍵數位資產不能支援自動化機制的使用，以強制存取限制和往後法令活動查核的情況下，包含下列全部事項：

- 實體限制存取。
- 監控和記錄實體存取能夠對入侵及時做偵測和回應。
- 採用查核和確認方法。
- 依據 10 CFR 73.56，確保被授權人士可信任並且可靠的。
- 確保授權者正在已建立的工作管理控制下操作。
- 處理維修後的測試以確認變更實行正確。

C.11.7 組態設定 (Configuration Settings)

持有執照者和申請人對關鍵數位資產實施組態設定，透過(a)文件化最嚴格的模式；(b)評估業務需求；(c)基於明確的業務需求，執行及文件化最嚴格的業務組態設定。

這些需要透過下列事項達成：

- 針對反映最嚴格模式的關鍵數位資產建立及文件化組態設定。
- 基於明確的操作需求，對個別在關鍵數位資產中的元件文件化及批准任何從最嚴格模式的組態設定的例外。
- 執行關鍵數位資產的組態設定及監控和控制組態設定根據持有執照者和申請人的政策和程序的變更。
- 文件化及採用自動化機制以[集中]管理、應用及確認組態設定。
- 文件化及採用[自動機制/手動機制]以回應持有執照者和申請人所定義的組態設定的未經授權的變更。
- 在關鍵數位資產無法支持自動化機制去[集中]管理、應用及確認組態設定的情況下，文件化替代安全控制措施的正當理由，包含下列全部事項：
  - 實體限制存取。
  - 監控及記錄對能夠即時偵測和回覆入侵的實體存取。
  - 採用審查和確認方法。
  - 根據 10 CFR 73.56 確保授權者是值得信任並且可靠的。
  - 確保授權者正在已建立的工作管理控制下操作。
  - 處理維修後的測試以確認變更實行正確。

C.11.8 最少功能 (Least Functionality)

持有執照者和申請人配置及文件化關鍵數位資產組態設定以提供必要能力，及避免與限制使用不安全的功能、節點、協定及服務。持有執照者和申請人每月審查關鍵數位資產以識別及消除不必要的功能、節點、協定及服務。持有執照者和申請人文件化及採用自動化機制以預防計畫執行。持有執照者和申請人使用[白名單、黑名單、灰名單 (White-lists, Black-lists, Gray-lists)]應用程式控制技術。

C.11.9 元件庫存 (Component Inventory)

持有執照者和申請人開發、文件化及維護擁有下列屬性的關鍵數位資產元件庫存：

- 準確反映目前系統組態。
- 確保每個元件的位置與關鍵數位資產授權範圍一致。
- 提供被認為對追蹤、報告及有效資產歸責性的 Granularity 合適層級。
- 當一部分完整元件安裝和系統更新時，更新系統的元件庫存 。
- 採用自動化機制以維護最新、完整、正確及隨時可用的系統元件庫存。
- 採用自動化機制以偵測未授權元件或設備新增到環境，無法透過元件和設備存取或是通知指定的持有執照者和申請人官員。
- 文件化個人負責管理元件的[名字或角色]。

C.12 系統和服務的取得 (System and Service Acquisition)

C.12.1 系統和服務取得的政策和程序 (System and Services Acquisition Policy and Procedures)

開發、宣導和[每年]審查和更新正式且文件化取得系統和服務的政策，該政策滿足目的、範圍、角色、責任、管理承諾，相關系統和服務取得的控制，並且遵守。

開發，宣導和[每年]正式審查和更新正式且文件化的程序，以促進系統和服務取得政策的實施和系統取得的政策和服務相關的控制。

C.12.2 供應鏈的保護 (Supply Chain Protection)

建立可信任的分佈路徑、供應商的驗證、需要防篡改產品或是取得的產品是有封條的，使用這些措施來防止供應鏈的威脅和弱點，維持 CDA 取得的完整性。

分析每個產品的取得，以確定該產品提供的安全要求可以解決 RG 5.71 附錄 B 和 C 的安全控制。

使用異質性，以減輕使用單一供應商其產品相關的弱點。

C.12.3 可信賴性 (Trustworthiness)

要求軟體開發人員使用軟體品質和驗證方法，以減少軟體的缺陷，並建立、實施以及記錄要求，以要求所有用來執行網路安全任務或 SSEP functions 的工具是經過商業品管程序的，類似的軟體工程工具是用於開發數位儀控系統。

C.12.4 安全能力的整合 (Integration of Security Capabilities)

記錄並且實施計畫，以確保新取得的系統和服務包含安全設計的資訊、功能或同時實施 RG 5.71 附錄 B 的安全控制，並設立時間表，以減少部署新的和更有效的保護策略和安全控制所花費的時間。

C.12.5 開發者安全測試 (Developer Security Testing)

記錄並要求取得 CDA 創造、實施以及記錄安全測試和評估計畫的系統開發商和整合商，以確保取得的產品的安全要求符合所有規定，並要求發展商執行並且記錄安全要求的驗證和確認，並且實施產品的安全控制以及符合這個計畫要求的測試，以確保它們是有

