A Holistic Approach to Critical Infrastructure Protection

GIE Security Day, Brussels

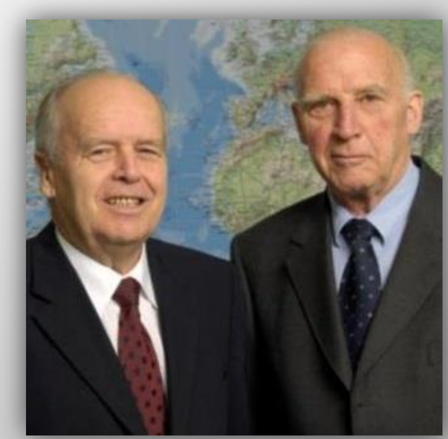
ILF
CONSULTING
ENGINEERS

ENGINEERING
EXCELLENCE

Michael Barth, November 16th, 2016

The ILF Group

1967	year of founding, development into a leading engineering, consulting and project management firm
100%	privately owned & independent
2,000+	employees
40+	offices
6,000+	projects
100+	countries
200+	million € revenue



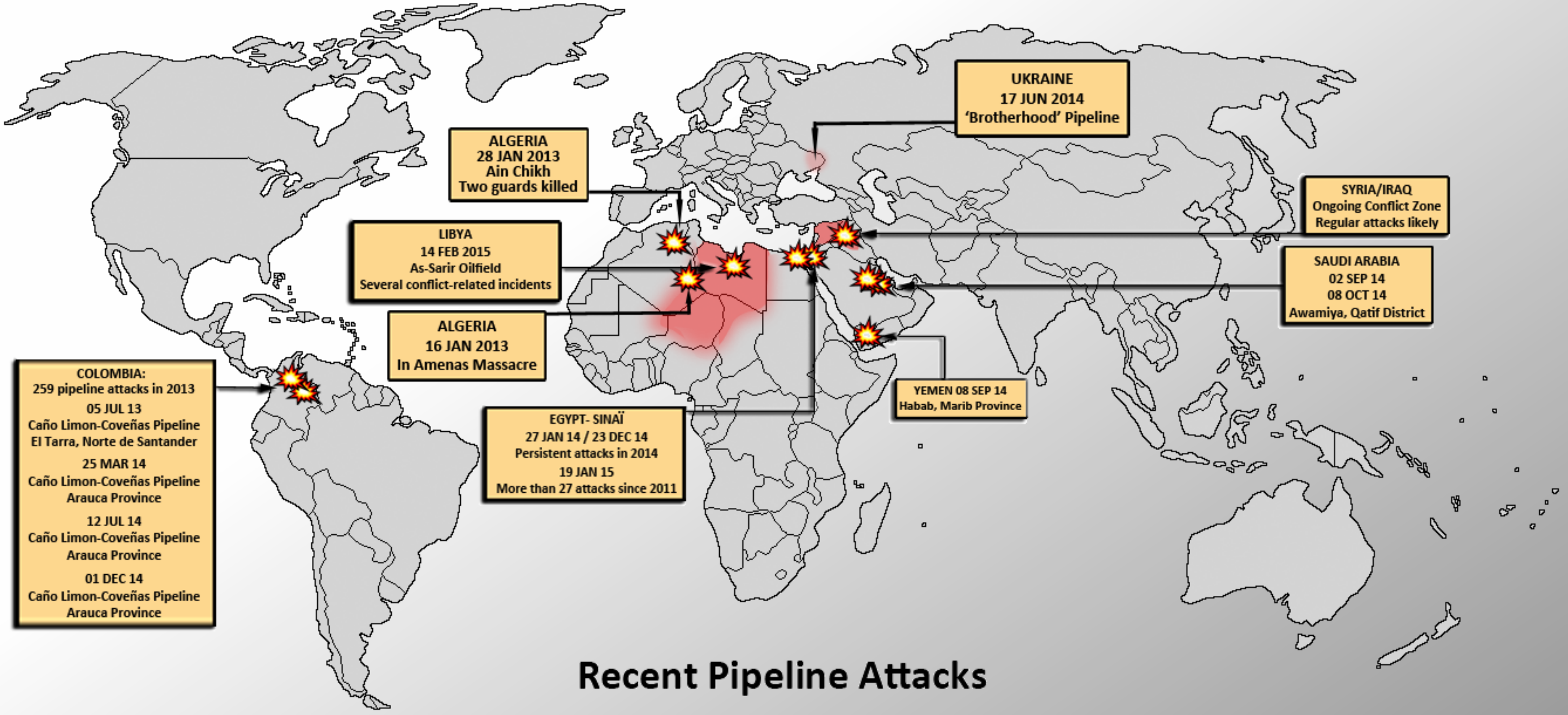
Agenda

1. Attacks against Critical Infrastructure
2. Changes in Legislation and Standardization
3. A Systematic and Integrated Approach to Security
4. Conclusions

