

YOKOGAWA ◆
Co-innovating tomorrow™

Plant & Process Safety = Safety + Security

Mark Hellinghuizer & Ton Beems
 Cyber Security Specialist Functional Safety Specialist
 December 14th 2023

| EPSC Safety Congress | December 14, 2023 |
© Yokogawa Electric Corporation

2


<p>Ton Beems 29 years Functional Safety expert</p>  <ul style="list-style-type: none"> ■ FS Engineer Trainer (TÜV Rheinland, SIS) ■ Maintenance + support of Functional Safety Management systems ■ Safety assessments and (site) validations ■ FSM Auditor ■ Safety promotion (lectures) 	<p>Mark Hellinghuizer 27 years Security & OT expert</p>  <ul style="list-style-type: none"> ■ Involved in planning and design of many OT facilities ■ DCS/Safety System/Field Instruments ■ Consultant for our customers ■ Part of the Global Security Organization
---	---

YOKOGAWA ◆ Co-innovating tomorrow™ | Document Number 12345 | Month DD, YYYY |
© Yokogawa Corporation of America

3

What will come in this presentation:

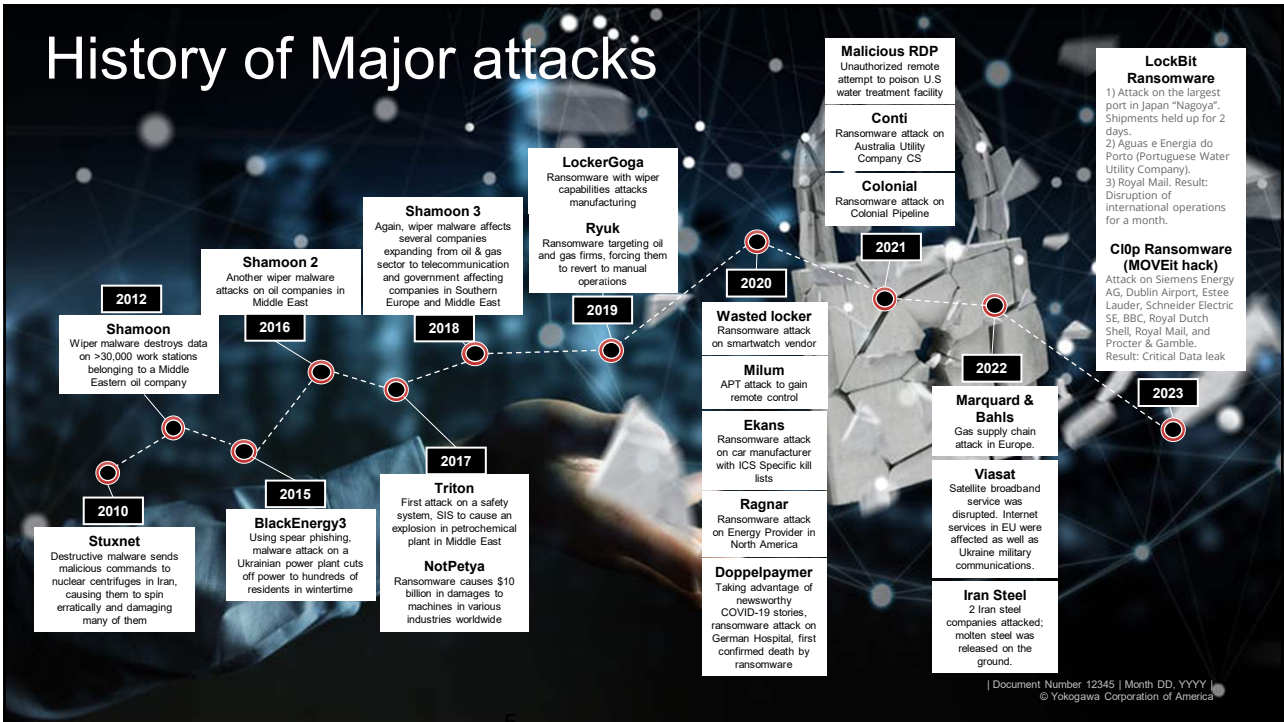
1. You cannot have safety if you do not have security
2. A flaw in security will jeopardize your safety
3. Risk assessments needed for both safety AND security
4. How can you address the security risk assessment when you do the safety risk assessment (different competency)



