TARGET	POSSIBLE ATTACK VECTORS	POSSIBLE ATTACK METHODS	POSSIBLE CONSEQUENSES
ACCESS CONTROL SYSTEM	• Identification cards • Closed-circuit television (CCTV) • Building management network • Software vendor support portal	• Exploitation of unpatched application (building management systems) • RFID spoofing • Network access through unprotected access points • Network pivoting through unregulated network boundaries	• Unauthorized physical access • Lack of (video) detection capabilities • Unauthorized access to additional ICS assets (pivoting)
ANALYZERS/ANALYZER MANAGEMENT SYSTEM	• Subcontractor Laptop • Maintenance remote access • Plant (analyzer network)	• Exploitation of unpatched application • Network access via insecure access points (analyzer shelters) • Remote access VPN via stolen or compromised subcontractor laptop • Remote Access VPN via compromise of maintenance vendor site • Insecure implementation of OPC (protocol)	• Product quality – spoilage, loss of production, loss of revenue • Reputation – product recall, product reliability
APPLICATION SERVERS	• Remote user access (interactive sessions) • Business application integration communication channel • Plant network • Software vendor support portal	• Exploitation of unpatched application • Installation of malware via unvalidated vendor software • Remote access via interactive accounts • Database injection • Insecure implementation of OPC	• Plant upset/shutdown • Credential leakage (control) • Sensitive/confidential information leakage • Unauthorized access to additional ICS assets (pivoting)
ASSET MANAGEMENT SYSTEM	• Plant Maintenance Software/erp • Database integration functionality • Mobile devices used for device configuration • Wireless device network	• Exploitation of unpatched application • Installation of malware via unvalidated vendor software • Remote access via interactive accounts • Database injection • Installation of malware via mobile devices	• Calibration errors-product quality • Credential leakage (business) • Credential leakage (control) • Unauthorized access to additional business assets like plant maintenance/ERP (pivoting)

	• Software vendor support portal	• Access via insecure wireless infrastructure	• Unauthorized access to additional ICS assets (pivoting)
CONDITION MONITORING SYSTEM	• Subcontractor laptop • Maintenance remote access • Plant (maintenance) network • Software vendor support portal	• Exploitation of unpatched application • Installation of malware via unvalidated vendor software • Network access via unsecure access points (compressor/pump house) • Remote access VPN via stolen or compromised subcontractor laptop • Remote access VPN via compromise of maintenance vendor site • Remote access via interactive accounts • Database injection • Insecure implementation of OPC	• Equipment damage/sabotage • Plant upset/shutdown • Unauthorized access to additional ICS assets (pivoting)
CONTROLLER (PLC)	• Engineering workstation • Operator HMI • Standalone engineering tools • Rogue device in control zone • USB/removable Media • Controller network • Controller device network	• Engineer/technician misuse • Network exploitation of industrial protocol – known vulnerability • Network exploitation of industrial protocol – known functionality • Network replay attack • Network DoS via communication buffer overload • Direct Code/malware injection via USB • Direct access to device via rogue network (local/remote) PC with appropriate tools/software)	• Manipulation of controlled processes • Controller fault condition • Manipulation/masking of input/output date to/from controller • Plant upset/shutdown • Command-and-control
DATA HISTORIAN	• Business network client • ERP data integration communication channel • Database integration communication channel	• Exploitation of unpatched application • Installation of malware via unvalidated vendor software • Remote access via interactive accounts • Database injection	• Manipulation of process/batch records • Credential leakage (business) • Credential leakage (control) • Unauthorized access to additional business assets like MES, ERP (pivoting)