Section 1

Attacks against Critical Infrastructure

A Holistic Approach To Critical Infrastructure Protection



UKRAINE
17 JUN 2014
'Brotherhood' Pipeline

ALGERIA
28 JAN 2013
Ain Chikh
Two guards killed

SYRIA/IRAQ
Ongoing Conflict Zone
Regular attacks likely

LIBYA
14 FEB 2015
As-Sarir Oilfield
Several conflict-related incidents

SAUDI ARABIA
02 SEP 14
08 OCT 14
Awamiya, Qatif District

ALGERIA
16 JAN 2013
In Amenas Massacre

COLOMBIA:
259 pipeline attacks in 2013
05 JUL 13
Caño Limon-Coveñas Pipeline
El Tarra, Norte de Santander
25 MAR 14
Caño Limon-Coveñas Pipeline
Arauca Province
12 JUL 14
Caño Limon-Coveñas Pipeline
Arauca Province
01 DEC 14
Caño Limon-Coveñas Pipeline
Arauca Province

YEMEN 08 SEP 14
Habab, Marib Province

EGYPT- SINAÏ
27 JAN 14 / 23 DEC 14
Persistent attacks in 2014
19 JAN 15
More than 27 attacks since 2011

Recent Pipeline Attacks

🟥 - MENA: Current ongoing Zones of Conflict

A Holistic Approach To Critical Infrastructure Protection

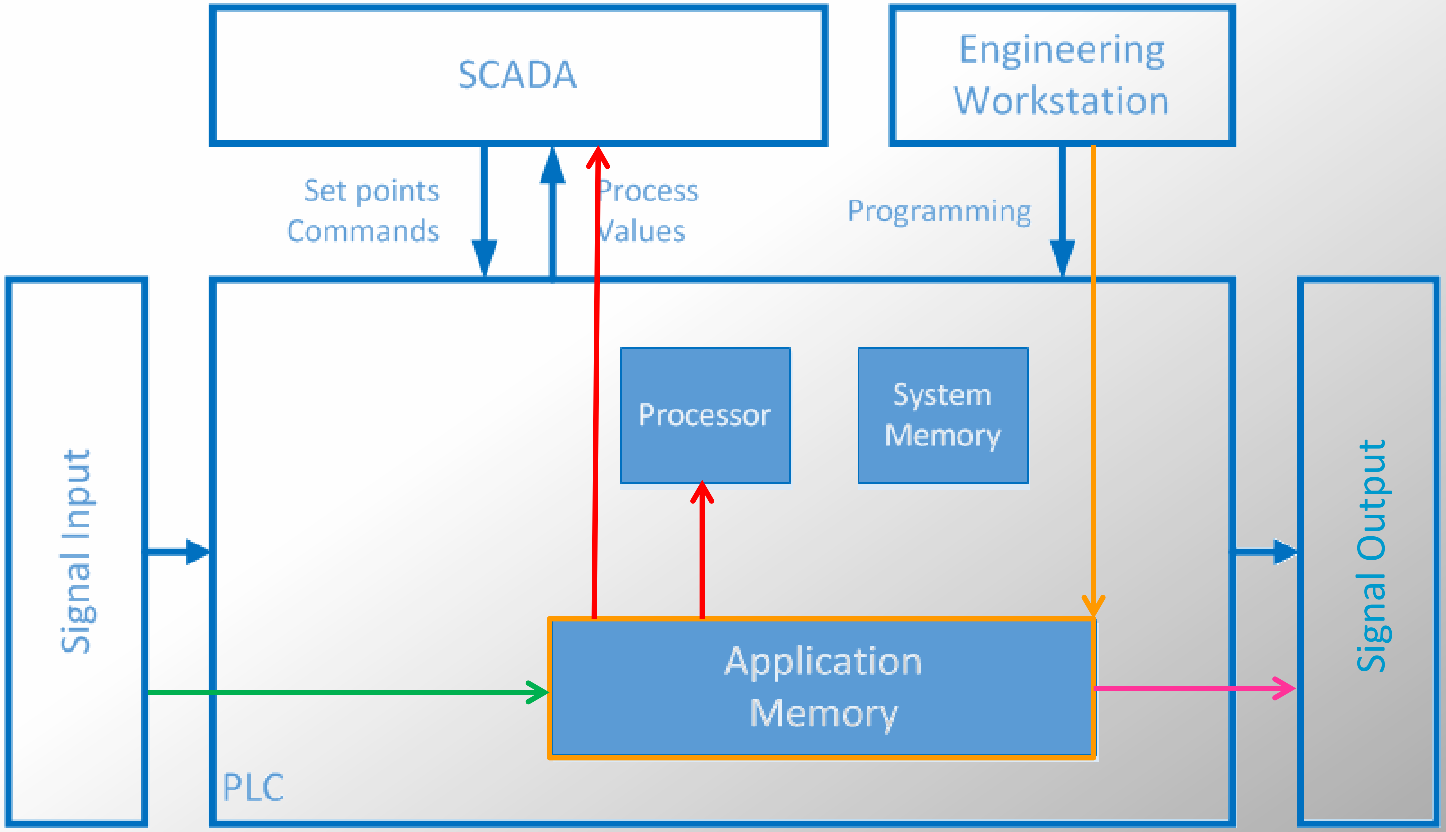
Detected in	Malware	Characteristics
2010	Stuxnet	Attack against the Uranium Enrichment Plant at Natanz/ Iran with the goal to damage centrifuges • Code injection into the PLC • Manipulation of Safety System
2011 - 2014	Duqu, Flame, Gauss	Sophisticated information stealers
2012	Havex / Draconfly	Attacks against energy firms in Western Europe and North America via trojanized ICS software
2012		Attack against the Maintenance Center of a major SCADA system provider
2015	Spear phishing BlackEnergy Manipulated Firmware	Attack against Ukrainian power companies, operating in manual mode for about 6 months
2016	Ransomware DDoS attack against Dyn	Encrypts e.g. hard disks, according to German BSI about 1/3 of enterprises hit Executed by a botnet of IoT devices, many Internet services where not reachable

A Holistic Approach To Critical Infrastructure Protection

Dangerous trends with regard to Cyber Security:

- Networks are breached following a stock-piling approach
- 46% of all breaches without any sign of malware
- Attacks on HW- level
- Malware and back doors hidden in firmware

