

Analyse de sécurité relative à la gestion des patches
des systèmes d'exploitation en industrie
pharmaceutique

Bob MULUMBA TUBADI



UNIVERSITÉ DU
LUXEMBOURG

Faculté des Sciences, de la Technologie et de la Communication (FSTC)

Master en Management de la Sécurité des Systèmes d'Information

Année académique 2017-2018 - Promotion 8

**Analyse de sécurité relative à la gestion des
patches des systèmes d'exploitation en
industrie pharmaceutique**

Bob MULUMBA TUBADI

*Responsable
académique*

Nicolas MAYER, PhD
Senior R&T Associate
Luxembourg Institute of Science and Technology

Responsable local

Cecile MIGNON
Senior Manager
GlaxoSmithKline Vaccines

Bob MULUMBA TUBADI

Analyse de sécurité relative à la gestion des patches des systèmes d'exploitation en industrie pharmaceutique

Master en Management de la Sécurité des Systèmes d'Information

Responsable académique : Nicolas MAYER, PhD

Responsable local : Cecile MIGNON

Université du Luxembourg

Faculté des Sciences, de la Technologie et de la Communication (FSTC)

2, avenue de l'Université

L-4365 Esch-sur-Alzette

Résumé

Nous vivons dans un monde où les systèmes de contrôle et de fabrication industrielle modernes sont de plus en plus complexes, numériques et connectés.

Dans le passé, ces technologies ont été isolées d'autres réseaux, les opérateurs d'aujourd'hui exigent généralement que les données soient transférées entre les réseaux industriels et externes.

Tout logiciel, utilisé à cette fin, est sujet à des vulnérabilités techniques. Une fois découverte et partagée publiquement. Ces vulnérabilités peuvent être exploités rapidement par les cybercriminels et exposent les entreprises à des risques.

Les pirates informatiques peuvent tirer parti des vulnérabilités connues dans les systèmes d'exploitation et les applications tierces, si elles ne sont pas correctement mises à jour et perturber les systèmes de contrôle en temps réel et les infrastructures dépendantes.

Ce mémoire décrit les différents types de systèmes d'information et de contrôle industriels dans le secteur pharmaceutique. Il propose une stratégie de mise en place, selon un comparatif des méthodes existants, et outils dans la gestion des correctifs de sécurité au niveau des systèmes d'exploitation jointe à une analyse de risque.

L'ensemble dans le but de maîtriser au mieux la sécurité dans les systèmes de type opérationnels critiques.

Mots clés : Sécurité, Patching, Systèmes d'exploitation, Systèmes industriels, Sociétés pharmaceutiques, Méthodologies de gestion de risques, Technologie de l'information (IT), Technologie opérationnelle (OT)

Abstract

We live in a world where modern control systems are increasingly complex, digital and connected.

In the past, these technologies have been isolated from other networks, today's operators generally require that data be transferred between industrial and external networks.

Any software, in use for that purpose, is prone to technical vulnerabilities. Once discovered and shared publicly.

These pitfalls can rapidly be exploited by cybercriminals and exposes organisations to risk that hackers can take advantage of known vulnerabilities in operating systems and third-party applications, if they are not properly patched or updated and disrupt real-time control systems and dependent infrastructures.

This master thesis describes the different types of information and industrial control systems in the pharmaceutical sector. It proposes a strategy using a comparison to implement methods and tools on the management of operating systems security patches as well as a related risk analysis.

All in order to provide better security on a critical industrial system perspective.

Keywords : Security, Patching, Industrial operating systems, Pharmaceutical companies, Risk management frameworks, Information technology (IT), Operational technology (OT)

Déclaration d'honnêteté

Je déclare et confirme avoir réalisé ce mémoire sans l'aide illicite d'autrui et en me conformant aux règles d'honnêteté intellectuelle.

Esch-sur-Alzette, 1^{er} mai 2018

Bob MULUMBA TUBADI

Remerciements

Mes remerciements s'adressent à ma famille pour la patience et l'appui pendant ces années d'études. Leur soutien a été indéfectible tout au long de ce long processus d'apprentissage aussi bien au niveau des cours que lors de l'écriture de ce mémoire.

Je désire remercier mon responsable académique (Nicolas MAYER, PhD) pour la rigueur scientifique, les judicieux conseils, son expérience dans le domaine de la sécurité et sa patience qui m'ont stimulé lors de la réalisation de ce travail.

Je remercie mon responsable local (Cecile MIGNON, Senior Manager) pour le soutien moral adressé et pour m'avoir permis de mettre en pratique les aspects liés à ce cursus dans le cadre de mon travail quotidien.

Enfin, un grand merci à toutes les personnes (Professeurs, collègues et amis) qui m'ont supporté, dans tous les sens du terme, pendant ce programme d'étude.

À vous tous, MERCI.

