

No Safety without Security  
No Security without Safety



# Agenda

- Introduction
- Modern history of industrial disasters
- Functional Safety standards milestones
- 20 years later – What have we learned?
- Introduction to underlying digital computing security problems
- How to manage security vulnerabilities improvements
- Primary focus
- Summary



# Tino Vande Capelle, B.Eng.



- Native Flemish Belgium, 5 languages
- Started as Instrument engineer - LNG plant Belgium
- SIS Engineering 30+ years
- Principal Functional Safety Consultancy at TVC
- Director – Functional Safety Consultancy at GM International
- Functional Safety Senior Expert & Trainer (TÜV Rheinland) SIS #109/05
- ISA84 committee member

# Modern history of industrial disasters



- Failures at cost of life



- Failure at cost of environment



- Failure at cost of corporate image, profitability, production, ... etc

# Piper Alpha, Occidental Petroleum

NORTH SEA - 6 JULY 1988

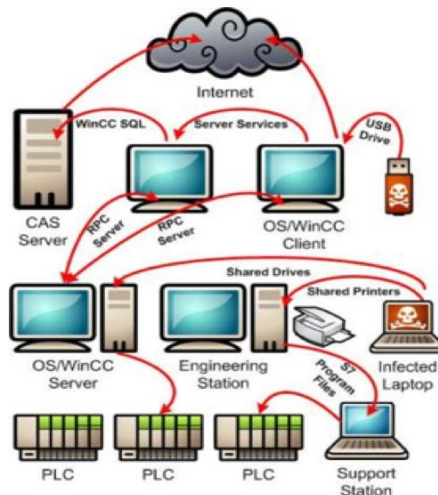


- Original designed for oil production, later modified for oil & gas production
- Explosion and fire claimed 167 lives, only 61 survivors
- Worst offshore accident
- HSE investigation was leading to the foundation for the Functional Safety Standard IEC61508



# Natanz Uranium Enrichment Plant

IRAN - JAN .. JUN 2010



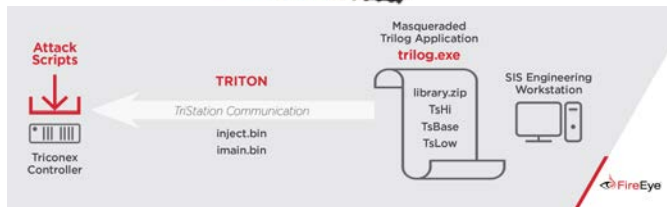
- Fact Sheet StuxNet virus,
- January 2010, IAEA inspection anomaly
- 17 June 2010:
  - Computer reboot loop in Iran
  - Rare Zero Day Exploit
  - Microsoft labels as ‘Stuxnet’
  - Identified 3 versions dating from June 2009
  - Targets Siemens Simatic systems

# TRITON/TRISIS

## SAUDI ARABIA – TARGETING TRICON SIS AUG .. DEC 2017










- Attacker gained remote access
- SIS chassis left with key to program
- SIS initiated a safe shutdown, causing operational disruption



Source: fireeye.com

# Functional Safety Milestones

- 1989 DIN V 19250 - Safety Systems principles 
- 1996 ISA SP84 - Safety Lifecycle 
- 1997 IEC 61508 ED1 - Safety Lifecycle E/E/PES 
- 2004 IEC 61511 ED1 == ANSI/ISA 84.00.01  
Functional Safety, SIS for the Process industry sector  
- 2010 IEC 61508 ED2- Safety Lifecycle E/E/PES  
04/2010 maintenance revision released 
- 2016 IEC 61511 ED2  
Functional Safety, SIS for the Process industry  
(Part 1 02/2016, Part 2 & 3 07/2016, TR0 01/2018) 





# IEC61508:2010

- Ed 2.0 changed things like, but not limited to:
  - Safety Manual - for the end user to understand the details...
  - Route 1H vs Route 2H
  - Proof test coverage influence
  - Systematic Capability SC besides SIL
  - MTTR - Mean Time To Restoration
  - MRT - Mean Repair Time
  - Competency requirements
- But how many of you here today understand 'ALL' this or you simple 'trust' your vendor / sales person?



# IEC61511:2016

- Ed 2.0 changed things like, but not limited to:
  - Functional Safety Management for everyone supplying services/products
  - Competency procedure and period review shall be carried out
  - End users shall carry out periodic assessment
  - Modification shall not start before independent FS assessment
  - Security Risk Assessment shall be carried out
  - Simplified architectural constraint (table 6 – HFT – SIL 2 – LDM) route 2H
  - Quality failure data collection required
  - Compensation measurement during bypass shall be defined
  - ... etc
- But how many of you here today feel competent using edition 2.0?