效的。

需要將下列活動文件化：

- 系統設計轉換成代碼、資料庫結構以及機器可執行的形式相關
- 硬體和軟體的配置及安裝
- 軟體代碼的作法和測試
- 通訊的配置和安裝(包括再使用的軟體和商業現成產品的結合)
- 單元測試進行的結果，以確保代碼的開發和完全正確，以及準確且完整的反映了要求的安全設計配置的轉變，
- 開發代碼庫裡每個所需要的安全功能其實施的細節。該清單包括開發這些安全功能的代碼其函式和模組的參照，
- 實施安全配置以滿足要求裡說明的安全設計特點，
- 實施作業系統安全配置以滿足要求裡記錄的安全設計特點，
- 對於編制程式語言，可以支援靜態的分析來源代碼的掃描機，下列結果需要記錄下來：
  - 進行靜態來源代碼的弱點分析，以檢查代碼的開發是否有潛在的安全缺陷、不良的編制程式作法、隱藏功能，以及這些用來消除這些弱點代碼基底和方法在實施的期間其代碼裡是否脆弱的特性，
  - 安全缺陷追蹤指標用於獲取和追蹤代碼裡發現的安全缺陷的身分、類型、分類、原因和修正，
  - 在要求裡指定的設計特點轉譯到代碼之間碰到的缺陷。
- 對於所有的程式語言，動態來源代碼的弱點分析、安全缺陷追蹤指標用於獲取和追蹤代碼裡發現的安全缺陷的身分、類型、分類、原因和修正指定的設計特點轉譯到代碼之間碰到的缺陷

之結果都要記錄下來：

- 要求 CDA 開發商/整合商在 CDA 設計，開發，實施和運作期間進行組態管理、管理和控制對 CDA 的改變，並記錄對 CDA 核准的改變，並追蹤安全缺陷和缺陷的解決方案。

C.12.6 持執照者或申請人的測試 (Licensee/Applicant testing)

驗證和確認開發人員的安全測試的結果是依照第 12.5 節進行的。並負責下列事項：

- 在安裝前就要測試 CDA 的（是離線狀態且類似的 CDA）安全設備、安全控制和軟體，確保不會破壞 CDA 或其相關功能的運作。
- 進行測試，以確保 CDA 不會提供一個損害 CDA 或其他 CDA 的路徑。
- 按照 RG 5.71 附錄 A 第 3.1.6 節所描述的流程，實施 RG 5.71 附錄 B 和 C 的安全控制。
- 安全控制有效性的測試，如 RG 5.71 附錄 A 第 4.1.2 節中描述的。
- 弱點掃描的效能，按照 RG 5.71 附錄 A 第 4.1.3 節和此計畫的第 13.1 節，對 CDA 完整狀態的修正、消除或發現弱點的討論。
- CDA 目標環境的安裝和測試。
- 接受審查的效能以及 CDA 安全功能的測試。

記錄下列事項：

- 安全控制要按照 RG 5.71 附錄 B 來實施。
- 安全控制有效性的驗證要按照 RG 5.71 附錄 C 來實施。
- 發展安全設計功能，以解決識別出的 CDA 的安全要求，按照

RG 5.71 附錄 B 的安全控制來實施。對於實施每一個安全功能或是組態，文件提供了包括特徵的描述、實施的方法，以及任何和功能相關的配置選擇。每個系統裡的安全功能設計可追蹤到其相應的安全要求。

實施由網路安全組織設計用來對關鍵資產、系統和網路的安全審查需要文件化。該審查確保從要求實施的轉變為安全設計組態項目是正確的、精確的、完整的。

C.13 安全評估和風險管理 (Security Assessment and Risk Management)

C.13.1 威脅和弱點管理 (Threat and Vulnerability Management)

- 當 CDA 新的潛在弱點被報告或是識別，執行 CDA 弱點的評估和掃描[頻率不能低於每季一次]並且要根據 RG 5.71 附錄 A 的第 4.1.3 節。
- 使用弱點掃描工具和技術，來促進弱點管理流程裡工具和自動化元件之間的互相操作性
- 在時間內分析弱點掃描報告和修補弱點，保護 CDA 不會受到網路攻擊行動包括 DBT。
- 消除其他 CDA 類似的弱點。
- 使用弱點掃描工具，當新的弱點被發現和宣佈時包括更新網路弱點掃描列表以及更新 CDA 掃描弱點的列表[每個月] 的能力。
- 使用弱點掃描程序，其範圍是最大的廣度和深度（即 CDA 元件掃描和弱點檢查）。
- 審查歷史稽核日誌，以確定是否識別 CDA 以暴露的弱點。

C.13.2 風險減緩 (Risk Mitigation)

保護和減緩風險可以藉由實施（1）RG 5.71 第 3.2 節討論的深度防禦策略，（2）RG 5.71 附錄 B 和 C 所描述的安全控制，（3）對範圍內系統、結構和元件的數位設備進行軟體網路攻擊偵測、預防和回復的技術和工具，（4）RG 5.71 附錄 A 的第 4 節。[持執照者/申請者]有詳細的資訊，這些資訊是這些要求要如何實施，以達到計畫中說明的安全控制目標。詳細資訊可用於 NRC 的檢查和稽核。