OKOGAWA Co-innovating tomorrow™
| EPSC Safety Congress | December 14, 2023 | © Yokogawa Electric Corporation 4

4

History of Major attacks



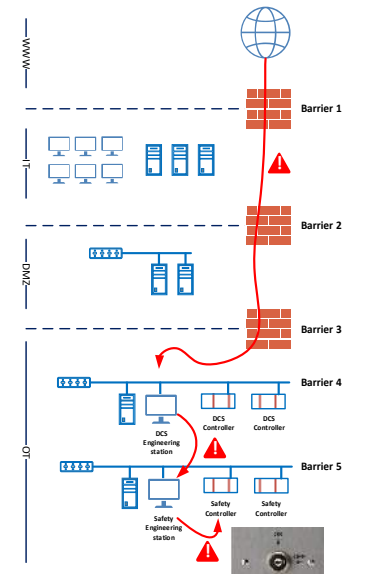
Year	Attack Name	Description
2010	Stuxnet	Destructive malware sends malicious commands to nuclear centrifuges in Iran, causing them to spin erratically and damaging many of them
2012	Shamoon	Wiper malware destroys data on >30,000 work stations belonging to a Middle Eastern oil company
2015	BlackEnergy3	Using spear phishing, malware attack on a Ukrainian power plant cuts off power to hundreds of residents in wintertime
2016	Shamoon 2	Another wiper malware attacks on oil companies in Middle East
2017	Triton	First attack on a safety system, SIS to cause an explosion in petrochemical plant in Middle East
2017	NotPetya	Ransomware causes \$10 billion in damages to machines in various industries worldwide
2018	Shamoon 3	Again, wiper malware affects several companies expanding from oil & gas sector to telecommunication and government affecting companies in Southern Europe and Middle East
2019	Ryuk	Ransomware targeting oil and gas firms, forcing them to revert to manual operations
2019	LockerGoga	Ransomware with wiper capabilities attacks manufacturing
2020	Wasted locker	Ransomware attack on smartwatch vendor
2020	Milum	APT attack to gain remote control
2020	Ekans	Ransomware attack on car manufacturer with ICS Specific kill lists
2020	Ragnar	Ransomware attack on Energy Provider in North America
2020	Doppelpaymer	Taking advantage of newsworthy COVID-19 stories, ransomware attack on German Hospital, first confirmed death by ransomware
2021	Malicious RDP	Unauthorized remote attempt to poison U.S water treatment facility
2021	Conti	Ransomware attack on Australia Utility Company CS
2021	Colonial	Ransomware attack on Colonial Pipeline
2021	LockBit Ransomware	1) Attack on the largest port in Japan "Nagoya". Shipments held up for 2 days. 2) Aguas e Energia do Porto (Portuguese Water Utility Company). 3) Royal Mail. Result: Disruption of international operations for a month.
2021	CI0p Ransomware (MOVEit hack)	Attack on Siemens Energy A.G. Dublin Airport, Estee Lauder, Schneider Electric SE, BBC, Royal Dutch Shell, Royal Mail, and Procter & Gamble. Result: Critical data leak
2022	Marquard & Bahls	Gas supply chain attack in Europe.
2022	Viasat	Satellite broadband service was disrupted. Internet services in EU were affected as well as Ukraine military communications.
2023	Iran Steel	2 Iran steel companies attacked; molten steel was released on the ground.

| Document Number 12345 | Month DD, YYYY | © Yokogawa Corporation of America

5

Example – TRISIS/TRITON Malware

- TRISIS/TRITON is malware that injects malicious code into the programmable memory of a specific Safety System
- Incident occurs in August 2017 at unnamed company in the Middle East resulting in unplanned shutdown
- Hacker had access via the Remote Desktop Protocol
- Via the DCS Engineering Station the hacker had access to the Safety Engineering Station
- Next the hacker had access to the safety controller because the safety key was in program mode
- Luckily some bug in the virus was present (triggered a fail safe shutdown, which triggered the investigation)