Table des matières

1	Introduction	1
1.1	Présentation	2
1.2	Contexte	4
1.3	Motivation et problématique	6
1.4	Objectifs et organisation du mémoire	7
2	Cadre théorique	9
2.1	Le contexte industriel pharmaceutique et les systèmes d'information industriels	10
2.1.1	Types de départements (R&D et GIO)	11
2.1.2	Architecture et terminologie	13
2.1.3	Utilisation	16
2.1.4	Cycle de vie	17
2.1.5	Limites	17
2.2	Les logiciels industriels	19
2.2.1	Types de systèmes d'exploitation	19
2.2.2	Types de logiciels (COTS vs non-COTS)	20
2.3	Les vulnérabilités	21
2.3.1	Vulnérabilités Zero-Day	22
2.3.2	Autres vulnérabilités	22
2.4	Le patching	24
2.4.1	Types de patches	24
2.4.2	Sources des patches	25
2.4.3	Indexes d'exploitabilité	26
2.5	La gestion des changements	27
2.6	Conclusion	28
3	Etat de l'art et analyse	31
3.1	Différences entre IT vs OT	31
3.2	Comparaison des méthodologies au niveau des patches	32
3.2.1	ANSI/ISA-TR62443-2-3-2015	33
3.2.2	NERC-CIP-007 Systems Security Management	35
3.2.3	NIST Special Publication 800-40 Version 2.0	37
3.2.4	ISO27001-2013	39

3.3	Analyse des échecs du patching en générale	41
3.4	Gestion des patches au niveau des systèmes d'exploitation	42
3.5	Approche méthodologie des risques : ISO27005 ou IEC 62443 3-2 . .	44
3.5.1	Gestion des risques	45
3.5.2	Scénarios de risques	47
3.5.3	Traitement des risques	49
3.5.4	Les responsabilités (Matrice RACI)	51
3.6	Conclusion	53
4	Mise en pratique en contexte local	55
4.1	Contexte détaillé	55
4.1.1	Méthodologie à appliquer	56
4.2	Stratégie de gestion des patches en environnement opérationnel . . .	58
4.3	Gestion des risques	59
4.3.1	Impact et mesure de probabilité	62
4.3.2	Évaluation des risques	64
4.3.3	Identification des actifs	66
4.3.4	Identification des expositions des risques	68
4.3.5	Menaces spécifiques	70
4.3.6	Vulnérabilités	73
4.3.7	Risques/Menaces	75
4.3.8	Estimation des risques par actif	77
4.3.9	Traitement du risques et liste des contrôles	79
4.4	Plan d'implémentation	81
4.5	Conclusion	84
5	Conclusion	85
5.1	Améliorations futures	85
6	Glossaire	87
	Bibliographie	89

Table des figures

1.1	Vulnérabilités déclarées depuis 2010 - (Source : ICS-CERT)	2
1.2	Ransomwares en 2017 - Source : NTT	3
1.3	Société GlaxoSmithKline - (Source : GSK)	4
1.4	3 secteurs d'activités de GlaxoSmithKline - (Source : GSK)	5
2.1	Régulateurs et standards GxP - (Source : GSK)	11
2.2	Cycle de vie R&D et GIO - (Source : Sanofi)	12
2.3	Structure des installations dans l'OT - (Source : ISA)	14
2.4	Modèle logique hiérarchique de PERA : IT vs OT - (Source : ISA)	14
2.5	Computer System vs Computerized System - (Source : GSK)	16
2.6	Système et validation des équipements - (Source : Sanofi)	16
2.7	Relations Utilisateur vs Matériel vs Logiciel	19
2.8	Computer System vs Computerized System - (Source : GSK)	21
2.9	Computer System vs Computerized System - (Source : GSK)	21

Introduction

Les systèmes d'information et de contrôle industriel pharmaceutiques sont composés de nombreux équipements pour accomplir des tâches primordiales lors de la recherche, du développement ou de la fabrication des médicaments ou vaccins. Le fonctionnement de ces composants repose sur un grand nombre de logiciels qui proviennent de multiples producteurs et répondent à différentes fonctions de réception et de transmission d'information à la criticité bien distincte.

La bonne activité de ces systèmes repose en partie sur la sécurité de chacun des éléments logiciels et dont les différents niveaux de complexité doivent être pris en compte. La gestion des correctifs de sécurité ou "patch management" est une composante essentielle dans la maîtrise du niveau de sécurité d'un système d'information aussi bien classique qu'industriel. En effet, des nombreuses attaques sont réalisées à partir des vulnérabilités connues pour lesquelles il existe des méthodologies d'exploitation accessible à tous mais aussi plus généralement des outils d'exploitation qui en automatisent les attaques.

La plupart de ces failles sont corrigées par des correctifs de sécurité ou "patches". De ce fait, et en exemple, quand un avis de sécurité vient d'un éditeur, et présente une vulnérabilité dans une application tierce. La vulnérabilité liée peut permettre l'exécution d'un code, souvent malicieux et destructeur. Sachant qu'il existe un certain nombre d'applications ou modules dans les différents logiciels de test d'intrusion et qui permettent l'exploitation automatique de toute nouvelle menace.

Un patch correctif de vulnérabilité peut-être publié. Cependant, tous les systèmes ne sont pas systématiquement corrigés dès l'apparition des correctifs, pour des raisons d'accord technologique, de régression fonctionnelle ou juste liées à une absence de politique de gestion des correctifs minutieuse.

Les systèmes d'exploitation sont la base maîtresse de tout système informatique car ils permettent et dirigent l'utilisation des ressources de tout système informatisé par des logiciels applicatifs et permettent le bon fonctionnement des activités du corps de métier. Il est nécessaire de comprendre et avoir une approche orientée vers la gestion des risques qui peuvent survenir pour ces composantes.

1.1 Présentation

Aujourd'hui, la plupart des incidents de sécurité sont causés par des failles dans les logiciels, aussi appelées vulnérabilités. Il est estimé qu'il y a jusqu'à 20 défauts par millier de lignes de code [May12] [McC08].