C.13.3 修正行動計畫 (Corrective Action Program)

建立、實施，並且記錄符合 RG 5.71 標準不利的條件並且要求修正行動。不利的影響是因為網路安全事件進行評估、追蹤和調整要根據[持執照者/申請者]的修正行動計畫並且符合 RG 5.71 的方法。

參、主要發現與結論

一、核能電廠儀控系統資安評估項目

根據 RG 5.71，網路安全計畫的實施包括以下步驟：

- Analyzing Digital Computer Systems
  - Security Assessment and Authorization
  - Cyber Security Team
  - Identification of Critical Digital Assets
  - Reviews and Validation Testing
  - Defense-in-Depth Protective Strategies
  - Application of Security Controls
- Incorporating the Cyber Security Program into the Physical Protection Program
- Policies and Implementing Procedures

在識別關鍵數位資產之後，就是要訂定深度防禦策略以及應用安全控制項目。因此，我們依據 RG 5.71 的這些安全控制項目分成四大觀點，來訂定適合核能電廠數位儀控系統之資安評估項目：

- 技術觀點
  - B.1 存取控制 (Access Control)
  - B.2 稽核與可歸責性 (Audit and Accountability)
  - B.3 關鍵數位資產與通訊保護 (Critical Digital Asset and Communications Protection)
  - B.4 識別和驗證 (Identification and Authentication)
  - B.5 系統強化 (System Hardening)
- 操作觀點
  - C.1 媒體保護 (Media Protection)

- C.2 人員安全 (Personnel Security)
- C.3 系統及資訊真確性 (System and Information Integrity)
- C.4 維護 (Maintenance)
- C.5 實體與環境保護 (Physical and Environmental Protection)
- C.8 事件回應 (Incident Response)
- C.9 SSEP 程序於意外發生時的持續計畫 (Contingency Planning/Continuity of Safety, Security, and Emergency Preparedness Functions)
- C.10 意識與訓練 (Awareness and Training)
- C.11 組態管理 (Configuration Management)

- 管理觀點
  - C.12 系統和服務的取得 (System and Service Acquisition)
  - C.13 安全評估和風險管理 (Security Assessment and Risk Management)
- 深度防禦觀點
  - C.6 防禦策略 (Defensive Strategy)
  - C.7 深度防禦 (Defense-in-Depth)

二、核能電廠儀控系統流程安全弱點分析方法設計

本研究提出一套考量安全性的系統分析方法論，可表達出資訊系統中的安全弱點、威脅、攻擊與防禦機制，並且以圖形化方式呈現。此方法稱為「資訊安全概念模式化 (Conceptual Modeling with Security)」，簡稱為 CMsec，為基於資料流程圖 (Data Flow Diagram, DFD) 設計之圖形化系統分析方法，採用了資產 (Asset)、威脅代理

(Threat Agent)、分析邊界 (Analysis Boundary)、威脅 (Threat)、弱點 (Vulnerability)、誤用流程 (Misuse Process)、控制措施 (Control Measure) 和安全假設 (Security Assumption) 等符號，其流程設計分為底下五個步驟：

- 步驟一：產生系統資料流程圖
- 步驟二：識別威脅代理並劃定其威脅作用範圍
- 步驟三：識別威脅焦點資產及其相關安全屬性
- 步驟四：針對威脅焦點資產進行弱點識別及威脅情境描述
- 步驟五：產生相關控制措施

三、應用安全分析於飼水控制系統之型態管理

(一) 飼水控制系統簡介

飼水控制 (Feedwater Control System, FWC) 系統主要是針對反應爐熱功率進行調節的系統。其控制邏輯如下：當反應爐功率小於25%時，反應爐水位資料會被送入 FWC 系統中，此時 FWC 系統會調節 RWCU 沖放閥流量以維持反應爐水位。當功率更高時，FWC 會調節 LFCV，來控制反應爐水位 。反應爐功率持續上升達 15-20% 時，FWC 會控制 TDRFP 速度控制器 。而當反應爐功率超過 25% 之後，FWC 開始輸入反應爐水位、蒸氣流量與飼水流量並調節 TDREF 速度以控制反應爐水位。

(二) 型態管理

型態管理根據 Cisco 的定義，是由一群流程與輔助工具所組成，其目的在於提升網路一致性 (Network Consistency)、記錄網路變更 (Network Change)，並且提供最新的網路文件與可見性

(Visibility)。因此，正確的型態管理是確保儀控網路安全運作的重要前提之一 ；具體而言，型態管理的目標是讓儀控網路資訊設備在出廠後仍能持續進行校調，以提升有效程度、效率或是安全性；校調範圍涵蓋硬體以及軟體。如果在調整型態之前未經妥善規劃與管理，很可能導致更新後的儀控系統運作失常，間接引發核能發電相關的風險。

