



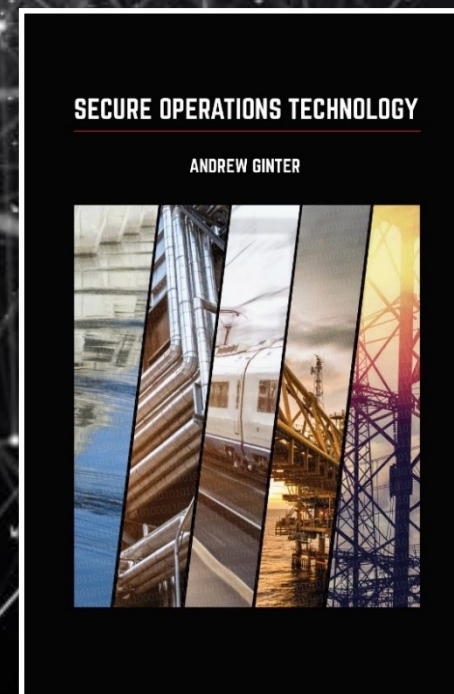
# Secure Operations Technology

Perspective, Méthodes et meilleures pratiques

**Thierry Kolton**

Star-Achats, Distributeur Waterfall Security  
Solutions , [contact@star-achats.com](mailto:contact@star-achats.com)

2019



# SECURE OPERATIONS TECHNOLOGY



**IT-SEC:**

Protéger l'information



**SEC-OT :**

Protéger les opérations  
physiques **de** l'information



Photo credit: shannonpatrick17 / CC BY-SA 2.0

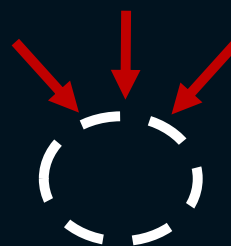
# PERIMÈTRES ONLINE & OFFLINE



Stronger Than Firewalls



Il y a **toujours** des  
périmètres autour de réseaux  
et sites industriels  
importants



Des flux d'information  
entrants sont aussi des  
vecteurs d'attaque



# TOUT LOGICIEL PEUT ÊTRE COMPROMIS

- Tout flux d'information peut être un vecteur d'attaque
- Focus sur la protection physique, non logicielle contre des cyberattaques



# CONTRÔLES OFFLINE

Offline Survey

Test Beds

Removable Media

Removable Devices

New Cyber Assets

Insider Attacks

Deceived Insiders

Nonessential Equipment

Interdire les parefeu de l'OT  
vers l'IT – n'autoriser que des  
passerelles unidirectionnelles

# CONTRÔLES ONLINE

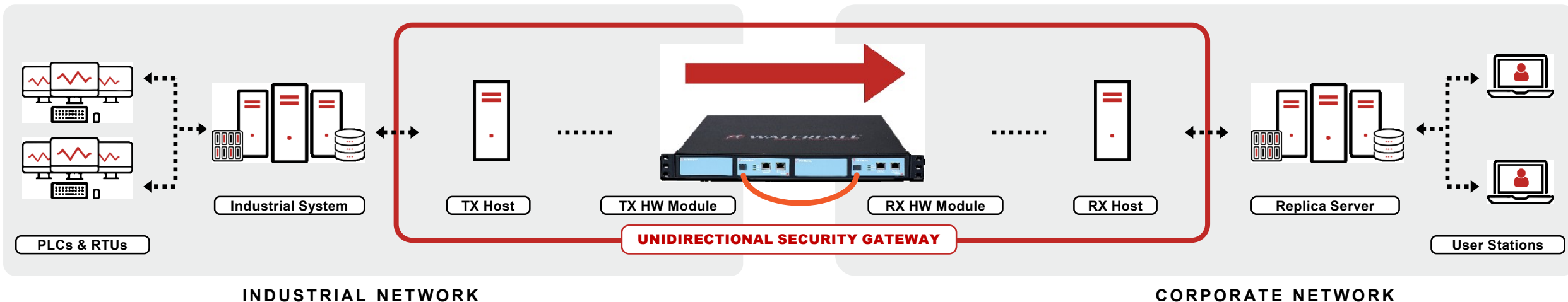
Utiliser les parefeu  
pour la segmentation  
inter ICS