Les statistiques des différents "Computer Security Incident Response Team" (CIRST) dont celui dédié aux systèmes industriels, l'ICS-CERT révèlent que le nombre de vulnérabilités signalées a considérablement augmenté au fil des années, passant de 37 en 2010 à 2317 en 2016.[ICS16]

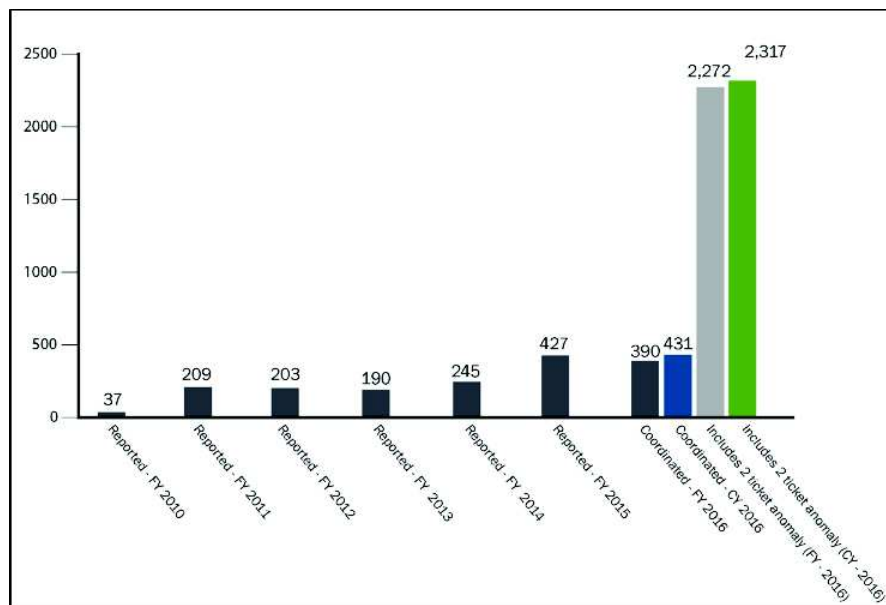


Fig. 1.1: Vulnérabilités déclarées depuis 2010 - (Source : ICS-CERT)

La solution ultime aux vulnérabilités logicielles est l'application de correctifs ou "patches". Tous les éditeurs de logiciels publient généralement des correctifs pour corriger les vulnérabilités de leurs produits. Ces patches, s'ils sont appliqués correctement, suppriment les vulnérabilités des systèmes. Cependant, de nombreux systèmes sont laissés sans surveillance pendant des mois, voire des années.

Selon le dernier rapport de NTT, environ 95 des atteintes à la sécurité pourraient être évitées en maintenant les systèmes à jour avec les correctifs appropriés. Les ransomwares "Locky", "WannaCry", "Petya" ou de souche commune, qui ont créé une crise sans précédente sur Internet et ont provoqué des pannes de réseau dans le monde entier, affectant les plus grosses compagnies, allant des compagnies aériennes au plus basique des guichets automatiques.

Pourtant Microsoft avait publié le correctif fixant la vulnérabilité que "WannaCry" exploite six mois avant l'incident. De même, pour "Locky" et "Petya" qui ont aussi fait des ravages dans les entreprises qui n'étaient pas à jour avec leurs correctifs logiciels.[NTT18]

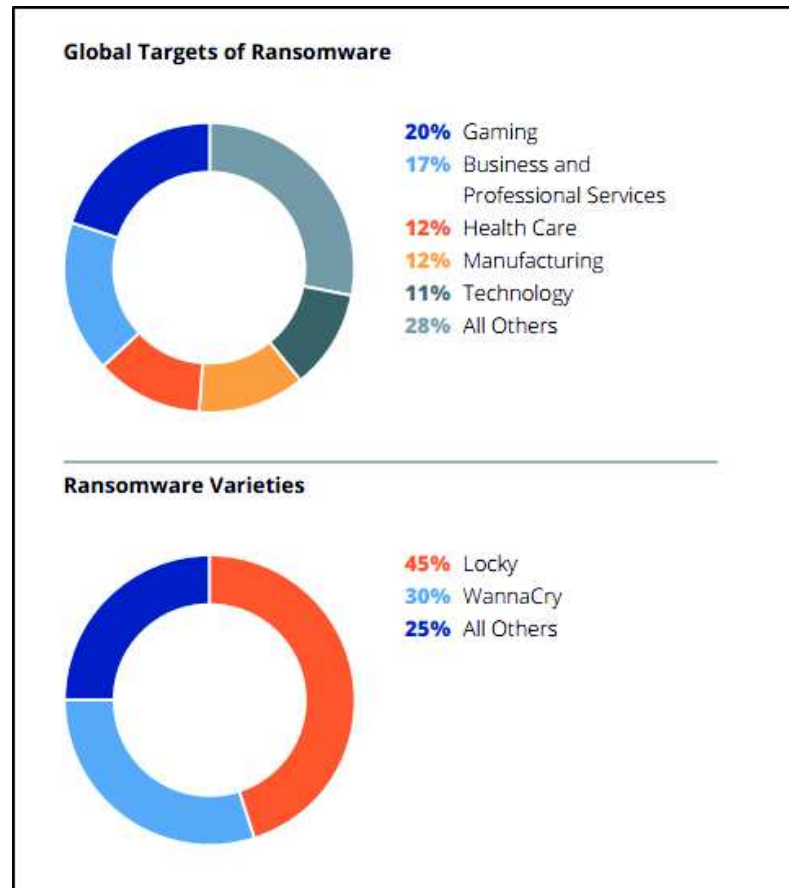


Fig. 1.2: Ransomwares en 2017 - Source : NTT

Ces attaques étaient relativement peu courantes avant 2017, mais ont explosé depuis et cela notamment à cause d'un manque de patching et de la gestion de risque qui s'en accommode.