因此，本研究先以軟體版本控制管理為例，說明儀控網路應有的軟體版本控管流程，再說明流程中可能遭受的安全威脅，並以 CMsec 加以表達。

Cisco 提出軟體版本控制管理之目的包括了：(1) 將正確版本的軟體更新到功能相同或相容的網路裝置中；(2) 實施管理流程有助於先行測試並驗證軟體的可靠度；(3) 降低因軟體瑕疵導致網路裝置無法協同運作的可能性。針對軟體版本控制的相關步驟如下：(1) 先將儀控網路中的網路裝置加以分類；(2) 將特定軟體版本設定為管理標的；(3) 針對管理標的進行測試、驗證並試運轉；(4) 將通過第 3 步驟的版本擇優視為上線版本；(5) 將上線版本部署於合適的網路裝置上。

(三) 飼水控制系統型態管理安全分析

依照 Cisco 提出軟體版本控制相關步驟，本研究針對飼水控制系統進行軟體版本控制時所面臨的可能風險進行分析，結果如下：

- 管理人員分類不當，導致錯誤的裝置被分在同一類，導致不該更新的網路裝置內的正確狀態被汙染或刪除。
- 管理人員未能取得必要的管理標的。
- 管理人員因疏忽導致測試過程不夠嚴謹，未能發現軟體的內在

缺陷。

- 管理人員所選擇的上線版本有誤，包括了：(1) 未實施應有的軟體更新；(2) 管理人員部署錯誤軟體版本。

針對上述的風險分析，我們透過 CMsec 資訊安全概念模式化方法進行相關安全分析表達。

步驟一：識別威脅代理並劃定其作用範圍

在此步驟中，主要是針對與飼水控制系統進行資料傳輸或交換的相關人員、系統以及設備進行識別與描述。由圖 3.1 中我們可以知道，反應爐偵測器會將偵測到的物理資訊傳給飼水控制系統，而飼水控制系統則會在進行相關資訊判別後，傳送控制訊息到反應爐進行相關的調節。除此之外，飼水控制系統也會將反應爐現場相關資料傳遞給運轉員，而運轉員也能夠針對飼水控制系統回傳的相關的資料進行判別後，下達相關的控制訊息。除了上述的運作外，由於相關的系統及設備需進行型態管理，以提升整體運作的效程度、效率或是安全性。因此設備及儀器廠商進行型態管理時，會傳遞型態管理相關的資訊至系統中。根據安全分析，當設備及儀器廠商進行型態管理資訊更新時，有可能因為人為意外的疏失，導致系統產生安全風險。因此我們識別出人為意外威脅代理並劃定其作用範圍在設備及儀器廠商與飼水控制系統之間，以及其所造成的衝擊程度為高度衝擊 (I:H)。