A Holistic Approach To Critical Infrastructure Protection



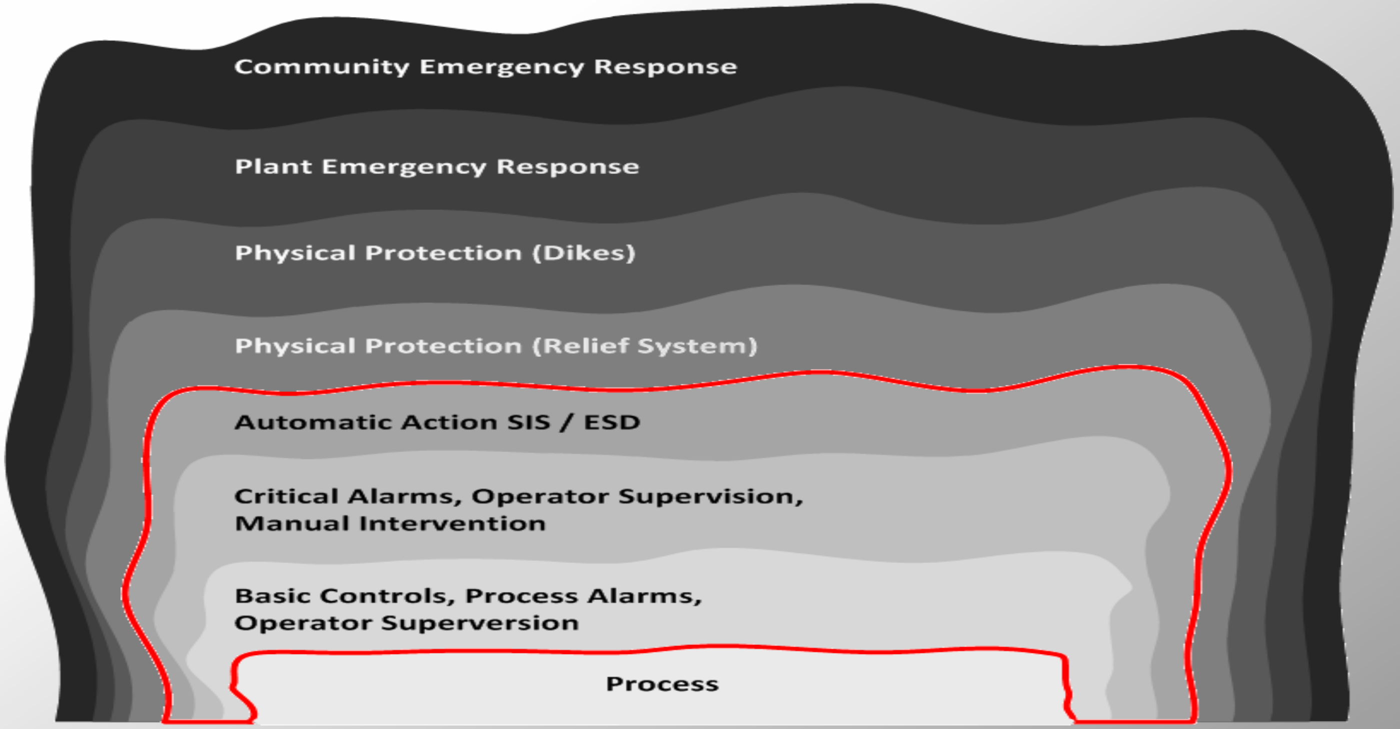
1. Modify main scan routine and inject additional routines
2. Record input values for some time
3. Disable scan cycle and replay recorded values to SCADA
4. Write outputs (change set points and send commands), independently from operator

A Holistic Approach To Critical Infrastructure Protection

Functional Layer	Attack Technique	Attacked Entity	Goals	Mainly Using
Enterprise	Water-holing Spear-phishing	SW Vendors Pipeline Operator Service Provider	Penetration Data Exfiltration Propagation	BUGS
SCADA	Trojanised Vendor SW Remote Access	SW Vendors Pipeline Operator Service Provider	Gain Remote Access	
Control	EWS Compromise Legitimate Commands PLC Code Manipulation	System Integrator Pipeline Operator Service Provider	Gain Control	FEATURES
Process	Sensor De- Calibration Fake Sensor Data	Pipeline Operator	Disrupt Process Damage Equipment	
Safety Systems	Sensor De- Calibration Physical manipulation	Pipeline Operator	Disable Protection Systems	

A Holistic Approach To Critical Infrastructure Protection

Consequence of a successful attack: **Layers of Protection compromised**


Community Emergency Response
Plant Emergency Response
Physical Protection (Dikes)
Physical Protection (Relief System)
Automatic Action SIS / ESD
Critical Alarms, Operator Supervision, Manual Intervention
Basic Controls, Process Alarms, Operator Superversion
Process

Consequences of a successful attack

- Dept. of Homeland Security
  - Up to 6 months to fully recover from a cyber attack assuming no major equipment damage
  - Plus lead times for replacing damaged equipment

- Ukrainian Power Grid
  - Power outage for several hours, about 225.000 customers impacted
  - Grid was operated for months in manual even thought there was no major equipment damage

    Amplifying attacks:

    - hard disks and storage cards in workstations, servers and HMI wiped
    - Firmware attacks against the Serial-to-Ethernet devices at substations