Le nombre de vulnérabilités zero-day continue à fluctuer, tout comme les attaques Web utilisant des vulnérabilités connues et cela restent un problème. Les systèmes d'information industriels, ainsi que les systèmes d'exploitation mobiles et non-Windows, et plus récemment l'Internet des objets (IoT) ne cessent d'augmenter la surface d'attaque et ne doivent plus être ignorés.

1.2 Contexte

GlaxoSmithKline (GSK) est une firme britannique et un des acteurs majeurs de l'industrie pharmaceutique, avec des médicaments innovants et des vaccins dans de nombreux domaines thérapeutiques.[Gla18]

Le laboratoire occupe également une place prépondérante en dermatologie, en hygiène bucco-dentaire et en automédication. Aujourd'hui, GSK représente près de 100 000 collaborateurs travaillant dans plus de 100 pays, plus de 100 médicaments de prescription et de vaccins vendus dans 190 pays.

GSK à travers le monde aujourd'hui

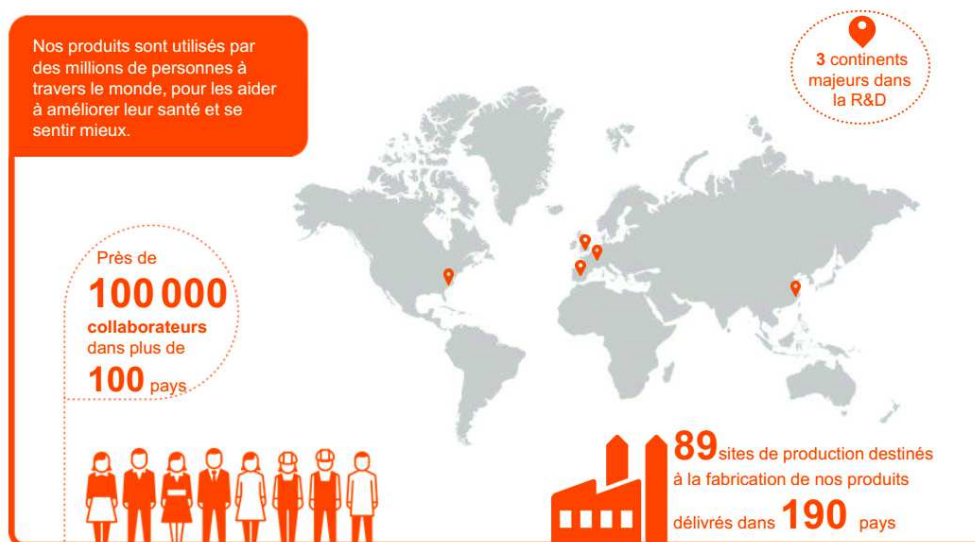


Fig. 1.3: Société GlaxoSmithKline - (Source : GSK)

Les infrastructures de production de GSK sont considérés comme des CI (Critical Infrastructure) de par le monde et utilise les systèmes d'information classique pour l'aspect commercial mais aussi les systèmes d'information industriels pour la R&D et le processus de fabrication des divers produits.[Arc16]

La firme recherche et développe une large gamme de produits innovants dans trois principaux domaines :

- Les produits Santé Grand Public - Consumer Healthcare
- Les vaccins - Vaccines
- Les produits pharmaceutiques - Pharmaceuticals

L'activité principale développe et commercialise une gamme de produits de soins de "**Consumer Healthcare**" basée sur l'innovation scientifique.

"**Vaccines**" L'activité au niveau des vaccins est l'une des plus importante dans le monde. En 2014, plus de 800 millions de doses ont été distribué dans 170 pays, dont plus de 80% ont été fournis aux pays en voie de développement.

"**Pharmaceuticals**" L'activité pharmaceutiques développe et propose des médicaments pour traiter un grand nombre de pathologies aiguës et chroniques



Fig. 1.4: 3 secteurs d'activités de GlaxoSmithKline - (Source : GSK)

1.3 Motivation et problématique

Le projet professionnel se base sur des questions de sécurisation des actifs d'une société pharmaceutique. En particulier, la gestion des patches des systèmes d'exploitation dans un environnement informatisé industriel, sujet à une validation et à des processus de contrôles régulés.

Un des points, sur lequel nous nous attardons dans ce mémoire reste que peu importe la criticité des infrastructures dans laquelle nous résidons et le secteur (aussi bien pharmaceutique, énergétique, électricité). N'importe quel système de production ou de R&D utilise de nos jours les ICS (Industrial Control System) ou OT (Operational Technology) selon l'appellation plus généraliste.

Au cours de la dernière décennie, les différentes technologies liées aux ICS ou à l'OT en général, ont subi une transformation. Ces infrastructures sont passées des systèmes isolés et exclusifs vers des architectures ouvertes et des standards technologiques fortement interconnectées avec d'autres réseaux d'entreprise et l'Internet. Une des conséquences de cette transformation est la vulnérabilité accrue aux attaques extérieures. Une façon d'améliorer la sécurité de ces systèmes est l'application de correctifs de sécurité au niveau logiciel (patches).

Deux des principaux problèmes importants avec les patches de sécurité, en ce moment sont le taux d'échecs des patches et le manque de correctifs pour les sous-systèmes des ICS. En gardant à l'esprit que l'application des patches correctifs a toujours été un problème pour les entreprises. Bien que celles-ci connaissent l'avantage évident de la correction rapide, elles peuvent hésiter à déployer des mises à jour susceptibles d'entraver les opérations ou d'affecter les systèmes critiques.