	• Remote user access (interactive session) • Plant network • Software vendor support portal	• Insecure implementation of required communication protocols • Exploitation of unnecessary/excessive openings on perimeter defense (firewall) due to insecure communication infrastructure between applications	• Unauthorized access to additional ICS assets (pivoting)
DIRECTORY SERVICES	• Replication services • Print spooler services • File sharing services • Authentication services • Plant network • Software vendor support portal	• Exploitation of unpatched applications • Installation of malware via unvalidated vendor software • DNS spoofing • NTP reflection attack • Exploitation of unnecessary/excessive openings on perimeter defense (firewall) due to replication requirements between servers • Installation of malware on file shares	• Communication disruptions via DNS • Authentication disruptions via NTP • Authentication disruptions via LDAP/Kerberos • Credential leakage • Information leakage – file shares • Malware distribution • Unauthorized access to all domain-connected ICS assets (pivoting) • Unauthorized access to business assets (pivoting)
ENGINEERING WORKSTATIONS	• Engineering tools and applications • Non-engineering client applications • USB/removable media • Elevated privileges (engineer/administrator) • Control network • Software vendor support portal	• Exploitation of unpatched applications • Installation of malware via unvalidated vendor software • Installation of malware via removable media • Installation of malware via keyboard • Exploitation of trusted connections across security perimeters • Authorization to ICS applications without sufficient access control mechanisms	• Plant upset / shutdown • Delay plant startup • Mechanical damage / sabotage • Unauthorized manipulation of operator graphics –inappropriate response to process action • Unauthorized modification of ICS databases • Unauthorized modification of critical status alarms • Unauthorized distribution of faulty firmware • Unauthorized startup/shutdown of ICS devices

			• Process/plant information leakage • ICS design application credential leakage • Unauthorized modifications of ICS access control mechanisms • Unauthorized access to most ICS assets (pivoting/own) • Unauthorized access to business assets (pivoting)
ENVIRONMENTAL CONTROL	• HVAC control • HVAC building management network • Software vendor support portal	• Exploitation of unpatched application (building management system) • Installation of malware via unvalidated vendor software • Network access through unprotected access points • Network pivoting through unregulated network boundaries	• Disruption of cooling/heating • Equipment failure /shutdown
FIRE DETECTION AND SUPPRESSION SYSTEM	• Fire alarm/evaluation • Fire suppressant system • Building management network • Software vendor support portal	• Exploitation of unpatched application (building management system) • Installation of malware via unvalidated vendor software • Network access through unprotected access points • Network pivoting through unregulated network boundaries	• Unauthorized release of suppressant • Equipment filure/shutdown
MASTER AND/OR SLAVE DEVICES	• Unauthorized /unvalidated firmware • Weak communication problems • Insufficient authentication for write operations • Control network	• Distribution of malicious firmware • Exploitation of vulnerable industrial protocols via rogue PC on network (local/remote) • Exploitation of vulnerable industrial protocols via compromised PC on network (local)	• Plant upset/shutdown • Delay plant start • Mechanical damage/sabotage • Inappropriate response to control action • Suppression of critical status/alarms

	• Device network	• Exploitation of industrial protocol functionality via compromised PC on network (local/remote) • Communication buffe overvlow via compromised PC on network (local)	
OPERATOR WORKSTATION (HMI)	• Operational applications (HMI) • Non-SCADA client applications • USB/removable media • Elevated privileges (administrator) • Control Network • Software vendor support portal	• Exploitation of unpatched applications • Installation of malware via unvalidated vendor software • Installation of malware via removable media • Installation of malware via keyboard • Authorization to ICS HMI functions without sufficient access control mechanisms	• Plant upstet/shutdown • Suppression of critical status/alarms • Product quality • Plant/process efficiency • Credential leakage (control) • Plant/operational information leakage • Unauthorized access to ICS assets (pivoting) • Unauthorized access to ICS assets (communication protocols)
PATCH MANAGEMENT SERVERS	• Software patches/hotfixes • Patch management software • Vendor software support portal • Business network • Plant network • Software vendor support portal	• Insufficient checking of patch "health" before deployment • Alternation of automatic deployment schedule • Installation of malicious software via trusted supplier media • Installation of malware via unvalidated vendor software	• Malware distribution server • Unauthorized modification of patch schedule • Credential leakage • Unauthorized access to ICS assets (pivoting)
PERIMETER PROTECTION (FIREWALL/IPS)	• Trusted connections (business-to-control) • Local user account database • Signature/rule updates	• Untested/unverified rules • Exploitation of unnecessary/excessive openings on perimeter defense (firewall) • Insecure office and industrial protocols allowed to cross security perimeter • Reuse of credentials across boundary	• Unauthorized access to business network • Unauthorized access to DMZ network • Unauthorized access to control network • Local credential leakage • Unauthorized modification of rulesets/signatures