Section 2

Changes in Legislation & Standardization

A Holistic Approach To Critical Infrastructure Protection

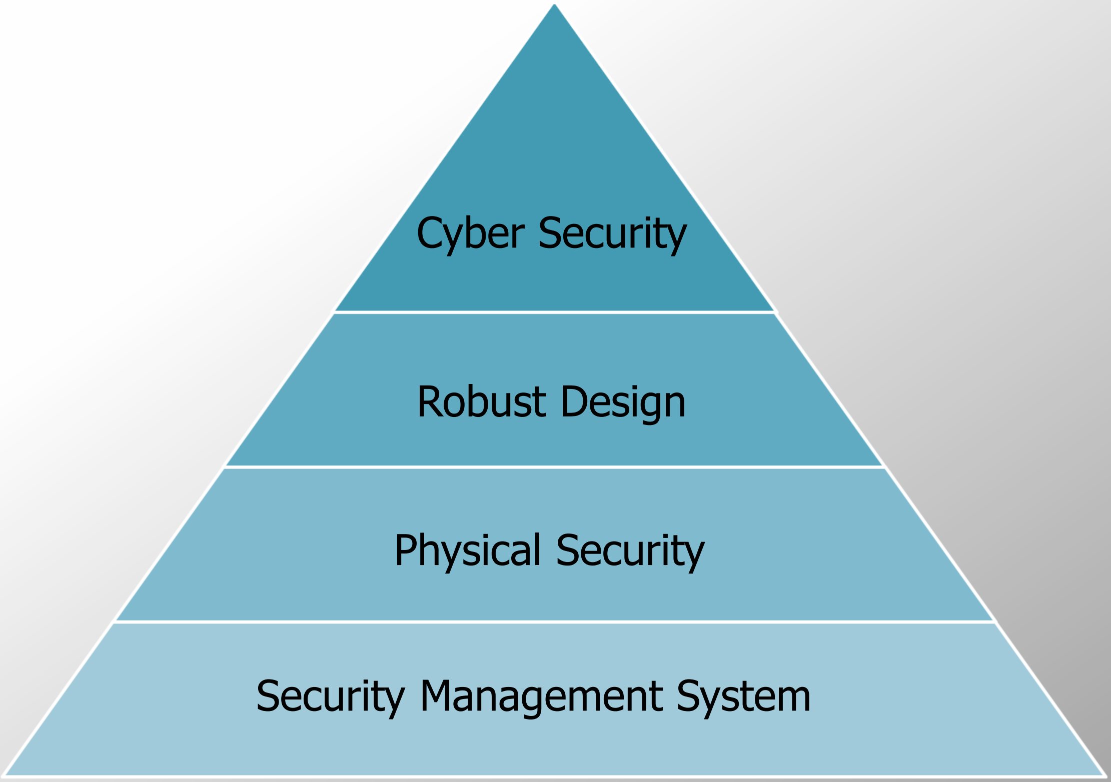
- Programs and Agencies for Critical Infrastructure Protection
  - e.g. EU, Germany, Netherlands, USA, Canada, UK, Australia, U.A.E., South Africa
- Laws
  - the German “IT Sicherheitsgesetz”
  - European “Network and Information Security Directive”
- Industry and Corporate Standards
  - NERC CIP
  - Shell DEPs

- IEC 61511 ed. 2
  - New security risk assessments included HAZOPs, relating to malicious interference
  - Measures making the SIS sufficiently resilient against identified security risks
  - Independence, diversity and physical separation between protection layers
- ISA 99 / IEC 62443 – Security for Industrial Automation Systems
  - Integrated Security Management System
  - Physical separation of networks into Zones and Conduits, Foundational Requirements
- IEC 62351 – information security for power system control operations