6

Regulation - NIS directive



The NIS Directive is the first piece of EU-wide legislation on cyber security

- NIS was adopted by the European Parliament on July 2016 and Member States have to transpose the Directive into their national laws by May 2018 and identify operators of essential services by November 2018.
- Most countries have started the process of preparing a cybersecurity strategy.
- The NIS Directive highlights two primary obligations to ensure the continuity of essential services:
 - ◆ To take appropriate technical and organizational measures to manage threats to networks and information systems
 - ◆ To notify 'without undue delay' the authorities about any significant security incident

7

Practical translation

- **There is no official translation**
On purpose
- **Practical translation**
- **How to prove to government inspector**
- **Show in your Policies you follow an international standard**
Like IEC-62443
- **Show proof that you comply to this policy**
By risk assessment or gap assessment



8

Why is Security important for Safety?

- A Hacker might want to**
- Gain money
 - Do physical damage
 - Economical damage
- **If the safety system is not well secured it might be hacked**
It is possible to setup good security

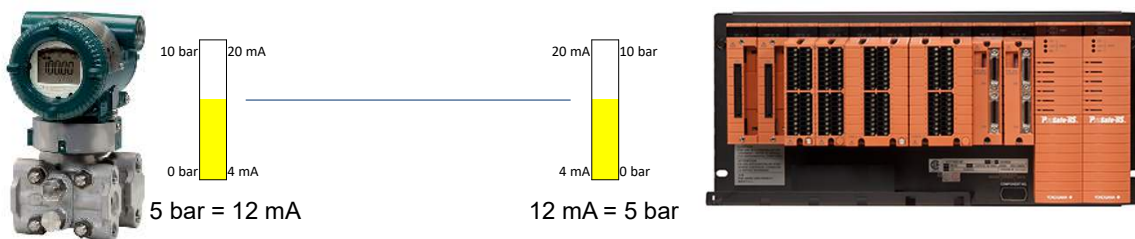


9

Theoretical Hack example

Transmitters and Safety system communicate using mA

- Milli Amperes
- Range is between 4mA and 20 mA, upper or lower mA will be detected/actioned
- Both transmitter and safety PLC need to program the ranges (e.g. 0 – 10 bar)



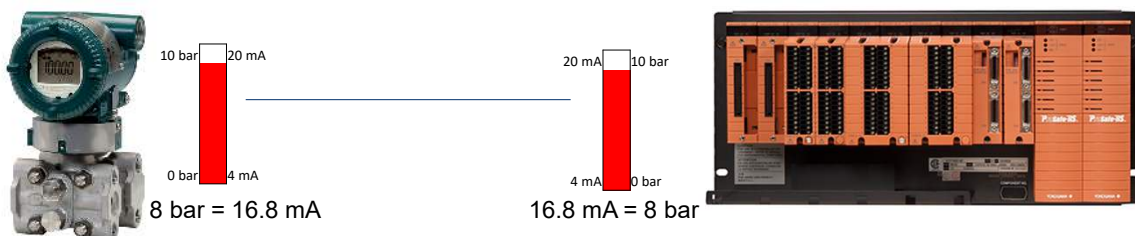
10

Theoretical Hack example

Trip setpoint is at 8 bar, when this is reached a shutdown is required

Pressure is increasing

- 8 bar is reached
- SCS takes action and shuts down the plant



11

But what if...



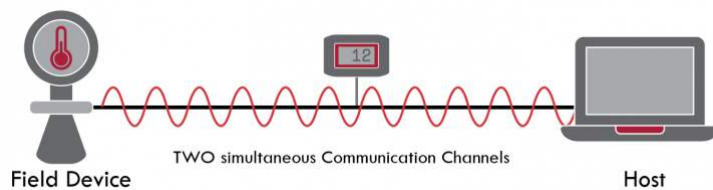
...there is bad intend?