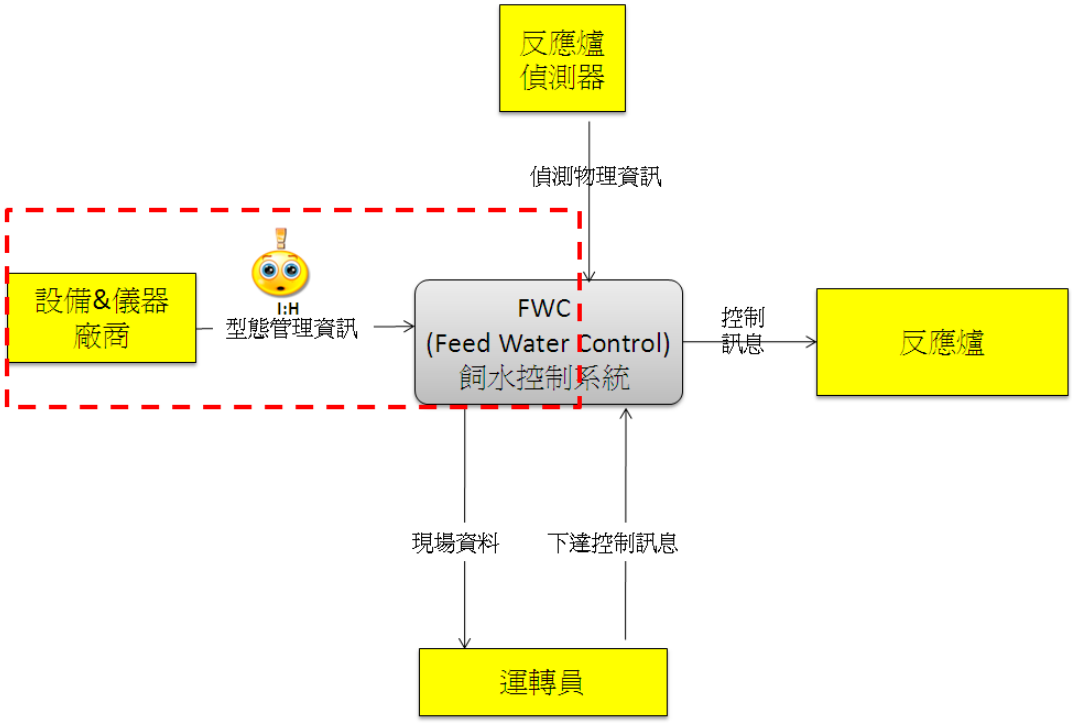

圖 3.1：Level-0 安全分析圖

當我們想要進一步了解飼水控制系統內部運作，並更清楚的了解此威脅代理實際上會對系統中的哪個資產造成威脅時，我們首先將 Level-0 分析圖切割至 Level-1 分析圖，其目的是為了更清楚了解飼水控制系統內部運作的情況以及運作相關的資產。由圖 3.2 我們可以知道，當反應爐偵測器偵測到相關物理資訊時，會透過飼水控制系統內的 FBM 輸入/輸出模組傳遞相關資訊到對應的控制流程。當功率小於 25%時，會傳送加熱階段啟動資訊至 RWCU 的控制流程中，並透過 RWCU 控制流程傳遞控制訊息到反應爐。當功率介於 15-20%時，會傳送相關資訊至 LFCV 控制流程中，並透過 LFCV 控制流程傳遞控制訊息到反應爐。而當功率超過 25%時則會傳送資訊至 TDRFP 蒸氣推動飼水訊號流程中，並透過 TDRFP 控制流程傳遞控制訊息到反應爐。除此之外，反應爐偵測器所偵測到的物理資訊

也會透過 FBM 輸入/輸出模組傳遞偵測到的資訊，透過 FCM 通訊模組、CP 控制處理器、CN 控制網路以及中控室電腦處理傳送相關偵測資訊給運轉員，而運轉員也可以透過此路徑傳遞相關的控制指令回 FBM 輸入/輸出模組，以進行反應爐的控制。

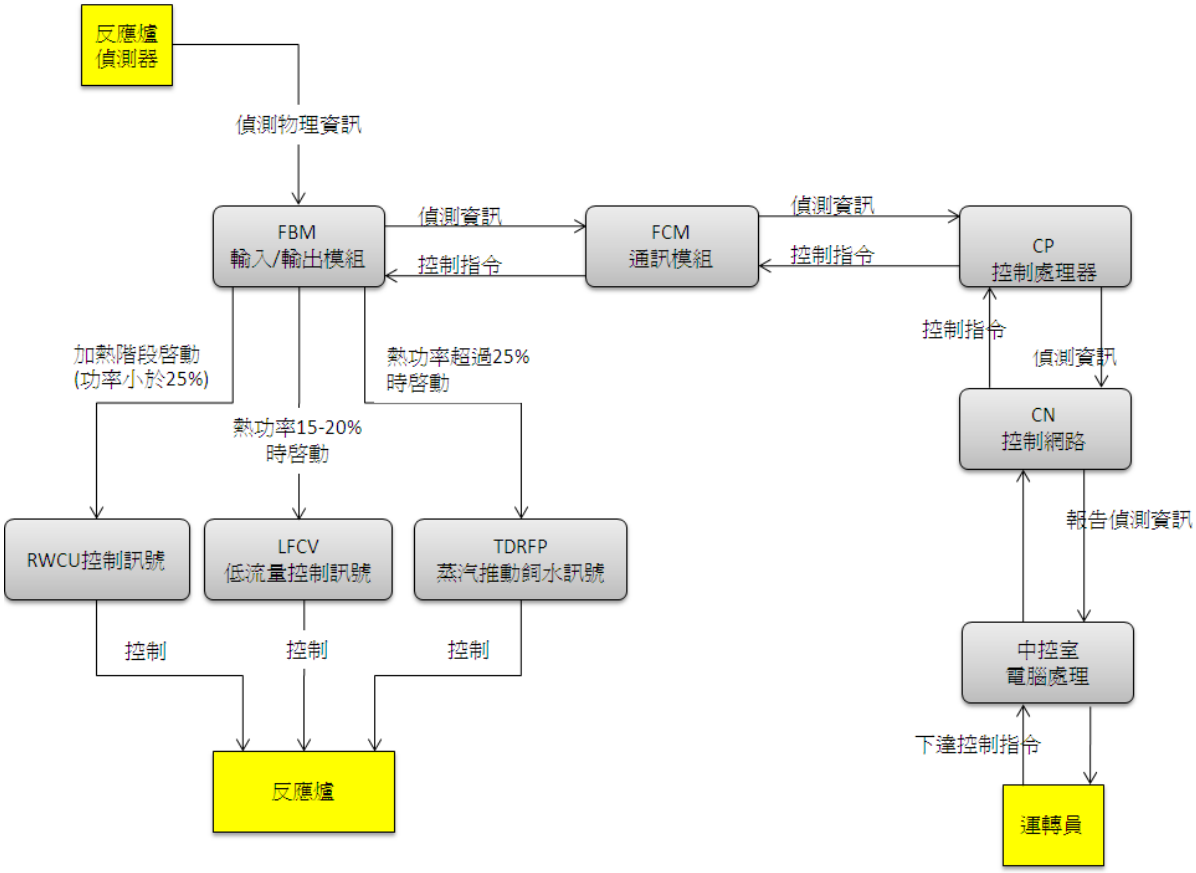

圖 3.2：Level-1 分析圖

對於飼水控制系統的型態管理，設備儀器及軟硬體廠商會對 CN 控制網路、CN 控制處理器、FCM 通訊模組以及 FBM 通訊模組進行相關的管理。因此會透過 CN 控制網路型態管理流程、CN 控制處理器型態管理流程、FCM 通訊模組型態管理流程以及 FBM 通訊模組型態管理流程傳遞相關型態管理資訊，如圖 3.3 所示。此時，