# 20 years later - What have we learned?

- Most engineers mainly focus on PFD (SIL) calculation using sophisticated calculation tools but with generic or not applicable failure data **BUT seems to forget the real reason for applying Functional Safety Management = minimise human failures ...**
- Modern technologies forced us to digitalise and connect instruments/systems as much as possible **BUT majority of the end users have no records on what firmware in all the devices and/or systems are keeping their process industry SAFE. Furthermore keep safety and control 'Independent' and 'Separate' is not a bad practice ...**



# Technical Cyber security threats in a nutshell?

Co-author of the remaining slides is Stephen Smith, Cybersecurity and Risk Management specialist in Industrial Environments (stephen@onrix.eu)

## Rule # 1

***“Any device with software-defined behaviour can be tricked into doing things its creators did not intend”***

*WEF Global Risk Report 2012 Seventh Edition*



# Technical Cyber security threats in a nutshell?

## Rule # 2

***“Any device connected to a network of any sort, in any way, can be compromised by an external party”***

*WEF Global Risk Report 2012 Seventh Edition*



# Technical Cyber security threats in a nutshell?

## Rule # 3

***“The user’s going to pick dancing pigs over security every time.”***

*Bruce Schneier*



# Human Cyber security risks

Threat Source	% of industrial Network Incidents	Incident type
Hackers and terrorist	9.4%	Intentional
Insiders	10.6%	
Human error	11.2%	Unintentional
Malware	30.4%	
Device and software failure	38.4%	

Source: *The repository for Industrial Security Incidents (RISI) 2011*



# Humans form a critical part of the security aspects (1)

- Software development (SDLC)
  - (a) Industry Average: "about 15 - 50 errors per 1000 lines of delivered code."
  - (b) Microsoft Applications: "about 10 - 20 defects per 1000 lines of code during in-house testing, and 0.5 defect per 1000 lines of code in released product."