12

12

Hart

Modern system are equipped with HART



- In this case the host is an Asset Management system
- Asset Management system is a Server with Microsoft O.S.
- This can be attacked and the attacker can remotely change the range of the transmitter

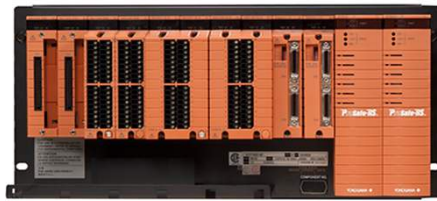
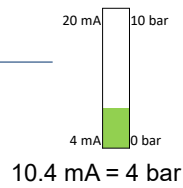
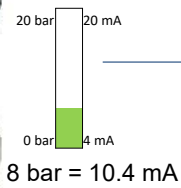
13

Range is changed

Transmitter Range changed to 0-20 bar

Pressure is increasing

- 8 bar is reached
- Safety System thinks it is only 4 bar,
- Trip setpoint will never be reached...



14

Consideration

Theoretical from safety point of view

- The safety system worked correctly
- We should be able to trust the information coming to us

Result is an Incident on the plant

- Explosion, Rupture, Personal and Environmental damage

Conclusion:

**A Safety system cannot do without
Security protection**

15

Security and Safety

16

Compliance - Safety

IEC 61511

- Quote:” 8.2.4 a security risk assessment shall be carried **out to identify the security vulnerabilities of the SIS”**
- This assessment should be performed during all stages of the project

'Shall' means mandatory, not having this means: not compliant Non-compliance will result in

- Insurance issues in case of an incident
- European Laws (Seveso) prescribes this must be done
- Your incident (name of the plant) may appear on Tiktok, Youtube etc.



17

Security is now more embedded in the IEC61511 Ed.2 (2016)

8.2.4 A security risk assessment shall be carried out to identify the security vulnerabilities of the SIS. It shall result in:

- a description of the devices covered by this risk assessment (e.g., SIS, BPCS or any other device connected to the SIS);
- a description of identified threats that could exploit vulnerabilities and result in security events (including intentional attacks on the hardware, application programs and related software, as well as unintended events resulting from human error);
- a description of the potential consequences resulting from the security events and the likelihood of these events occurring;
- consideration of various phases such as design, implementation, commissioning, operation, and maintenance;
- the determination of requirements for additional risk reduction;
- a description of, or references to information on, the measures taken to reduce or remove the threats.

11.2.12 The the identified

11.7.3.2 The m access security

11.7.3.4 E mode c

11.8.6 Forc program(s).

Forcing o supplier off an

part of application

YOKOGAWA ◆ Co-innovating tomorrow™

18

| EPSC Safety Congress | December 14, 2023 |
© Yokogawa Electric Corporation

18

18

Risk is not a matter of “IF”, it is a matter of “WHEN” ...

Risk is first discussed during HAZARD and RISK assessment

Safety Lifecycle IEC61511

1 Hazard and risk assessment

↓

2 Allocation of safety functions

- Facilitator (chairman/secretary)
- Process Eng.
- Instrumentation Eng.
- Operations/Maintenance Eng.
- Safety Eng.
- Rotating Equipment Eng.
- Other specialists

But are security risks also discussed during the HAZOP?

YOKOGAWA ◆ Co-innovating tomorrow™

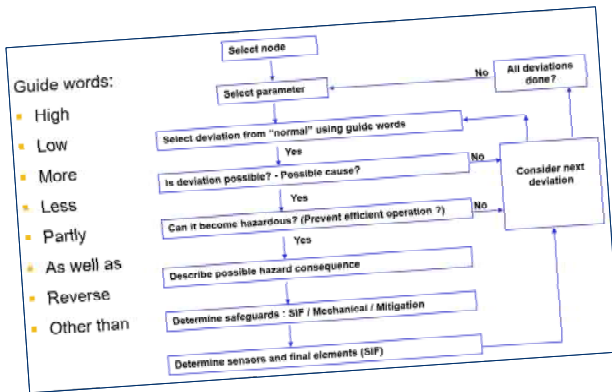
19

| EPSC Safety Congress | December 14, 2023 |
© Yokogawa Electric Corporation

19

How to HAZOP security risks?

- Can these be discussed during the 'normal' HAZOP?
- HAZOP participants are most likely not proven competent for security
- What to do during a HAZOP to help the security risk assessment:



Guide words:

- High
- Low
- More
- Less
- Partly
- As well as
- Reverse
- Other than

✓ If your list of SIFs is complete.