我們仍然無法識別出威脅會作用在系統哪個資產之中，因此我們仍然透過威脅代理人並劃定其作用範圍來進行表示，並針對作用範圍進行更進一步的安全分析。

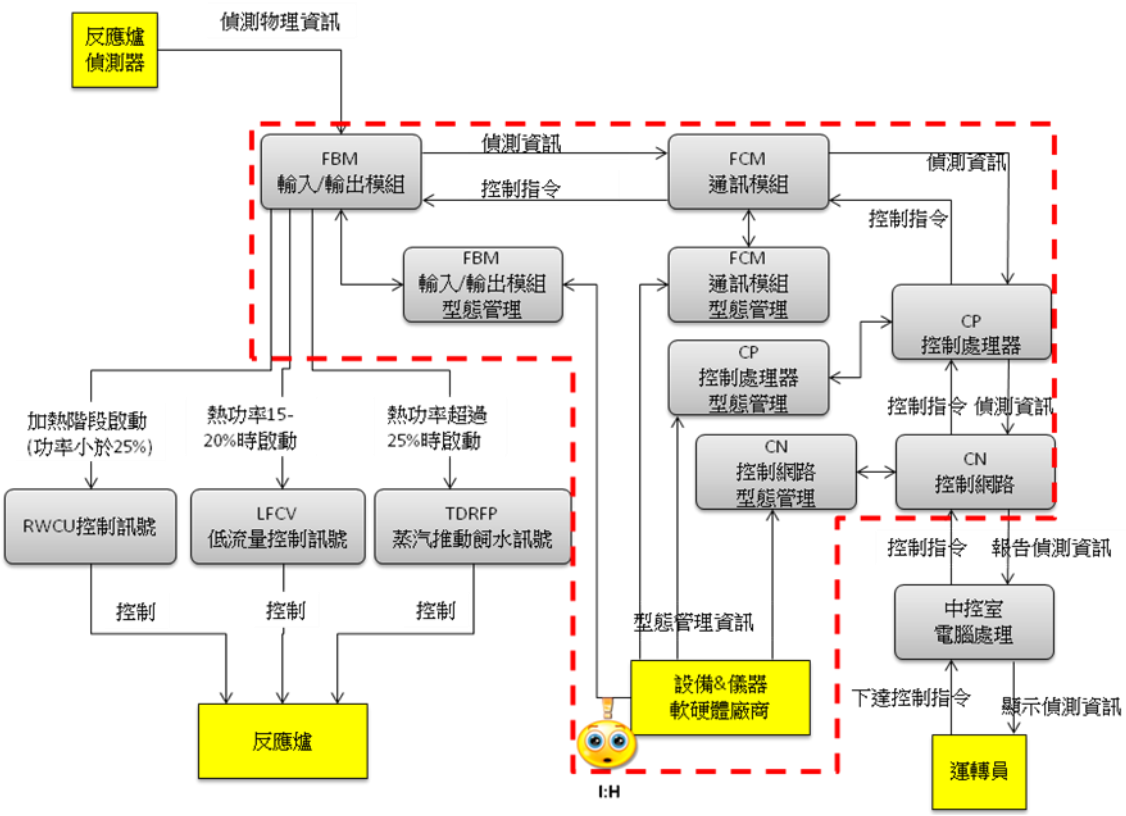

圖 3.3：Level-1 安全分析圖

步驟二：識別威脅及作用資產

由上述可知，從 Level-1 安全分析圖中我們仍然無法識別威脅用的資產，因此我們將分析圖再進行切割至下一層，其目的是為了更清楚了解當設備軟硬體廠商進行型態管理時相關的管理流程以及所對應的資產，並識別出威脅代理所作用的資產。由圖 3.4 及第二節提到之型態管理步驟可知，當設備儀器及軟硬體廠商進行軟體版本的型態管理的第一步驟時，會先針對網路裝置加以分類，並將分類

的結果儲存至資產清單資料庫之中。在進行分類後，會將所欲進行型態管理之軟硬體更新資訊設定相關的管理標的，接著產生測試計畫，並依照計畫進行測試、驗證以及試運轉。經測試、驗證及試運轉確認無誤後便能將之視為正式的更新軟體，並透過各模組及裝置更新流程將更新程序傳送至各個模組及裝置資料庫中，模組及裝置便能透過資料庫的更新來進行相關型態的變更。