L'application de correctifs peut représenter un véritable fardeau si aucune procédure n'est mise en place et que de nombreuses entreprises ne peuvent pas se permettre le temps d'arrêt, de sorte qu'elles acceptent simplement les risques. En plus de cela, il y a un certain nombre d'autres raisons qui peuvent retarder le patching ; les ressources pourraient être limitées, les systèmes existants pourraient être négligés pendant la correction, ou pire, certains systèmes sont tellement obsolètes qu'ils ne peuvent pas être corrigés.

Nous analysons les risques à l'aide des comparatifs de méthodes et la question pourquoi une mauvaise gestion des patches peut amener à des cas de corruption qui peuvent bloquer des processus et avoir des conséquences désastreuses ? Le sujet est vaste et pour cause, nous ne nous attarderons que sur la partie des systèmes d'exploitation.

1.4 Objectifs et organisation du mémoire

Ce mémoire est constitué de 3 parties :

1. Le cadre théorique, qui constitue les aspects de recherches académiques et littéraires et différentes analyses.
2. Le cadre pratique, qui mène à la mise en pratique de l'analyse et des résultats de la partie académique dans un contexte local industriel bien déterminé.
3. La conclusion générale

La **première partie** dresse un point de situation bibliographique exhaustif sur les pratiques dans le monde industriel afin de tenter de déterminer les grands principes de la gestion des correctifs.

Dans un premier temps, nous catégorisons les différents niveaux de composantes dans les systèmes industriels pharmaceutiques, dont les fonctions associés et les aspect logiciels. Nous dressons ensuite un ensemble des différences qui existent entre les systèmes d'information classiques et opérationnels.

Nous faisons une comparaison méthodologiques, qui ne se limite qu'aux correctifs de sécurité. Il s'agit ici de parcourir les méthodes les plus couramment utilisées afin de proposer une analyse qui s'alignent avec une approche de gestion des risques concernant la gestion des correctifs des systèmes d'exploitation dans un environnement industriel multi-vendeurs.

Nous clôturons par une conclusion présentant notre propre réflexion et choix pour la mise en contexte. Ces aspects sont traités dans les chapitres 2 et 3.

La **deuxième partie**, que constitue le chapitre 4, nous appliquons les recherches dans un contexte local industriel similaire à la société GSK et en particulier pour les corps des métiers "R&D" et "Opérations industrielles".

La **troisième partie**, qui équivaut au chapitre 5, nous évoquerons en plus des améliorations possibles au niveau du sujet des patches et des systèmes d'exploitation. L'apport global de ces études et l'écriture de ce mémoire.

Cadre théorique

Dans cette partie, nous allons revoir les aspects littéraires qui vont nous aider à mettre en pratique la suite du mémoire

2.1 Le contexte industriel pharmaceutique et les systèmes d'information industriels

Il est important de comprendre certaines terminologies spécifiques au monde industriel. Le but n'est pas de tout définir de manière exhaustive mais bien d'aider à la compréhension finale du sujet.

La plupart des gens connaissent le terme technologie de l'information (IT). Car beaucoup de ces personnes travaillent généralement de ce côté en entreprise. Il existe bien quelques définitions de ce terme. Mais la définition que donne Gartner semble la mieux correspondre à notre cas.[Gar18]

Selon Gartner, une définition de l'IT serait :

*"**Information Technology** is the common term for the entire spectrum of technologies for information processing, including software, hardware, communications technologies and related services. In general, IT does not include embedded technologies that do not generate data for enterprise use."*

Cette dernière partie est à souligner parce qu'elle joue un rôle important dans le reste de cette partie du mémoire. L'IT n'inclut donc pas toute partie de l'industrie et ce même Gartner nous définit cette autre partie comme étant aussi l'OT :

*"**Operational Technology** is hardware and software that detects or causes a change through the direct monitoring and/or control of physical devices, processes and events in the enterprise."*

Le monde pharmaceutique est composé de ces deux mondes. qui en plus d'avoir des fondements différents forme une entité qui doit suivre des exigences et des standards de qualités pour être certain que les produits délivrés sont sains et efficaces.

Les entreprises dans le milieu pharmaceutique ont régulièrement des inspections et des audits pour démontrer leur conformité au niveau des lois. Ne pas se conformer à ces demandes peuvent entraîner des fortes amendes, une attente dans la production de la marchandise, des injonctions criminelles ou autres pénalités civiles.[FA17]

En d'autres termes rien ne peut être laissé en marge dans les contrôles aussi bien des personnes que des équipements.

La figure 2.1 montre les régulateurs reconnus et quelques exigences de standardisation à suivre.





	USA	<ul style="list-style-type: none"> FDA 21 CFR Part 11 – Electronic Records and Electronic Signature
	EUROPE	<ul style="list-style-type: none"> Eudralex Volume 4 - Annex 11 "Computerized Systems" Eudralex Volume 4 - Annex 15 "Qualification and Validation"
	UK	<ul style="list-style-type: none"> MHRA Data Integrity Guidance
	International Guidance	<ul style="list-style-type: none"> PICS Guidance – PI 011-3 - Good Practices for Computerised Systems in Regulated "GxP" Environments
	International Guidance	<ul style="list-style-type: none"> GAMP 5 – A Risk-Based Approach to Compliant GxP Computerized Systems
	International Guidance	<ul style="list-style-type: none"> ICH E6 - Good Clinical Practice ICH Q7 - Good Manufacturing Guide for Active Pharmaceutical Ingredients ICH Q8 - Pharmaceutical Development

Fig. 2.1: Régulateurs et standards GxP - (Source : GSK)

Le plus connu des standard pour s'assurer de la qualité au niveau pharmaceutique est le "Good x Pratiques" (GxP). Le "x" est une variable que l'on peut remplacer avec un des termes suivants, et qui représente une étape dans le développement, la production et la distribution des produits :

- Good Laboratory Practices (GLP)
- Good Manufacturing Practices (GMP)
- Good Clinical Practices (GCP)
- Good Distribution Practices (GDP)
- etc.