Meilleure pratique SEC-  
OT: 1 niveau de  
passerelles  
unidirectionnelles pour  
défense en profondeur

**WHAT'S NEW:** two dozen unidirectional network  
reference architectures



# Passerelle Unidirectionnelle



## NIST 800-82 R2: Des Passerelles de Sécurité Unidirectionnelles sont une combinaison de **matériels** et **logiciels**

- Le matériel ne peut physiquement envoyer l'information que dans une seule direction
- Le logiciel réplique des serveurs et émule des automates du réseau OT vers le réseau IT
- Toutes les attaques sont des informations— aucune attaque même sophistiquée ne peut revenir vers le réseau OT à travers la passerelle

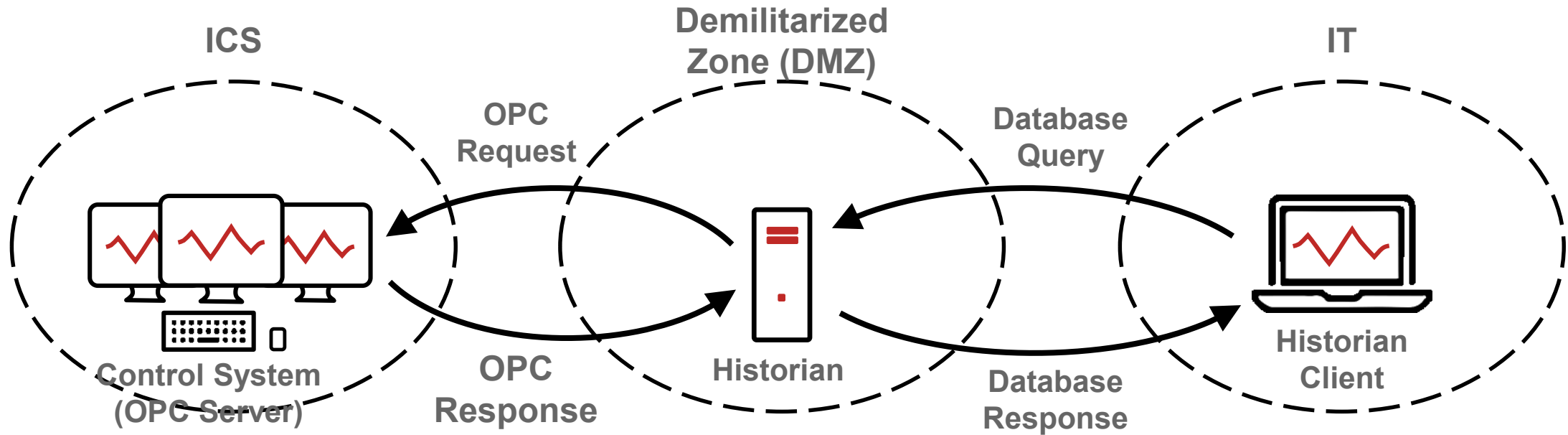
# EXAMPLES D'UTILISATION



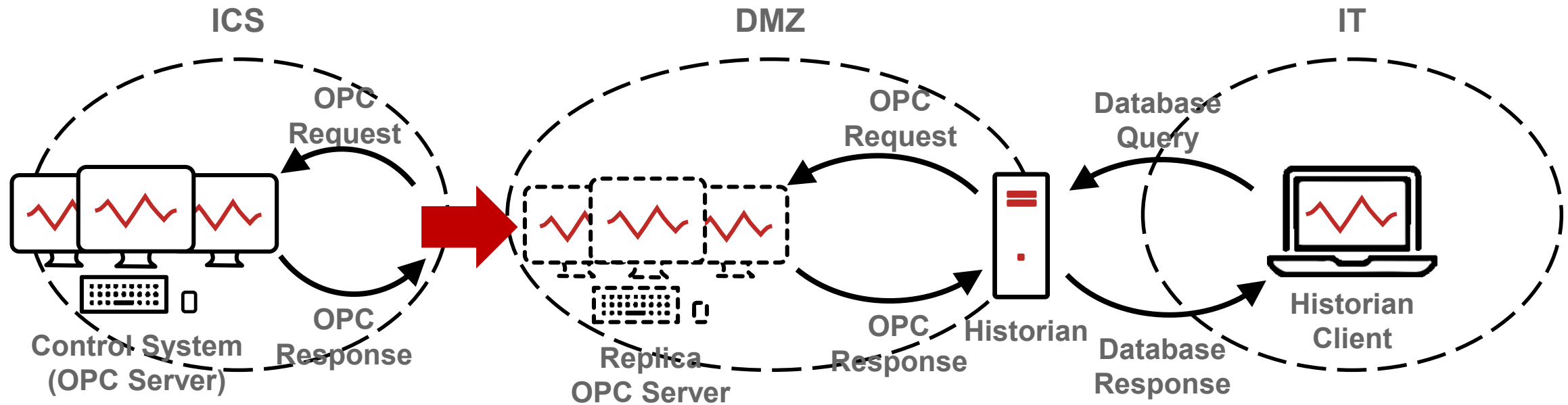
#1 Database Replication	#8 Central or Cloud SOC	#15 Safety Systems
#2 Device Emulation	#9 Network Intrusion Detection Systems	#16 Continuous High-Level Control
#3 Application Replication	#10 Convenient File Transfer	#17 SCADA WAN
#4 Remote Diagnostics & Maintenance	#11 IIoT And Cloud Communications	#18 Protective Relays
#5 Emergency Maintenance	#12 Electronic Mail and Web Browsing	#19 Replicas DMZ
#6 Continuous Remote Operation	#13 Partial Replication Protecting Trade Secrets	#20 Wireless Networks
#7 Device Data Sniffing	#14 Scheduled Updates	