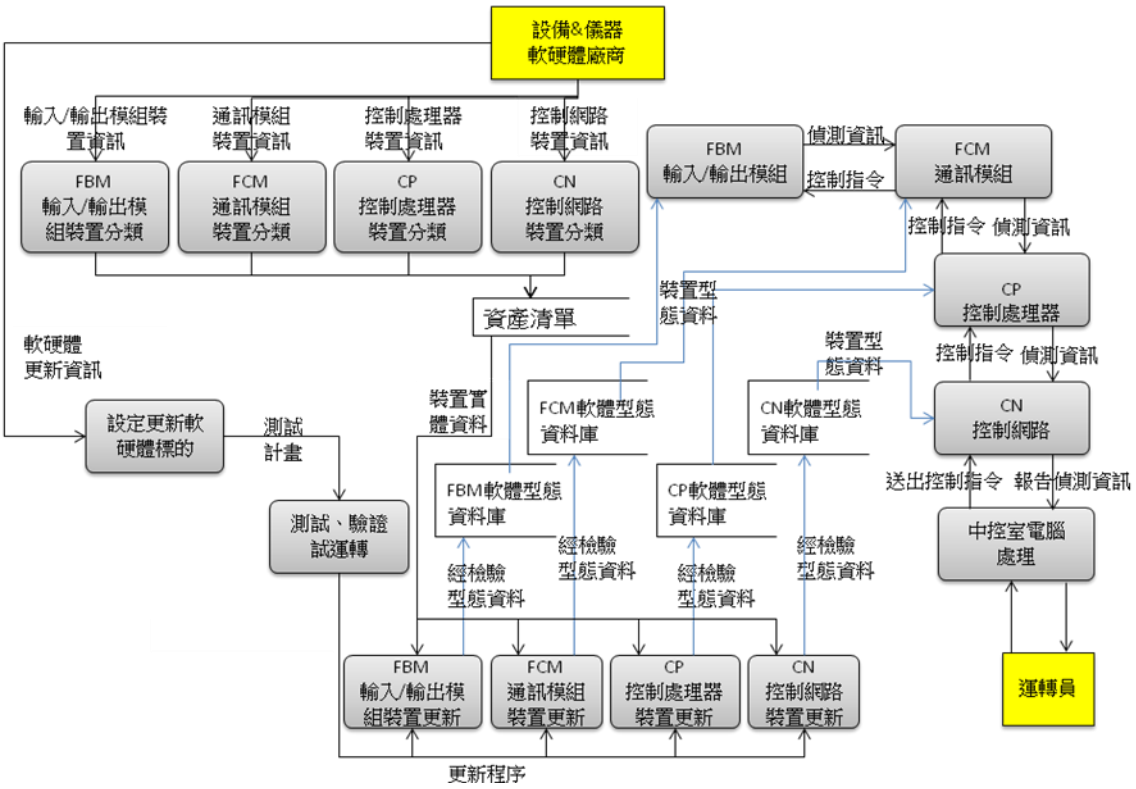

圖 3.4：Level-2 分析圖

從 Level-2 分析圖中，我們已經可以清楚的對相關威脅及其作用資產進行識別。由第三節飼水控制系統型態管理安全分析我們可以知道，當在進行裝置的分類時可能會因為錯誤的裝置被分在同一類，導致不該更新的網路裝置內的正確狀態被汙染或刪除，因此在圖 3.5 中我們可以識別出對於 FBM 輸入/輸出模組裝置分類、FCM

通訊模組裝置分類、CP 控制處理器裝置分類、CN 控制網路裝置分類，可能受到人為意外的分類錯誤的威脅。在進行分類後，會開始針對更新資訊設定管理標的，根據飼水控制系統型態管理安全分析，管理人員有可能未能取得必要的管理標的，導致意外的設定錯誤的管理標的，因此在圖 3.5 中我們可以識別出設定更新軟硬體標的流程，可能會受到意外的設定錯誤管理標的威脅。