2.1.1 Types de départements (R&D et GIO)

Il existe 2 grands départements au niveau de l'OT, la **Recherche et Développement - (R&D)** et les **Opérations Industrielles - GIO** [San14]

Ces deux départements permettent de mettre en place le cycle de développement d'un produit pharmaceutique. Cela engage la fabrication biologique et biochimique (mise en culture des germes, récoltes, purification, assemblage...) pour la R&D.

Et la partie purement opérationnelle, la fabrication pharmaceutique en complément, à savoir les formulation et répartitions, la lyophilisation, le conditionnement et la libération des lots ainsi que la distribution finale après les contrôles des autorités de santé.

L'ensemble toujours en mettant en place des contrôles de qualité et d'assurance.

Par exemple pour un vaccin, la mise en place peut aller jusqu'à 14 ans en moyenne et à terme, tous les systèmes doivent être conservés tant que le produit est d'actualité).

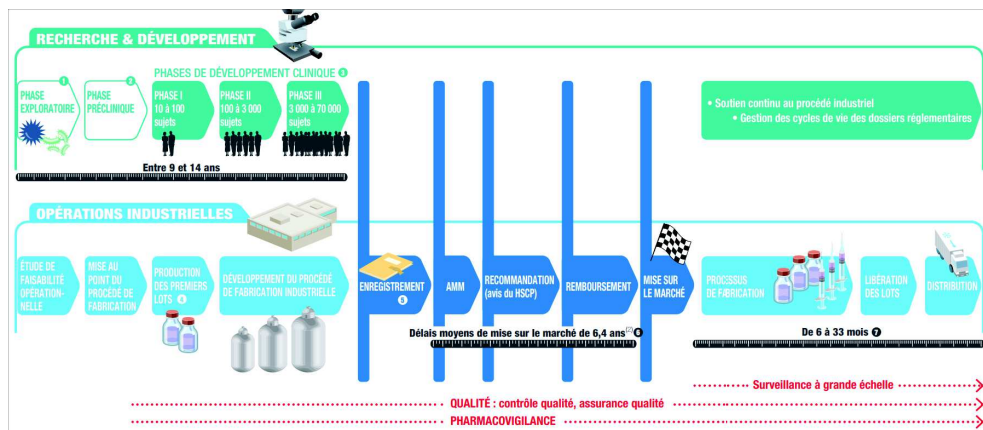


Fig. 2.2: Cycle de vie R&D et GIO - (Source : Sanofi)

Comme on peut le voir dans la figure 2.2, les rôles sont attribués de la sorte :

1. Recherche et Développement

- Phases exploratoire ou fabrication biologique et biochimique (2-4 ans)
- Phases pré-clinique ou évaluation sur les animaux et sélection du plus adéquat (1-2 ans)
- Phase de développement clinique ou évaluation sur l'être humain (6-8 ans)
- Soutien dans les procédés industriels (toute la durée de vie)
- Gestion des dossiers réglementaires jusqu'au retrait du produit (toute la durée de vie)

2. Opérations Industrielles

- Etude de faisabilité opérationnelle ou fabrication pharmaceutique
- Mise au point des procédés de fabrication
- Production des lots d'essais
- Développement des procédés entières de fabrication industrielle
- Processus automatisés de fabrication
- Distribution d'ensemble du produit
- Soutien dans les procédés de recherche et développement (toute la durée de vie)
- Gestion des dossiers réglementaires jusqu'au retrait du produit (toute la durée de vie)

2.1.2 Architecture et terminologie

Selon Reix et cie[Rei+16], un système d'information aussi bien industriel que classique a pour objectif de restituer aux différents membres de l'entreprise les informations sous une forme directement utilisable afin de faciliter la prise de décision. Le tout en remplissant ces 4 tâches spécifiques :

1. La collecte :
L'origine de l'information peut être interne (comptes, stocks,...) ou externe (information sur le concurrent, disposition nouvelle d'ordre fiscale ou sociale).
2. Le stockage :
Une fois l'information recueillie il faut la conserver, et pour cela tenir compte de 2 facteurs :
 - L'information doit pouvoir être disponible, organisées et accessibles.
 - L'information doit être pérenne, elle doit pouvoir être conservée dans le temps, d'où le choix du support (papier ou numérique) et de son mode de conservation.
3. Le traitement :
La phase de traitement va commencer avec le choix du support utilisé puisqu'il va falloir trouver une construction formalisée pour traiter l'information.- Soit la centralisation (réalisée à un seul endroit donc un seul niveau dans l'entreprise).
 - Soit la décentralisation.
 - Soit la distribution.
4. La diffusion :
Elle doit répondre à 4 critères :
 - Quelle est son origine et sa destination ?
 - Quelle est sa forme ? (orale, écrite,...)
 - Dans quel délai l'information devra-t-elle parvenir à son destinataire ?
 - La diffusion sera-t-elle large ou restreinte ?

Les systèmes qui résident au niveau de l'OT sont communément appelés "**Systèmes d'information industriels**" (SII). Bien plus spécifiquement nommés pour la partie GIO en termes de : "**Systèmes de contrôle industriel**" ou **Industrial Control system (ICS)**".