# Exemple: Requête / Réponse

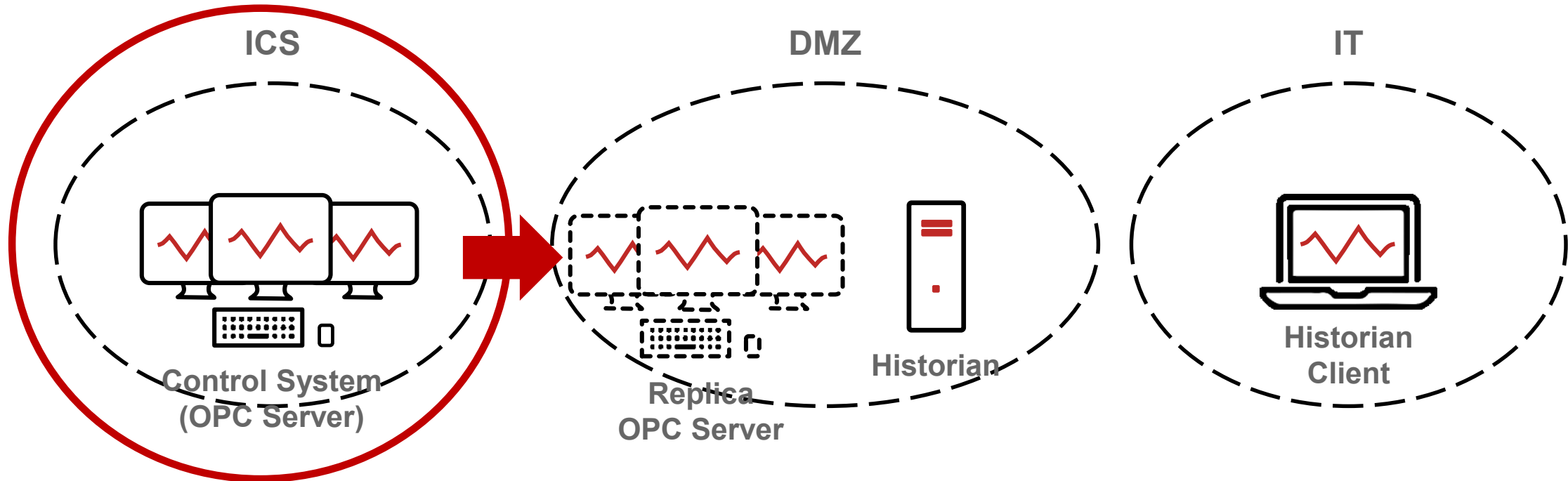


# Réplication Serveur OPC



***La replication du serveur OPC évite d'envoyer des requêtes de la DMZ vers le reseau OT,***

# Réplication Serveur OPC



## Control-Critical Network

***Le reseau industriel dans cet exemple est le reseau critique  
Aucune communication entrante***



- Invités venant de multiples horizons Cybersécurité Systèmes Industriels
  - Fournisseurs – défis, technos & approches
  - Agences gouvernementales – programmes & ressources
  - Opérateurs – priorités & approches



***<https://waterfall-security.com/podcasts>***

# La société



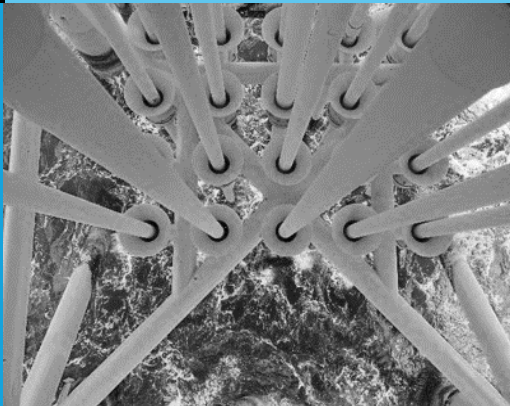
**Création en  
2007**



