

TABLE DE MATIERES

1	GENERALITE SUR LES SYSTEMES ISC/SCADA	1
1.1	DEFINITIONS	1
1.1.1	IT	1
1.1.2	OT	2
1.1.3	ICS	2
1.1.4	SCADA	3
1.1.5	DCS	4
1.1.6	SIS	4
1.2	ARCHITECTURE D'UN ICS	5
1.2.1	COUCHE DE TERRAIN	6
1.2.2	COUCHE DE CONTROLE	6
1.2.3	COUCHE DE SUPERVISION	7
1.2.4	COUCHE D'ENTREPRISE	7
1.3	ÉVOLUTION DE L'ARCHITECTURE DES SYSTEMES SCADA	8
1.3.1	PREMIERE GENERATION : « SYSTEMES SCADA MONOLITHIQUES »	8
1.3.2	DEUXIEME GENERATION : « SYSTEMES SCADA DISTRIBUES »	9
1.3.3	TROISIEME GENERATION : « SYSTEMES SCADA EN RESEAU »	9
1.3.4	QUATRIEME GENERATION « SYSTEME SCADA DE L'INDUSTRIE 4.0 »	10
1.4	ELEMENTS ET FONCTIONNEMENT DU SYSTEME SCADA	10
1.4.1	CENTRE DE CONTROLE	11
1.4.1.1	IHM (Interface Homme Machine)	12
1.4.1.2	Serveur SCADA	13
1.4.1.3	Serveur (Historian)	13
1.4.2	DISPOSITIFS DE TERRAIN	13
1.4.2.1	PLC	14
1.4.2.2	RTU	15
1.4.2.3	Dispositifs électroniques intelligents	15
1.5	PROTOCOLES EMPLOYES DANS UN ENVIRONNEMENT ICS	16
1.5.1	MODBUS	16

1.5.1.1	Modbus série	18
1.5.1.2	Modbus TCP	18
1.5.2	PROTOCOLE DE RESEAU DISTRIBUE DNP3	19

2 MENACES DANS LES SYSTEMES INDUSTRIELS 21

2.1	DIFFERENCES ENTRE LES SYSTEMES IT ET OT	21
2.1.1	NATURE DES DONNEES	22
2.1.2	ARCHITECTURE TECHNOLOGIQUE	23
2.1.3	SECURITE	23
2.1.4	DUREE DE VIE DES SYSTEMES	24
2.2	CONVERGENCE IT/OT	24
2.3	OBJECTIFS DE LA CYBERSECURITE DES ICS	25
2.4	MENACES SUR LES SYSTEMES ICS/SCADA	27
2.4.1	MENACES INTERNES	29
2.4.1.1	Menaces intentionnelles	29
2.4.1.2	Menaces involontaires/accidentelles	30
2.4.2	MENACES EXTERNES	30
2.4.2.1	Catastrophes naturelles	30
2.4.2.2	Catastrophes d'origine humaine	30
2.4.2.3	Menaces liées à la chaîne d'approvisionnement	31
2.4.2.4	Menaces ciblées	32
2.4.2.5	Motivations financières	33
2.4.2.6	Services de renseignements étrangers	33
2.4.2.7	Menaces liées aux fournisseurs et aux partenaires	33
2.4.2.8	Menaces liées à la cybersécurité	34
2.5	INCIDENTS DE SECURITE DANS LES ICS	34
2.5.1	STUXNET	35
2.5.2	PANNE DE COURANT EN UKRAINE	38
2.6	VULNERABILITES COURANTES DES ICS	41
2.6.1	VULNERABILITES LIEES A L'ELEMENT HUMAIN	41
2.6.2	VULNERABILITES DU MATERIEL	42
2.6.3	VULNERABILITES DES LOGICIELS	42
2.6.4	VULNERABILITES DU RESEAU	43
2.6.5	VULNERABILITES DES PROTOCOLES DE COMMUNICATION	43
2.6.6	VULNERABILITES LIEES A L'ADMINISTRATION ET A LA GESTION	44
2.6.7	VULNERABILITES LIEES A L'AUTHENTIFICATION ET AUX	