Section 3

A Systematic & Integrated Approach to Security

Security Master Plan



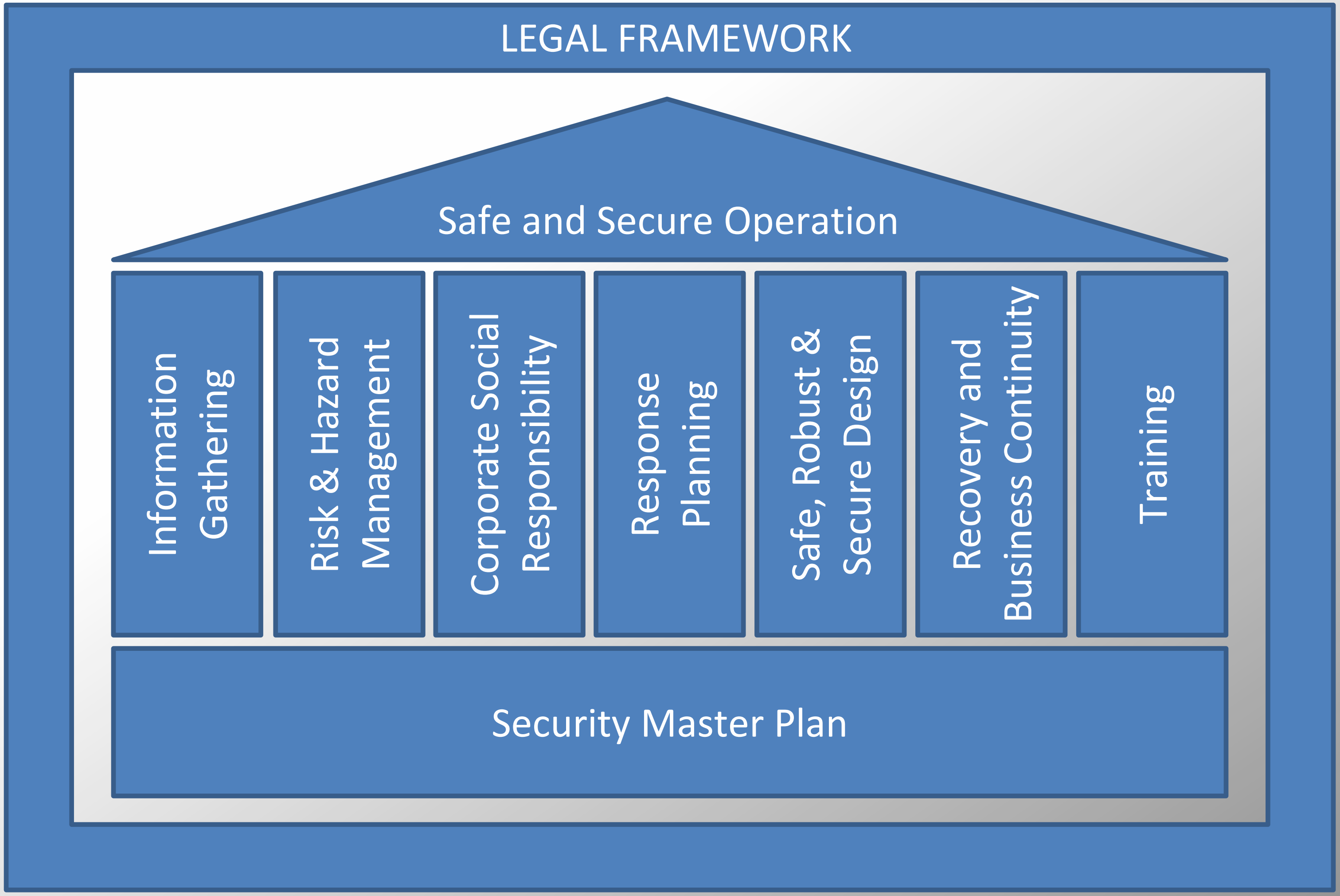
Cyber Security

Robust Design

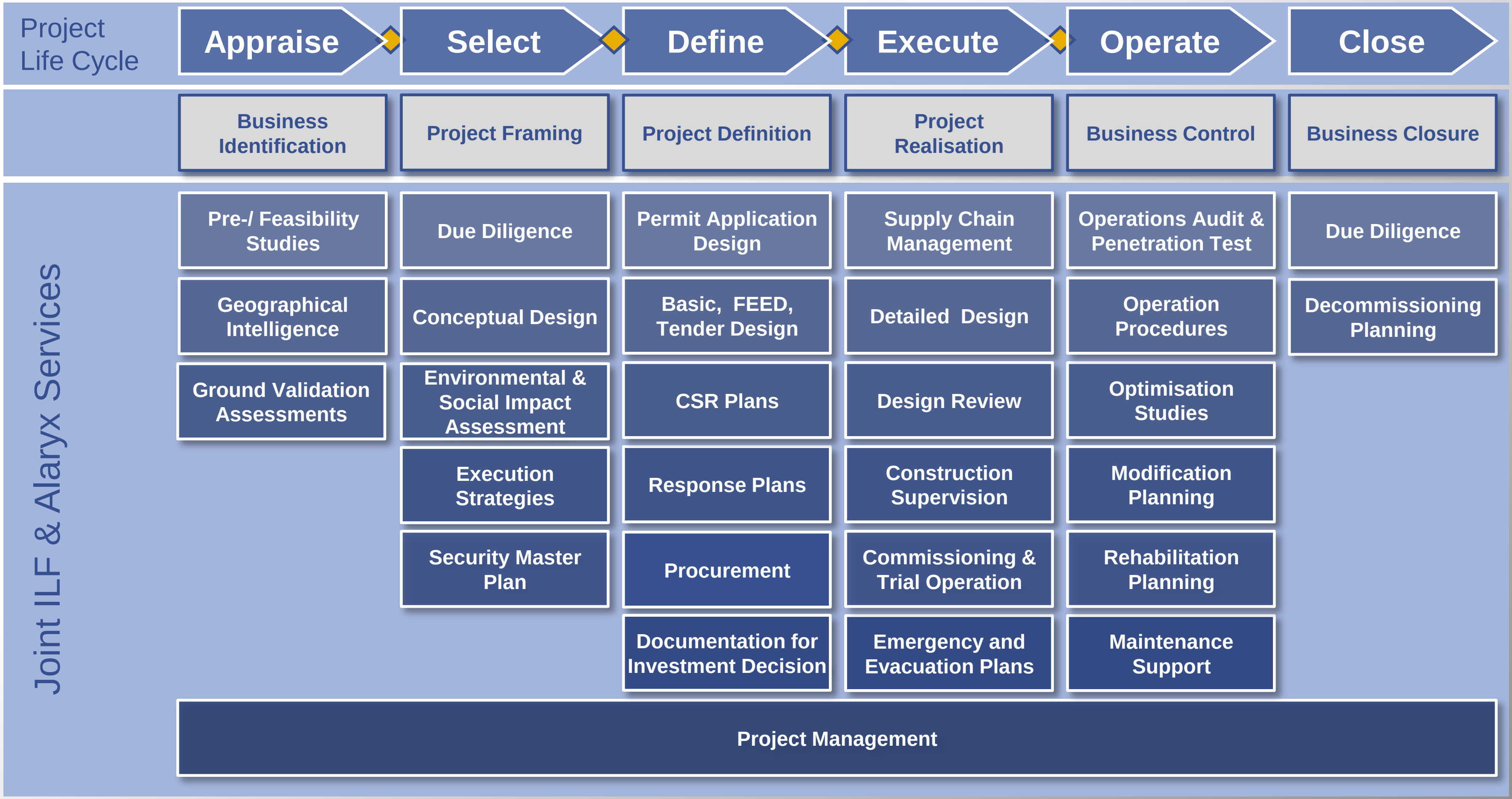
Physical Security

Security Management System

A Holistic Approach To Critical Infrastructure Protection
A Joint ILF and ALARYX Concept


LEGAL FRAMEWORK
Safe and Secure Operation
Information Gathering
Risk & Hazard Management
Corporate Social Responsibility
Response Planning
Safe, Robust & Secure Design
Recovery and Business Continuity
Training
Security Master Plan

A Holistic Approach To Critical Infrastructure Protection
A Joint ILF and ALARYX Concept



