1-IoT-Enabled Manufacturing Plant

Asset	Threat / Vulnerability	Existing Controls	Likelihood	Consequence (1–6)	Level of Risk	Risk Priority
1. Programmable Logic Controllers (PLCs)	Malware injection via unpatched firmware	Network segmentation (plant VLAN); periodic firmware updates	Possible	5 (Catastrophic)	High	1
2. Robotic Arm Controllers	Unauthorized command injection (weak authentication)	Role-based access control; strong passwords	Possible	4 (Major)	High	2
3. IoT Temperature Sensors	Tampering/spoofing of sensor data	Sensor-to-gateway TLS encryption; physical tamper switches	Likely	4 (Major)	Extreme	3
4. Manufacturing Execution System (MES) Server	SQL injection or privilege escalation	WAF in front; strict input validation; hardened OS	Unlikely	5 (Catastrophic)	High	4
5. CNC Machine (networked)	Ransomware deployment through infected USB or network share	USB port lockdown; endpoint AV; scheduled backups	Possible	4 (Major)	High	5
6. Wireless Industrial Access Points	Rogue AP insertion / Wi-Fi phishing	WPA3 with strong passphrase; 802.1X authentication; wireless IDS	Possible	3 (Moderate)	Medium	6
7. Employee Workstations (factory floor)	Inadequate patching leading to exploit	Automated patch management; EDR solution	Possible	3 (Moderate)	Medium	7

8. Environmental Monitoring Cameras	Video feed eavesdropping or unauthorized tampering	Encrypted video streams; camera-firmware PIN; VLAN isolation	Unlikely	3 (Moderate)	Low	8
9. Core Network Switches	Unauthorized configuration change (default SNMP, no MFA)	Secure SNMPv3; TACACS+ for admin access; configuration backups	Unlikely	4 (Major)	Medium	9
10. Physical Access Control Panel	Card reader cloning / tampering	Tamper-evident enclosure; CCTV monitoring; quarterly lock inspection	Unlikely	3 (Moderate)	Low	10

2. Smart Hospital

Asset	Threat / Vulnerability	Existing Controls	Likelihood	Consequence (1–6)	Level of Risk	Risk Priority
1. Patient Vital-Sign Monitors	False data injection (no integrity checks)	TLS 1.2+ encryption; periodic device audits	Possible	5 (Catastrophic)	High	1
2. Infusion Pumps (networked)	Unauthorized dosage manipulation (weak default credentials)	Unique strong credentials; central patch management	Likely	5 (Catastrophic)	Extreme	2
3. Electronic Health Record (EHR) Server	Ransomware or data breach (incomplete backups)	Daily encrypted backups; EDR; WAF; network segmentation	Unlikely	6 (Doomsday)	Extreme	3
4. MRI/CT Imaging System	Malware from external USB or network share	USB port control; OS hardening; restricted admin privileges	Possible	5 (Catastrophic)	High	4
5. Smart Infusion Monitoring Network	Replay attacks on patient alarms	Network time-sync over TLS; anomaly detection in SIEM	Possible	4 (Major)	High	5
6. Nurse Workstations	Phishing-delivered credential theft	Email filtering; 2FA; regular phishing simulations	Likely	4 (Major)	Extreme	6
7. HVAC Building Automation System	Insider change of set-points or denial of service	VLAN isolation; MFA for admin console; runtime integrity monitoring	Possible	4 (Major)	High	7

8. Hospital Mobile Devices (BYOD)	Data leakage via unsecured health apps	MDM enforcement; containerization; VPN requirement	Possible	3 (Moderate)	Medium	8
9. Pharmacy Automated Dispensing Cabinet	Unauthorized override (weak audit/logging)	Role-based access; tamper-evident seals; audit logging	Unlikely	4 (Major)	Medium	9
10. Visitor-Area Surveillance Cameras	Video feed interception / tampering	Encrypted video streams; access logged in SIEM; tamper alarms	Unlikely	3 (Moderate)	Low	10

3. IoT-Enabled Bank

Asset	Threat / Vulnerability	Existing Controls	Likelihood	Consequence (1–6)	Level of Risk	Risk Priority
1. ATM Machines (networked)	Skimming malware / remote takeover	Anti-skimming hardware; OS hardening; encrypted PIN pads	Possible	5 (Catastrophic)	High	1
2. Core Banking Server	SQL injection / unauthorized data access	WAF; RBAC; database encryption at rest & in transit	Unlikely	6 (Doomsday)	Extreme	2
3. Biometric Access Readers	Spoofed biometric data (no liveness detection)	Dual-factor authentication (badge + fingerprint); periodic calibration	Possible	4 (Major)	High	3
4. Teller Workstations	Phishing leading to credential compromise	EDR; email filtering; mandatory 2FA	Likely	4 (Major)	Extreme	4
5. Smart Safe (IoT-connected)	Remote unlocking via exploit	Encrypted communications; HSM for key management; tamper detection	Possible	5 (Catastrophic)	High	5
6. Customer VLAN Router (Branch)	Rogue device insertion / weak WPA2	WPA3 with strong passphrase; 802.1X for staff; NAC for unknown devices	Possible	3 (Moderate)	Medium	6
7. Mobile Banking App Server	API abuse / DoS	API gateway with rate-limiting; WAF; autoscaling	Unlikely	5 (Catastrophic)	High	7