AUTORISATIONS	44
2.6.8 VULNERABILITES LIEES A L'ABSENCE DE SURVEILLANCE ET DE JOURNALISATION	45

3 TESTS D'INTRUSION DANS LES SYSTEMES INDUSTRIELS **47**

3.1 TEST D'INTRUSION DANS LES ENVIRONNEMENTS ICS/SCADA	47
3.1.1 AVANTAGES DES TESTS D'INTRUSION ICS	48
3.1.2 DEFIS DES TESTS D'INTRUSION ICS	49
3.1.3 TYPES DE TESTS D'INTRUSION DANS L'ENVIRONNEMENT ICS	50
3.1.3.1 Boîte noire (Black-Box)	50
3.1.3.2 Boîte blanche (White-Box)	50
3.1.3.3 Boîte grise (Gray-Box)	51
3.1.4 METHODES DE TEST D'INTRUSION DANS L'ENVIRONNEMENT ICS	52
3.1.4.1 Test d'intrusion externe	52
3.1.4.2 Test d'intrusion interne	52
3.1.5 DEROULEMENT D'UN TEST D'INTRUSION	53
3.1.5.1 Phase de préparation et planification	53
3.1.5.2 Phase de collecte de renseignements (reconnaissance)	53
3.1.5.3 Phase de cartographie des vulnérabilités	54
3.1.5.4 Phase d'exploitation des vulnérabilités	54
3.1.5.5 Phase de rapport	54
3.1.6 OUTILS UTILISES POUR LES TESTS D'INTRUSION	55
3.1.6.1 Systèmes d'exploitation	55
3.1.6.2 Outils de reconnaissance	56
3.1.6.3 Outils de threat modeling	57
3.1.6.4 Outils d'analyse des vulnérabilités	58
3.1.6.5 Outils d'exploitation	59
3.1.6.6 Outils de post-exploitation	60
3.1.7 SCENARIOS DE PENETRATION EXTERNE ET TESTS D'INTRUSION DANS ICS	61
3.1.7.1 Reconnaissance	61
3.1.7.2 Phishing et ingénierie sociale	62
3.1.7.3 Analyse des vulnérabilités	62

3.1.7.4	Exploitation des vulnérabilités	63
3.1.7.5	Établissement de la persistance	63
3.1.7.6	Mouvement latéral et élévation des privilèges	64
3.1.7.7	Atteinte des objectifs	64

4 ATTAQUES VISANT LES SYSTEMES INDUSTRIELS

65

4.1	ATTAQUES TRADITIONNELLES	66
4.1.1	ATTAQUES EXPLOITANT LE FACTEUR HUMAIN "INGENIERIE SOCIALE"	66
4.1.2	L'HOMME DU MILIEU UTILISANT L'EMPOISONNEMENT DU PROTOCOLE ARP	68
4.1.3	EMPOISONNEMENT DU SERVICE DE NOM DE DOMAINE DNS	69
4.1.4	ATTAQUE SPOOFING DE NTP	70
4.2	ATTAQUES PHYSIQUES	71
4.3	CYBERATTAQUES SUR LES LOGICIELS	72
4.3.1	CONCEPTION ET MISE EN ŒUVRE DU CODE SOURCE	72
4.3.2	DEBORDEMENT DE MEMOIRE TAMPON	74
4.3.3	INJECTION SQL	75
4.4	ATTAQUE EXPLOITANT UNE FAILLE ZERO-DAY	76
4.5	ATTAQUES SPECIFIQUES AUX PROTOCOLES	76
4.6	ATTAQUES MODBUS SERIAL	77
4.6.1	ATTAQUES UNIQUEMENT SUR MODBUS TCP	78
4.6.2	ATTAQUES SUR MODBUS SERIAL ET TCP	79
4.6.3	ATTAQUES SUR DNP3	83