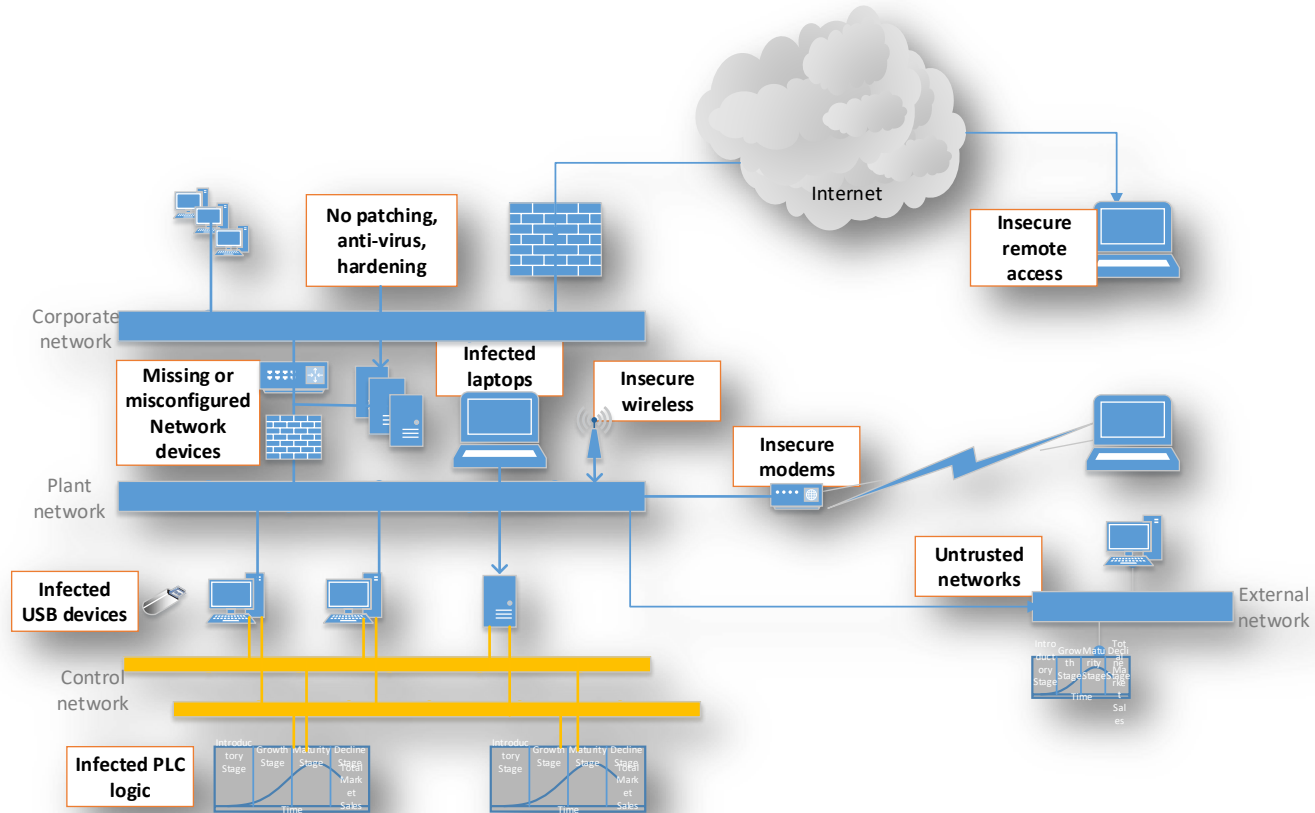


# Humans form a critical part of the security aspects (2)

- System/Device configuration
- System/Device connectivity
- System/Device usage
- System/Device maintenance



# Managing Cybersecurity



# Managing Cybersecurity

***“If you think technology can solve your security problems,  
then you don’t understand the problems and  
you don’t understand the technology.”***

*Bruce Schneier*



# Where should you start?

- ISO 27000 series – Information security management systems
- ISA99 Security Guidelines and User Resources for Industrial Automation and Control Systems
- ANSI/ISA-TR99.00.01-2007 Security Technologies for Industrial Automation and Control Systems
- ISA99 Manufacturing & Control Systems Security
- IEC 62443 series – Industrial networks and system security
- IEC 27019 series – Information security for process control in the energy industry
- National Compliance Standards
  - NIST -USA
  - NESAS – UAE
  - Norway
- Industry Standards
  - IAEA – Nuclear
- Associations / Studies / Recommendations
- ...



# Know your Digital Footprint?

- Identify all existing digital computing systems:
- Industrial control systems (SCADA, PCS,...)
- Safety systems
- Security systems (physical security, video, badging,...)
- Environmental systems (ventilation, airco, heating,...)
- Energy systems (emergency backup, batteries,...)
- Office and corporate systems (Enterprise systems, email, shared environments, etc)

*Rob Joyce, NSA chief hacker on building infrastructure:*

*“The heating and cooling systems and other elements of building infrastructure also provide unexpected pathways into your network.”*



# Start with common recommendations?

DNV GL The top ten cyber security vulnerabilities:

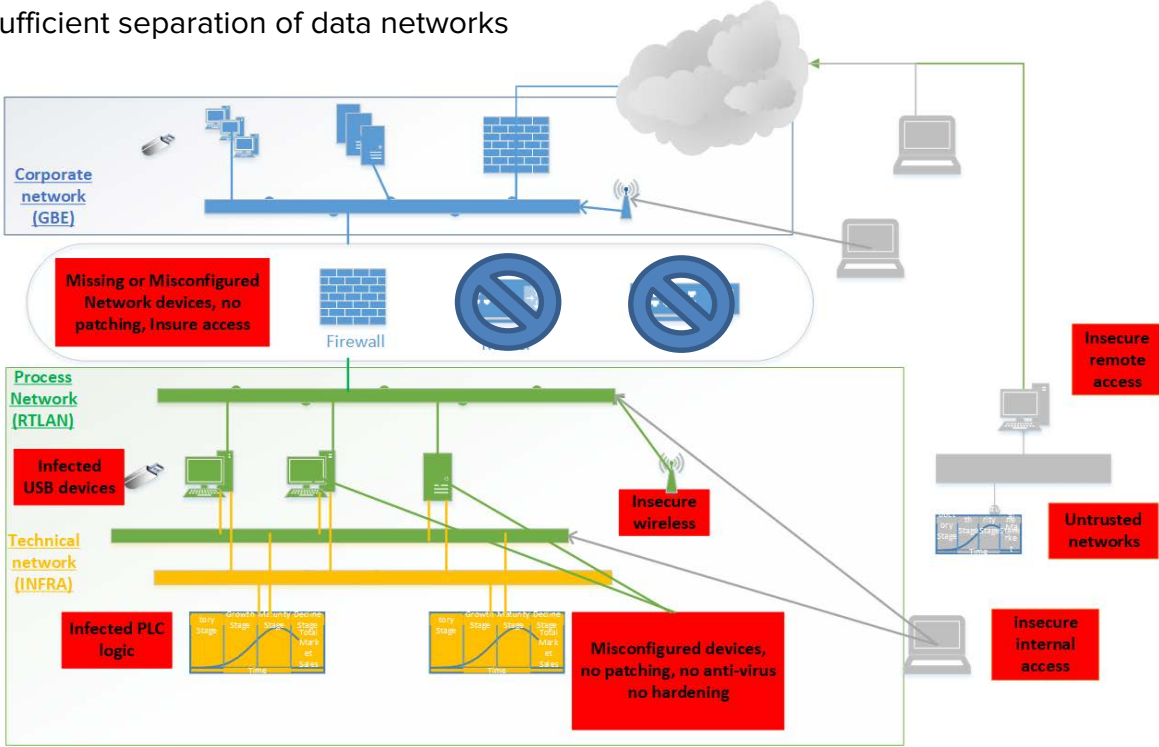
1. Lack of cyber security awareness and training among employees
2. Remote work during operations and maintenance
3. Using standard IT products with known vulnerabilities in the production environment
4. A limited cyber security culture among vendors, suppliers and contractors
5. Insufficient separation of data networks
6. The use of mobile devices and storage units including smartphones
7. Data networks between on- and offshore facilities
8. Insufficient physical security of data rooms, cabinets, etc.
9. Vulnerable software
10. Outdated and ageing control systems in facilities