**1000+ sites  
Dans le  
monde**



**Fiabilité et  
sûreté des  
systems  
industriels**



**Protection  
contre les  
attaques à  
distance**



**Déploiements  
aux Etats-  
Unis, Asie et  
Europe**



**Certification  
ANSSI CSPN**



**Partenaires  
Globaux**



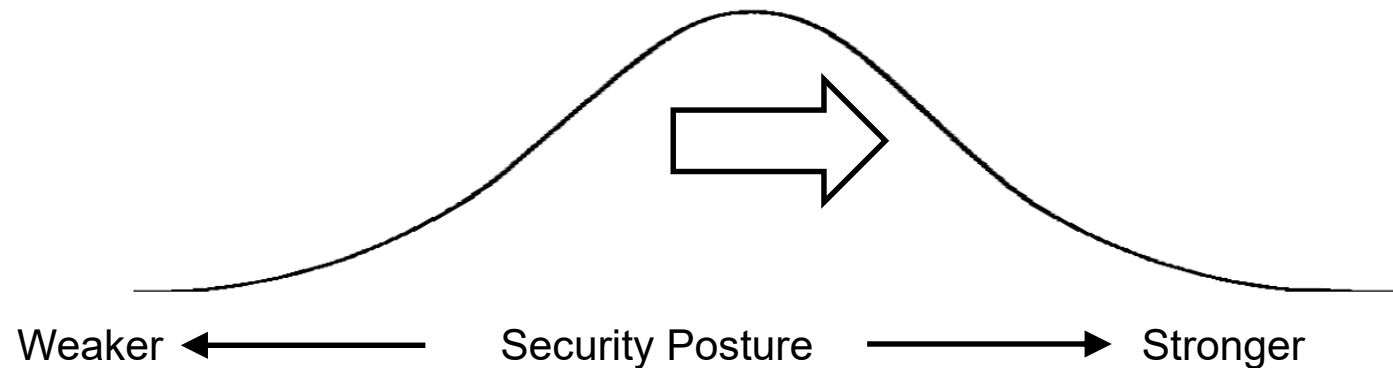
# Secure Operation Technology



**Attack capabilities  
only increase,  
so must our  
security posture**

**All Attacks Are  
Information  
Protect Physical  
Operations From  
Information**

**Waterfall: Safe OT  
Visibility  
With Disciplined  
Control**



**Obtenir l'ouvrage gratuitement :  
[France@waterfall-security.com](mailto:France@waterfall-security.com)**