En général, un système SII regroupe plusieurs types de systèmes de contrôle spécifiques à chaque installation et utilisation.

Dans notre cas, tous les systèmes sont existants aussi bien ceux dans le département "Recherche et Développement" que le département des opérations purement industrielles.

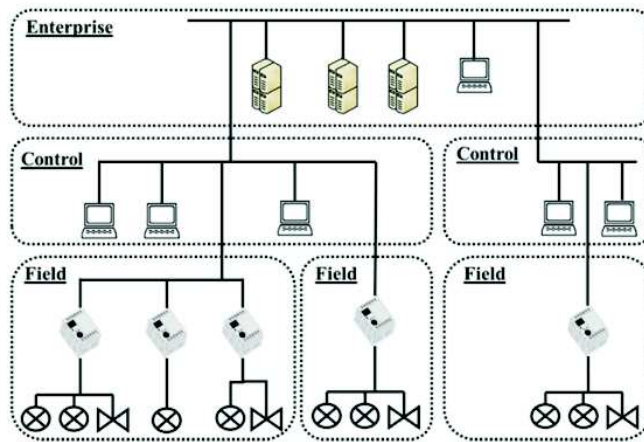


Fig. 2.3: Structure des installations dans l'OT - (Source : ISA)

En général, les installations suivent une seule et même structure d'architecture comme visualisé avec la figure 2.3.

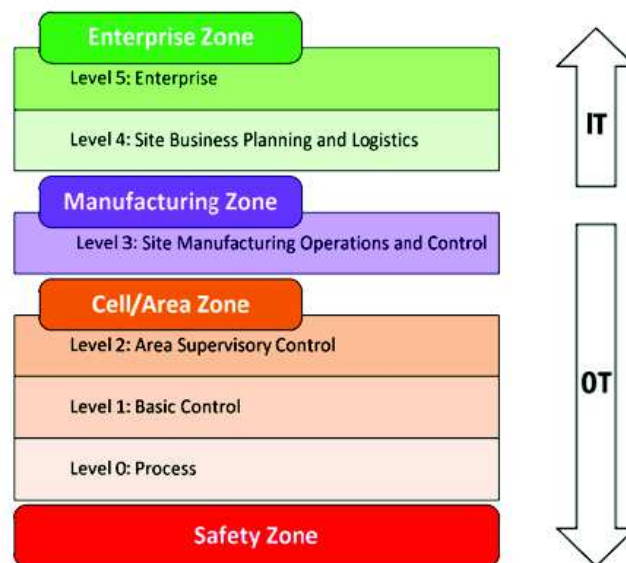


Fig. 2.4: Modèle logique hiérarchique de PERA : IT vs OT - (Source : ISA)

Cette architecture est détaillée selon le modèle de PERA qui permet de contrôler de manière hiérarchique et logique les différents niveaux d'interconnexions au sein des zones dédiées à l'IT et l'OT.[ANS10]

La figure 2.4 montre que la majorité des systèmes OT étaient propriétaires, analogiques et uniquement supportés par les vendeurs/fournisseurs du produit.

- IT : Le segment du réseau d'entreprise (Office) qui fonctionne de la même manière qu'un réseau général d'information et de communication, effectue ainsi les mêmes opérations, telle que la communication via les lignes WAN.
- OT : Le segment de réseau d'équipements de laboratoire, fabrication, de surveillance ou d'acquisition : Il contient aussi des serveurs, des postes de travail, des PLC, des HMI et des data historians entre autres.

Les systèmes et sous-systèmes industriels les plus récents sont maintenant une combinaison des technologies opérationnelles (OT) et des technologies de l'information (IT).

Quelques exemples en R&D :

- **Clinical Analytics and Automation Solutions - (CAAS)**
Une solution d'analyse clinique améliore la qualité et les résultats des recherches cliniques en permettant d'utiliser, de partager et d'analyser des données structurées et non-structurées.
- **Laboratory Instrument Control Systems (LICS)**
Ensemble des systèmes contenant d'équipements et d'instruments scientifiques à des fins de recherches et développements scientifiques dans le but d'acquérir des données et de les exploiter de la meilleure des manières qu'il soit.
- **Laboratory Information Management Systems (LIMS)**
Un système de gestion de l'information de laboratoire (LIMS) permet de gérer efficacement des échantillons et leurs données. Un laboratoire peut de la sorte automatiser son flux de travail et intégrer des instruments.

Quelques exemples en GIO :

- **Building Automation Systems (BAS)**
Un système d'automatisation du bâtiment est un type d'ICS qui surveille et contrôle les services d'infrastructure d'un bâtiment tels que le chauffage, la ventilation, la climatisation et le refroidissement (HVAC), l'éclairage, les pare-soleil, la protection contre les incendies, la gestion de l'énergie.
- **Process Control Systems (PCS)**
Un système de contrôle de processus contrôle un processus d'automatisation dans un environnement de fabrication.
Des exemples de PCS sont des systèmes d'information industriel qui surveillent et contrôlent les processus pour produire des médicaments ou des adhésifs dans un processus discontinu ou des produits chimiques dans un processus continu.
- **Supervisory Control and Data Acquisition (SCADA)**
Un système d'acquisition et de contrôle de données est un type d'ICS qui collecte des données et surveille l'automatisation des processus dans des zones géographiques éloignées les unes des autres.

2.1.3 Utilisation

Dans l'industrie pharmaceutique, un système informatiques est plus qu'un simple ordinateur et l'ensemble de ses logiciels, système d'exploitation compris.