\* DNV GL is today delivering a cybersecurity study to the Lysne Committee, a body appointed by the Norwegian Ministry of Justice and Public Security to assess the country's digital vulnerabilities



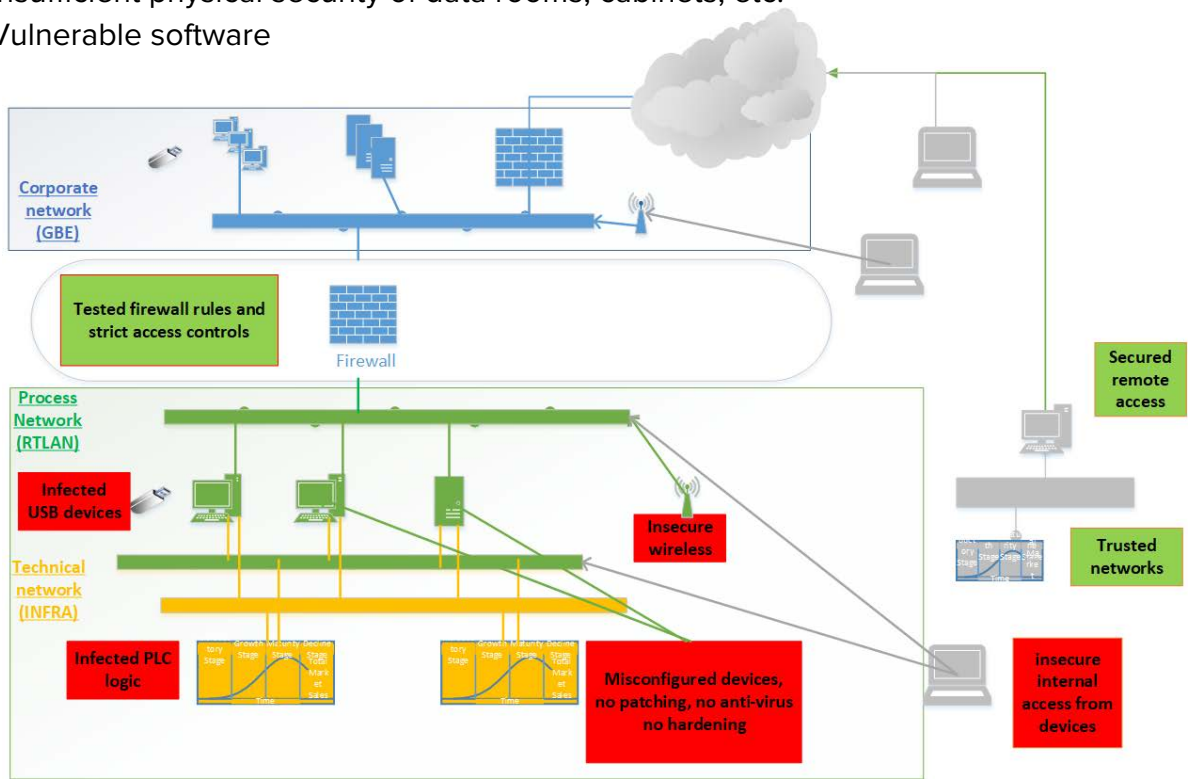
# Start with common recommendations?