5 SECURISATION DES SYSTEMES INDUSTRIELS

91

5.1	PRINCIPES DE LA DEFENSE EN PROFONDEUR	91
5.1.1	ORGANISATION ET ASPECTS HUMAINS	93
5.1.2	SECURITE PHYSIQUE	94
5.1.3	DEFENSE DU PERIMETRE	95
5.1.4	DEFENSE DU RESEAU	97
5.1.5	DEFENSE DES ORDINATEURS ET DISPOSITIFS	97
5.1.6	DEFENSE DES APPLICATIONS	98
5.1.7	DEFENSE DES DONNEES OU DU PROCESSUS PHYSIQUE	98

5.2	METHODES ET OUTILS POUR SECURISER LES ICS	98
5.2.1	IDENTIFICATION DES ACTIFS	99
5.2.2	SECURITE ARCHITECTURALE	101
5.2.2.1	Architecture sécurisée	101
5.2.2.2	Partitionnement en zones	102
5.2.3	PARE-FEU	103
5.2.4	DIODE DE DONNEES	105
5.2.5	SYSTEME DE DETECTION D'INTRUSION	105
5.2.6	GESTION DES CORRECTIFS ET DES VULNERABILITES	109
5.2.7	SURVEILLANCE DE LA SECURITE ET LA REPONSE AUX INCIDENTS	110
5.2.8	ÉVALUATIONS DE SECURITE DES FOURNISSEURS	110
5.2.9	FORMATION ET SENSIBILISATION DES EMPLOYES	111
 <u>CONCLUSION</u>		 <u>113</u>
 <u>REFERENCES</u>		 <u>115</u>

1 Généralité sur les systèmes ISC/SCADA

Ce chapitre vise à présenter les aspects généraux des ICS (Industrial Control System), en mettant l'accent sur les définitions clés, l'architecture des ICS, l'évolution des systèmes Supervisory Control and Data Acquisition (SCADA), les composants et le fonctionnement d'un système SCADA, ainsi que les protocoles couramment utilisés dans un environnement ICS.

1.1 Définitions

Dans cette section, nous présentons les définitions des termes : IT (Information Technology), OT (Operational Technology), ICS, SCADA, DCS (Distributed Control Systems) et SIS (Safety Instrumented System).

1.1.1 IT

Information Technology (IT) également connues sous le nom Technologie de l'Information englobe l'ensemble des ressources, des pratiques et des systèmes utilisés pour gérer, traiter, stocker, transmettre et sécuriser l'information au sein d'une organisation. Il s'agit d'un domaine qui se concentre sur l'exploitation des technologies, des infrastructures et des logiciels pour soutenir les opérations et les processus métier d'une entreprise.

L'IT est responsable de la gestion des systèmes d'information d'entreprise qui automatisent les processus opérationnels, tels que la gestion des ressources humaines, la comptabilité, la gestion des stocks, le marketing, la gestion des ventes et bien d'autres. Ces systèmes permettent de collecter, organiser, analyser et interpréter les données, offrant ainsi des informations précieuses pour la prise de décisions éclairées.

1.1.2 OT

Operational Technology (OT) également connues sous le nom Technologie Opérationnelle fait référence à l'ensemble des technologies, des systèmes et des processus utilisés pour gérer, contrôler et superviser les opérations physiques dans un environnement industriel. Contrairement à l'IT qui se concentre sur la gestion des informations et des processus de l'entreprise, l'OT est spécifiquement axé sur les systèmes qui ont un impact direct sur l'environnement physique et le fonctionnement des outils de production.

1.1.3 ICS

Les systèmes de contrôle industriel, ou Industrial Control Systems (ICS), sont l'une des principales catégories de l'OT. Un ICS est un ensemble de composants matériels, logiciels et de communication utilisé pour superviser, contrôler et réguler les opérations dans des environnements industriels. Les ICS sont conçus pour automatiser les processus physiques, surveiller les variables opérationnelles et prendre des décisions en temps réel pour assurer un fonctionnement efficace et sûr des installations industrielles. Ils regroupent différents sous-ensembles tels que le SCADA, le DCS et le SIS (figure 1.1), qui fournissent des fonctionnalités spécifiques en matière de surveillance, de contrôle distribué et de sécurité des processus industriels.