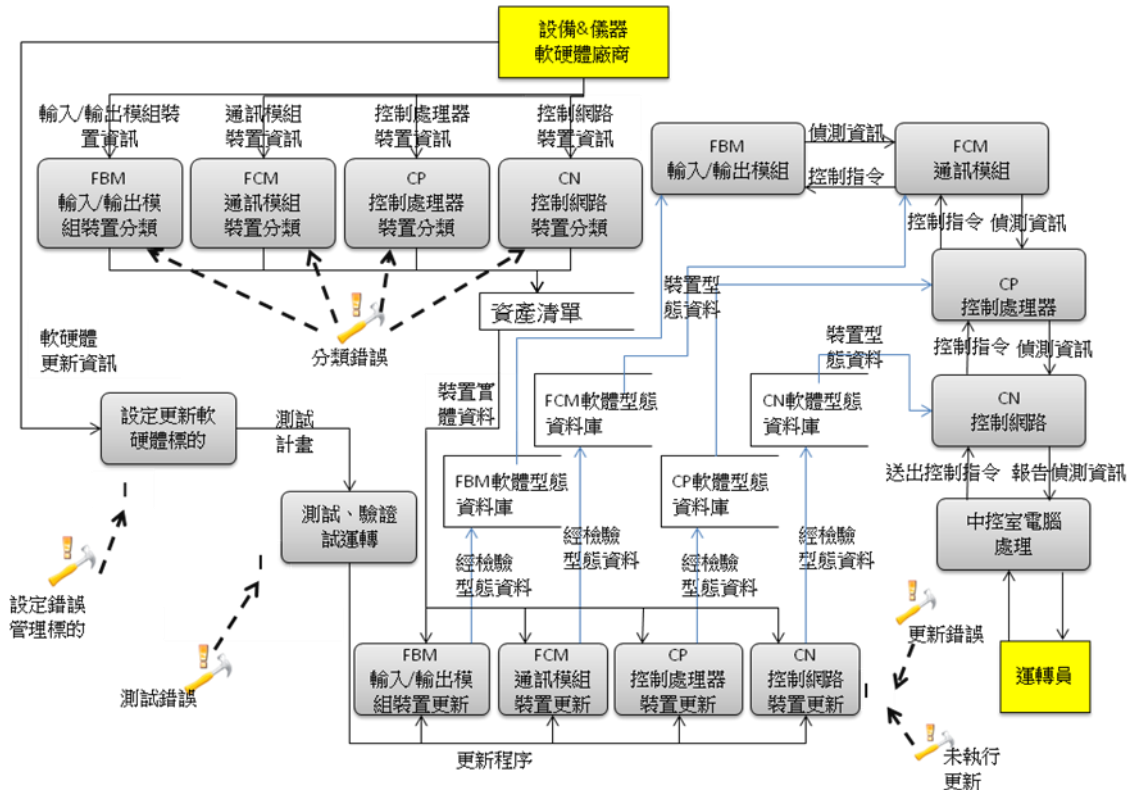

圖 3.5：Level-2 安全分析圖

在測試、驗證以及試運轉的過程中，根據飼水控制系統型態管理安全分析，管理人員可能因疏忽導致測試過程不夠嚴謹，未能發現軟體的內在缺陷。在圖 3.5 中我們可以識別出測試、驗證以及試運轉流程，可能會受到意外測試錯誤的威脅。在進行測試、驗證及

試運轉後，確定無誤之軟體版本便可以透過各模組及裝置更新流程進行軟體版本之更新。根據飼水控制系統型態管理安全分析指出，管理人員可能會選擇有誤的上線版本，包括了軟體佈署未實施以及管理人員佈署錯誤軟體版本。在圖 3.5 中我們可以識別出各模組及裝置更新流程，可能會受到意外的未執行更新以及意外的更新錯誤的威脅。

四、結論與效益

(一) 結論

1. 發展中核能安全標準相關研究

本研究針對與核能電廠有關之資訊安全相關標準和法規指引進行研究，包括底下幾項：

- 前期標準回顧
  - NERC CIP-002-3 ~ CIP-009-3
  - DI&C-ISG-04
- 本期標準研讀
  - 10 CFR 73.1: “Purpose and Scope”
  - 10 CFR 73.54: “Protection of Digital Computer and Communication Systems and Networks”
  - 10 CFR 73.55: “Requirements for Physical Protection of Licensed Activities in Nuclear Power Reactors against Radiological Sabotage”
  - RG 1.152: “Criteria for Use of Computers in Safety Systems of Nuclear Power Plants”
  - RG 5.71: “Cyber Security Programs for Nuclear Facilities”

其中，又以 RG 5.71 為本年度之重要研究對象。

2. 核能電廠儀控系統資安評估項目

本研究透過對 RG 5.71 的瞭解，取其安全控制項目作為核能電廠數位儀控系統之資安評估項目，並且將這些項目依據不同觀點分為四大類，分別是：技術觀點、操作觀點、管理觀點與深度防禦觀點。

3. 核能電廠儀控系統流程安全弱點分析方法設計

本研究提出一套考量安全性的系統分析方法論，可表達出資訊系統中的安全弱點、威脅、攻擊與防禦機制，並且以圖形化方式呈現。

4. 應用安全弱點分析方法加強核能電廠資安於型態管理之作法

利用前一點所提安全弱點分析方法，本研究針對核能電廠儀控系統流程進行安全弱點分析，以飼水控制系統為分析對象，針對飼水控制系統之型態管理進行安全弱點分析，以加強核能電廠資安於型態管理之作法。

(二) 主要效益

本研究成果所產生的主要效益如下：

- 本計畫的執行成果可以協助核能電廠建立其數位儀控系統之資安評估項目，以作為制訂網路安全計畫 (Cyber Security Plan) 之重要基礎。
- 所設計之圖形化安全弱點分析方法，能夠為核能電廠儀控系統

流程進行清楚的安全弱點與可能遭受威脅之描述，並能加強核能電廠型態管理於資訊安全之作法。

- 藉由所描述之安全弱點與威脅所在以及相對應之防禦對策，除了可供核電廠瞭解自身數位儀控系統的弱點所在，以加強型態管理之安全，對於支援原能會核電廠數位儀控系統審查管制將有所助益。

參考文獻

[1] U.S. NRC, “ISG-04 Control Room Communications,” 2007.

[2] U.S. NRC, “RG-5.71 Cyber Security Program for Nuclear Facilities,” 2009.

[3] NERC, “Critical Infrastructure Protection (CIP),” 2006.

[4] NRC, http://www.nrc.gov/.

[5] NERC, http://www.nerc.com/.

[6] WANO, http://www.wano.org.uk/.

[7] 「97 年核能電廠異常事件統計分析」,行政院原子能委員會核能管制處，2007 年。

[8] 「龍門電廠數位儀控網路 ISG-04 適用性評估報告」，行政院原子能委員會核能研究所，2009 年。

[9] 行政院原子能委員會，http://www.aec.gov.tw/www/index.php。

[10]財團法人核能資訊中心，http://www.nicenter.org.tw/modules/news/。

[11]台灣電力公司，http://www.taipower.com.tw/。