- 2. Remote work during operations and maintenance
- 4. A limited cyber security culture among vendors, suppliers and contractors
- 5. Insufficient separation of data networks



# Start with common recommendations?

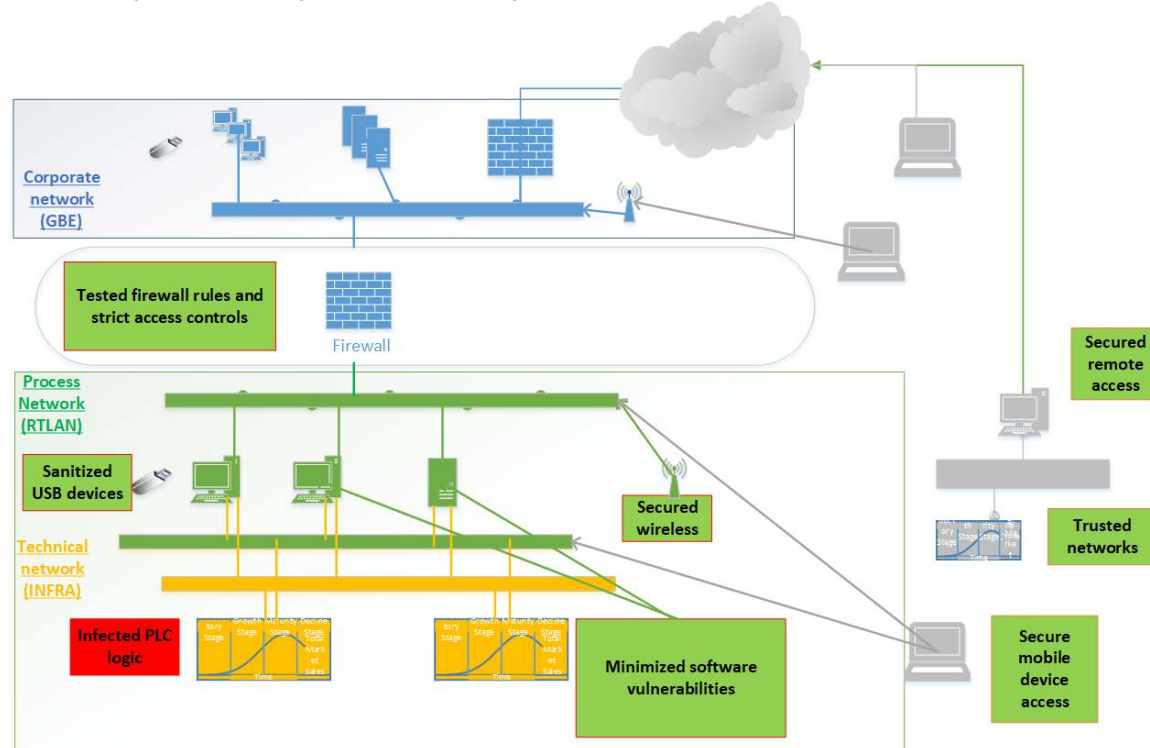
- 6. The use of mobile devices and storage units including smartphones
- 8. Insufficient physical security of data rooms, cabinets, etc.
- 9. Vulnerable software





# Start with common recommendations?

1. Lack of cyber security awareness and training among employees
4. A limited cyber security culture among vendors, suppliers and contractors



Beware...

**Beware**  
**of the false sense of security**  
**and**  
**security by obscurity**



# Findings the vulnerabilities

- ✓ NSA Hacker Chief, Rob Joyce, explanations
  - ✓ Hunting sysadmins
  - ✓ Clear text authentication
  - ✓ Finding an opening, no matter how small
  - ✓ Temporary open access

***«You know the technologies you intended to use,***

***we know the technologies that are actually in use...»***



# Critical points of focus

- ✓ Identify the most critical systems
- ✓ Restrict all remote access
- ✓ Protect critical devices (physically and logically, zoning)
- ✓ Ensure system recovery
- ✓ Promote security awareness
- ✓ Manage your suppliers security



# Manage all your risks - old and new!

***“Progress just means bad things happen faster”***

*Terry Pratchett (2010). “Witches Abroad: (Discworld Novel 12)”, p.317, Random House*



REMEMBER...

**NO SAFETY WITHOUT SECURITY**

**NO SECURITY WITHOUT SAFETY**



# THANK YOU

[www.gminternational.com](http://www.gminternational.com)



© G.M. International s.r.l.

Data specified in this document are merely descriptive of the products and should be integrated with relevant technical specifications. Our products are constantly being further developed and the information presented herein refers to the latest product release. No statements concerning a certain condition or suitability for a certain application can be derived from our information. The information given does not release the user from the obligation of own judgment and verification. Terms & Conditions can be found at [www.gminternational.com](http://www.gminternational.com)