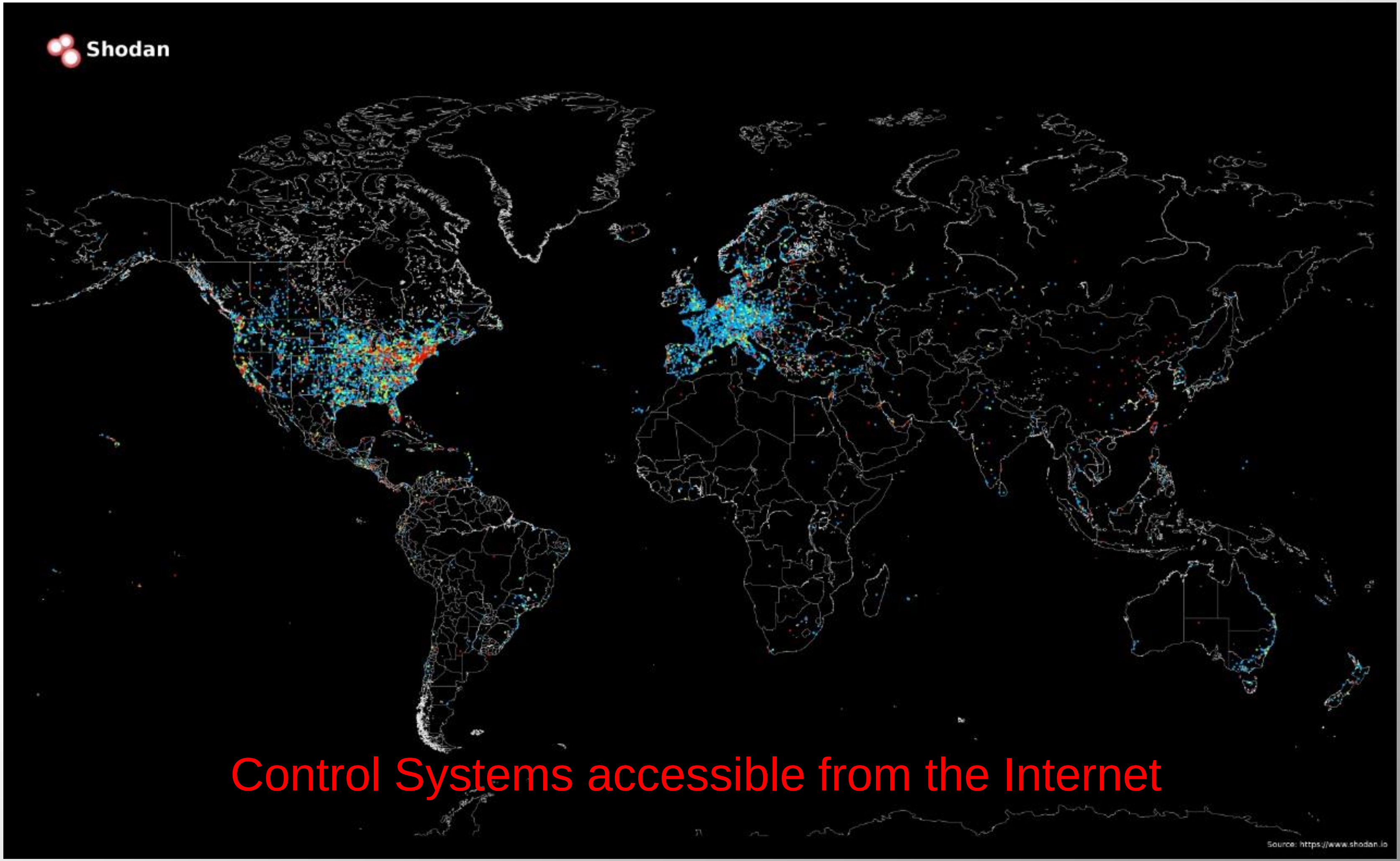
Project Life Cycle	Appraise	Select	Define	Execute	Operate	Close
	Business Identification	Project Framing	Project Definition	Project Realisation	Business Control	Business Closure
Joint ILF & Alaryx Services	Pre-/ Feasibility Studies	Due Diligence	Permit Application Design	Supply Chain Management	Operations Audit & Penetration Test	Due Diligence
	Geographical Intelligence	Conceptual Design	Basic, FEED, Tender Design	Detailed Design	Operation Procedures	Decommissioning Planning
	Ground Validation Assessments	Environmental & Social Impact Assessment	CSR Plans	Design Review	Optimisation Studies	
		Execution Strategies	Response Plans	Construction Supervision	Modification Planning	
		Security Master Plan	Procurement	Commissioning & Trial Operation	Rehabilitation Planning	
			Documentation for Investment Decision	Emergency and Evacuation Plans	Maintenance Support	
	Project Management					

ILF integrates “Security Engineering” into standard engineering process

Section 3

Conclusions

A Holistic Approach To Critical Infrastructure Protection



Control Systems accessible from the Internet

Source: https://www.shodan.io

Contact Details

Michael BARTH

website:	www.ilf.com
e-mail:	Michael.Barth@ilf.com
voice:	+49 (0)89 / 25 55 94 - 118
fax:	+49 (0)89 / 25 55 94 - 144

A Holistic Approach to Critical Infrastructure Protection

ILF CONSULTING ENGINEERS

Thank you for your attention!

多谢你们的关注!

Спасибо за внимание!

أشكركم على حسن استماعكم !

Vielen Dank für Ihre Aufmerksamkeit!