Il est inclus aussi tout la documentation comment fonctionne, les équipes qui le supportent tout comme toutes les fonctions de contrôle et les processus permettant l'exécution complète dans l'environnement de travail qui lui est dédié.

Tous les éléments ensemble sont ce qu'on appelle "Computerized Systems". Les figures 2.5 et 2.8 nous montrent cette relation.



Fig. 2.5: Computer System vs Computerized System - (Source : GSK)

Ce qui nous prouve qu'un systèmes informatique n'est vraiment qu'un actif de support pour le bien fonctionnement de tout un corps de métier complet.

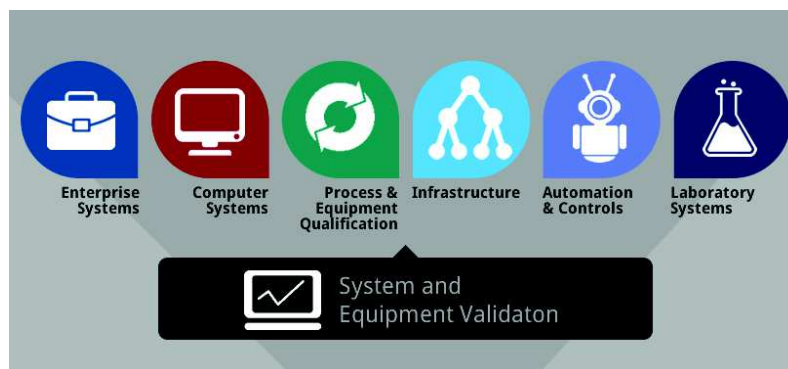


Fig. 2.6: Système et validation des équipements - (Source : Sanofi)

2.1.4 Cycle de vie

En raison de la durée de vie économique des composants industriels, aussi bien logiciels que matériels. La majorité des systèmes en milieu industriel pharmaceutique sont construits à partir d'une base de matériels déjà installée et vieillissante ou devenue obsolète avec en parallèle des systèmes d'exploitation et logiciels qui ne peuvent être remplacés que de manière délicate.

Bien que ce fait soit accepté par les propriétaires des systèmes et autres acteurs, cela a de l'importance de faire un choix judicieux en ce qui a trait à la sécurisation des systèmes lorsque des possibilités de migration apparaissent. Le remplacement des systèmes hérités par un nouveau système sans tenir compte de sa sécurisation de nos jours peut créer de sérieux risques pour l'entreprise et ce durant de nombreuses années.

Un inventaire précis des actifs, y compris les versions matérielles, logicielles et firmwares permet d'établir une stratégie de migration et de palier à toute surprise désagréable.

Cela permet une approche par étapes cohérente et une allocation des budgets en temps opportun. Le remplacement des composants industriels ne doit pas seulement être basé sur des décisions isolées limitées par des considérations budgétaires locales.

2.1.5 Limites

Selon les recherches de la société NextDefense [Har16], il est dit qu'en dehors des différences de fonctionnalité et de technologie, les systèmes OT et IT ont toujours été historiquement gérés par des unités organisationnelles distinctes. Ce qui a eu tendance à accroître ces deux tendances ci-dessous :

1. Divergence des cultures

- Les systèmes IT ont tendance à ne pas jamais s'accorder avec les personnes des départements orientés processus, en majorité par manque d'intérêt car il s'agit des termes comme pompes, moteurs, vannes et qui ne sont certainement pas de l'informatique au sens initial.
- Les départements industriels optimisent les processus et les gère, choses qui n'est pas prise en considération par les départements IT.

- Au fur et à mesure que les différentes technologies industrielles convergent vers l'informatique classique, une coopération plus étroite entre les domaines OT et IT est souhaitable. Les organisations qui ont réuni les personnes de ces différents domaines réussissent à combler l'écart, à améliorer la compréhension mutuelle et à sensiblement augmenter la position de sécurité.

2. Lacunes dans la sensibilisation, l'éducation et les intérêts

- Le personnel des systèmes industriels est habituellement constitué d'employés d'âge moyen ayant une vaste connaissance et une expérience des technologies industrielles, mais ne possède que rarement une éducation accrue sur les développements actuels des systèmes classiques.
- D'une manière conventionnelle, les ingénieurs d'automatisation des processus n'ont pas été formés à la sécurité de l'information. Ils, tout comme leurs employeurs, ignorent en grande partie qu'une tâche a été ajoutée à leur profil d'emploi.
- Même lorsque les gestionnaires de l'automatisation des processus sont conscients des problèmes de sécurité informatique, ils trouvent rarement une oreille d'écoute dans la hiérarchie, car la mise en œuvre de la sécurité pour les systèmes industriels coûte souvent beaucoup d'argent (malgré le risque potentiel d'impact sur les entreprises).
- Le personnel informatique est, quant à lui, constitué en général des employés plus jeunes ayant généralement plus de connaissances sur la sécurité informatique. Cependant, ces personnes ne font pas l'effort de sécuriser les systèmes industriels, car dans l'automatisation et le contrôle des processus, il n'existe pas de reconnaissance des aspects informatiques. Même s'ils le font, ils ne connaissent généralement pas les particularités et les limites des technologies industrielles.
- Chaque fois que des ingénieurs d'automatisation des processus et des personnes des services informatiques essaient de travailler ensemble, une énorme différence culturelle devient évidente entre l'approche de contrôle des processus (tourner sans interruption 24h/7) d'une part, et l'approche de gestion informatique (juste relancer pendant le temps de midi) d'autre part.

Cela étant grâce aux efforts de chacun et la convergence qui a commencé depuis un certain temps les difficultés s'amenuisent.