8. Core Network Switches	Unauthorized config change (default SNMP, no MFA)	SNMPv3; TACACS+; config backups	Unlikely	4 (Major)	Medium	8
9. Physical Access Control System	Card cloning / insider tampering	Tamper logs; CCTV; quarterly card-reader audits	Unlikely	3 (Moderate)	Low	9
10. Branch Surveillance Cameras	Video feed interception / tampering	Encrypted feeds; access restrictions in VMS; tamper-evident mounts	Unlikely	3 (Moderate)	Low	10

4. Smart University Campus

Asset	Threat / Vulnerability	Existing Controls	Likelihood	Consequence (1–6)	Level of Risk	Risk Priority
1. Student ID Card Readers (dorms)	Card cloning / unauthorized entry	Multi-factor (card + PIN); tamper-evident casing; audit logs	Possible	4 (Major)	High	1
2. Smart Classroom Projectors	Ransomware via infected USB or network share	USB port lockdown; OS patching; network access restricted to classroom VLAN	Possible	3 (Moderate)	Medium	2
3. Campus Wi-Fi Access Points	Rogue AP insertion / weak WPA2 deployment	WPA3 Enterprise (802.1X); RADIUS authentication	Likely	3 (Moderate)	High	3
4. Laboratory IoT Environmental Sensors	Data spoofing (no integrity checks)	TLS 1.2 encryption; periodic sensor calibration; VLAN isolation	Possible	3 (Moderate)	Medium	4
5. University Database Server	SQL injection / unauthorized data download	WAF; RBAC; database encryption; quarterly code audits	Unlikely	5 (Catastrophic)	High	5
6. Faculty Workstations	Phishing / credential theft	EDR; email filtering; mandatory 2FA	Likely	4 (Major)	Extreme	6

7. Dorm IoT Thermostats	Default credentials / remote temperature manipulation	Default password change; secure TLS-based management; network ACLs	Likely	3 (Moderate)	High	7
8. EV Charging Stations	Firmware compromise (no secure update mechanism)	Signed firmware enforcement; charging-station VLAN; periodic integrity checks	Possible	4 (Major)	High	8
9. Physical Access Control Kiosks	Card reader jamming / insider tampering	CCTV monitoring; tamper-evident seals; daily access log review	Unlikely	3 (Moderate)	Low	9
10. Campus Surveillance Cameras	Video feed eavesdropping or DoS	Encrypted video streams; NVRs with RBAC; UPS to prevent outages	Unlikely	3 (Moderate)	Low	10

5. Smart Retail Store

Asset	Threat / Vulnerability	Existing Controls	Likelihood	Consequence (1–6)	Level of Risk	Risk Priority
1. Smart POS Terminals	Malware injection via compromised payment card readers	PCI-DSS compliance; POS whitelisting; endpoint AV	Possible	5 (Catastrophic)	High	1
2. Inventory RFID Reader System	Replay/spoofing of RFID tags (no encryption)	TLS encryption between RFID gateway and backend; tag authentication	Likely	4 (Major)	Extreme	2
3. Smart Shelves (weight sensors)	Data spoofing (no tamper detection)	VLAN isolation; encrypted MQTT; periodic calibration	Possible	3 (Moderate)	Medium	3
4. Digital Signage Displays	Unauthorized content push (weak default credentials)	Unique strong credentials; scheduled firmware updates; screen lockdown	Possible	3 (Moderate)	Medium	4
5. Customer Wi-Fi Access Points	Rogue AP insertion / weak WPA2 settings	WPA3 Enterprise; RADIUS authentication; NAC	Likely	3 (Moderate)	High	5
6. Retail Database Server	SQL injection / privileged escalation	WAF; RBAC; encryption at rest & in transit; periodic pentesting	Unlikely	5 (Catastrophic)	High	6

7. Employee Workstations	Phishing / credential theft	EDR; email filtering; mandatory 2FA; security awareness training	Likely	4 (Major)	Extreme	7
8. Smart HVAC Control System	Insider manipulation of set points	VLAN isolation; MFA for admin; runtime integrity checks	Possible	4 (Major)	High	8
9. Smart Lighting Controllers	Unauthorized remote shutoff (default creds)	Unique strong credentials; TLS encryption; device-level ACLs	Possible	3 (Moderate)	Medium	9
10. Surveillance Cameras	Video feed interception / tampering	Encrypted RTSP; NVR RBAC; tamper detection alerts	Unlikely	3 (Moderate)	Low	10