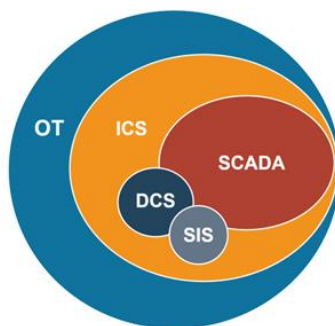


Figure 1.1 – OT/ICS

Les ICS intègrent des capteurs, des dispositifs de surveillance, des unités de commande, des actionneurs et des réseaux de communication pour collecter des données en temps réel, effectuer des analyses, prendre des décisions et contrôler les équipements industriels. Ils permettent aux opérateurs de surveiller les processus, de réguler les paramètres opérationnels, d'optimiser les performances, de détecter les anomalies et de garantir la sécurité des installations industrielles.

Les ICS sont utilisés dans une variété d'industries telles que l'énergie, la production manufacturière, l'automatisation des bâtiments, les infrastructures critiques, les services publics, les raffineries, les usines chimiques, le traitement des eaux et bien d'autres (Stouffer, Falco, Scarfone, Abrams, & Hahn, 2011).

1.1.4 SCADA

Le SCADA (Supervisory Control and Data Acquisition) est un système de contrôle utilisé pour superviser, contrôler et acquérir des données à partir de processus industriels distribués sur de vastes zones géographiques. Il se compose de plusieurs composants, tels que des capteurs, des dispositifs de surveillance, des unités de commande, des interfaces utilisateur et un logiciel de supervision (Kruz, 2015). Les fonctionnalités clés du SCADA incluent la collecte de données en temps réel, la surveillance des processus, l'acquisition de données, le contrôle à distance, l'analyse des données et la génération de rapports. Les systèmes SCADA sont couramment utilisés dans des industries telles que l'énergie, les systèmes de gestion de l'eau, l'industrie pétrolière et gazière, pour permettre une gestion centralisée et une surveillance à distance des processus industriels. Ils sont conçus pour être évolutifs, flexibles et capables de s'interconnecter avec d'autres systèmes.

1.1.5 DCS

Le DCS (Distributed Control Systems) est un système de contrôle distribué utilisé pour réguler et contrôler les processus industriels à l'échelle locale, généralement dans une usine ou une installation spécifique. Contrairement aux systèmes SCADA, qui sont souvent utilisés pour surveiller de vastes zones géographiques, les systèmes DCS sont spécifiquement conçus pour des opérations de contrôle et de régulation locales. Ils se composent généralement de plusieurs unités de commande distribuées (DCU : Distributed Control Unit) interconnectées pour contrôler et surveiller les équipements et les processus dans différentes parties de l'installation. Les fonctionnalités clés des systèmes DCS comprennent le contrôle en temps réel des processus, la gestion des alarmes, la gestion des données, l'optimisation des performances et la sécurité des processus. Les systèmes DCS sont couramment utilisés dans des industries telles que la production chimique, les raffineries, l'industrie manufacturière, où un contrôle précis et localisé des processus est essentiel (TIB, 2004).

1.1.6 SIS

Le SIS (Safety Instrumented System) est un composant clé des ICS qui vise à assurer la sécurité des processus industriels en détectant les conditions dangereuses et en prenant des mesures de sécurité appropriées. Il utilise des capteurs de sécurité, des logiques de sécurité programmables et des actionneurs pour surveiller en temps réel les paramètres des processus et réagir aux situations dangereuses (Instrumentation, 2023).

Le rôle principal du SIS est de prévenir les accidents industriels graves en réduisant les risques pour les travailleurs, les installations et l'environnement. En détectant les conditions dangereuses, il déclenche