			• Communication disruption across perimeter/boundary
SCADA SERVERS	• Non-SCADA client applications • Application integration communication channels • Data Historian • Engineering workstation • Control network • Software vendor support portal	• Exploitation of unpatched applications • Installation of malware via unvalidated vendor software • Remote access via interactive accounts • Installation of malware via removable media • Exploitation of trusted connections within control network • Authorization to ICS applications without sufficient access control mechanisms	• Plant Upset/shutdown • Delay plant startup • Mechanical damage/sabotage • Unauthorized manipulation of operator graphics – inappropriate response to process action • Unauthorized modification of ICS databases • Unauthorized startup/shutdown of ICS devices • Credential leakage (control) • Plant/operational information leakage • Unauthorized modifications of ICS access control mechanisms • Unauthorized access to most ICS assets (pivoting/own) • Unauthorized access to ICS assets (communication protocols) • Unauthorized access to business assets (pivoting)
SAFETY SYSTEMS	• Safety engineering tools • Plant /emergency shutdown communication channels (DCS/SCADA) • Control safety network • Software vendor support portal	• Exploitation of unpatched applications • Installation of malware via unvalidated vendor software • Installation of malware via removable media • Installation of malware via keyboard • Authorization to ICS applications without sufficient access control mechanisms	• Plant shutdown • Equipment damage/sabotage • Environmental impact • Loss of life • Product quality • Company reputation

TELECOMMUNICATIONS SYSTEMS	• Public key infrastructure • Internet visibility	• Disclosure of private key via external compromise • Exploitation of device unknowingly connected to public networks • Network access through unmonitored access points • Network pivoting through unregulated network boundaries	• Credential leakage (control) • Information leakage • Unauthorized remote access • Unauthorized access to ICS assets (pivoting) • Command and control
UNINTERRUPTIBLE POWER SYSTEMS (UPS	• Electrical management network • Vendor/subcontractor maintenance	• Exploitation of unpatched application (building management systems) • Installation of malware via unvalidated vendor software • Network access through unprotected access points • Network pivoting through unregulated network boundaries	• Equipment failure/shutdown • Plant upset/ shutdown • Credential leakage • Unauthorized access to ICS assets (pivoting)
USER – ICS ENGINEER	• Social engineering – corporate assets • Social engineering – personal assets • E-mail attachments • File shares	• Introduction of malware through watering hole or spear-phising attack on business PC • Introduction of malware via malicious email attachment on business PC from trusted source • Introduction of malware on control network via unauthorized/foreign host • Introduction of malware on control network via shared virtual machines • Introduction of malware via inappropriate use of removable media between security zones (home-business-control) • Propagation of malware due to poor segmentation and full visibility from EWS (engineering works station)	• Process/plant information leakage • ICS design/application credential leakage • Unauthorized access to business assets (pivoting) • Unauthorized access to ICS assets (pivoting/own)

		• Establishment of a C2 via inappropriate control-to-business connections • Exploitation of communication channels resulting from unapproved architecture changes • Exploitation of applications due to unnecessary use of administrative rights • Exploitation of applications due to failure to logout/disconnect when unused	
USER – ICS TECHNICIAN	• Social engineering – corporate assets • Social engineering – personal assets • E-mail attachments • File shares	• Introduction of malware on control network via unauthorized/foreign host • Introduction of malware on control network via shared virtual machines • Introduction of malware via inappropriate use of removable media between security zones (home-business-control) • Exploitation of applications due to unnecessary use of administrative rights • Network disturbances resulting from connection to network with poor segmentation	• Plant upset/shutdown • Delay plant startup • Mechanical damage /sabotage • Unauthorized manipulation of operator graphics – inappropriate response to process action • Unauthorized modification of status /alarm settings • Unauthorized download of faulty firmware • Unauthorized startup /shutdown of ICS devices • Design information leakage • ICS application credential leakage • Unauthorized access to most ICS assets (pivoting/own)
USER – PLANT OPERATOR	• Keyboard • Removable Media – USB • Removable Media – CD/DVD	• Introduction of malware on control network via unauthorized /foreign host • Introduction of malware via inappropriate use of removable media between security zones (home-business-control)	• Plant upset/shutdown • Mechanical damage /sabotage • Unauthorized startup/shutdown of mechanical equipment

	• Exploitation of applications due to unnecessary use of administrative rights	• Process/plant operational information leakage • Credential leakage • Unauthorized access to ICS assets (pivoting) • Unauthorized access to ICS assets (communication protocols)

Source :
Industrial network security Securing critical infrastructure netwoks for smart grid, SCADA, and other industrial control systems (Second edition)

– Eric D. Knapp & Joel Thomas Langill