✓ What is your ultimate important Safety Instrumented Function? One or more?

✓ Do the risk assessment as usual.

20

How to HAZOP security risks (continued)

- Shortlist of most important SIFs (with a SIL level)
- A higher SIL level does not always make the SIF more important
- Once it is known how all plant networks will be connected
- Then, in general, do the Security Risk Assessment



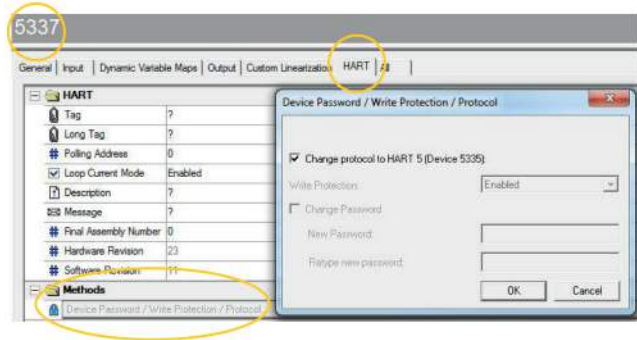
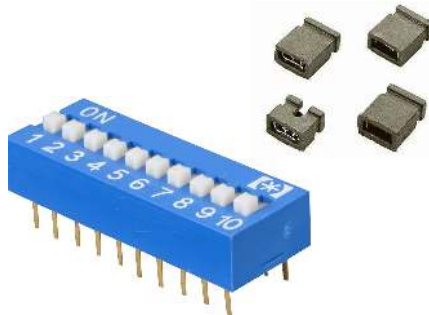
SECURITY CHECK



21

Security risks for Sensors

- Which sensor instruments will be on what network: HART, Fieldbus, Profibus etc.
- Are they hardwired write protected? Or software write protected?



22

Security risks for Final Elements

- Which valves will be on any network?
- Simple valves will be type A and will not be connected to any network.
- When applying Partial Stroke Testing, things can get complicated, if PST is initiated from a PRM network via HART, Fieldbus, Profibus?
- Will it be possible to manipulate the valve remotely?



Courtesy: Mokveld Valves bv

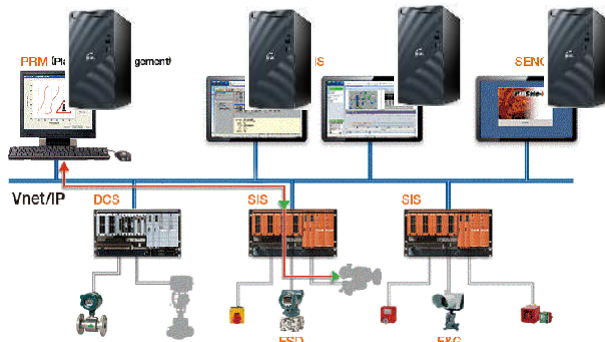


Courtesy: Masoneilan

23

Security risks for Logic Solvers

- Application Program configuration from a PC/Laptop (Windows OS)
- Safety PLC's, how many networks will they eventually be connected to?



24

Security risks for Logic Solvers (continued)

- Hackers to be blocked by means of physical access countermeasures
- Therefore, (key)switches before configuration download can be done
- Who operates this switch?



What if you forget to switch back to "write protected" directly after the download?

What if this will last for a weekend or holiday?



25

What is Risk management?

“The process of identifying the risks to system security and determining the probability of occurrence, the resulting impact, and additional safeguards that would mitigate this impact.”

26

Workflow Process

KOM, Workshop to VA, Workshop to RA, Reporting (led by consultant)
 Site inspection, Network scan (led by local engineer)

TIME FRAME	
Week 1	Week 2
Preparation phase Kickoff meeting → Internal preparation	Vulnerability assessment phase Assessment questionnaire (Consultant) Technical inspection (Engineer) Passive network scanning (Engineer) → Vulnerability database
	Risk assessment phase Vulnerability database → Pre defined threat scenarios Assess consequence Assess Likelihood → Risk matrix
	Reporting and close-out phase Reporting → Close-out Meeting Security vulnerability and risk assessment report
RESOURCES	
Consultant and Engineer	
Consultant	

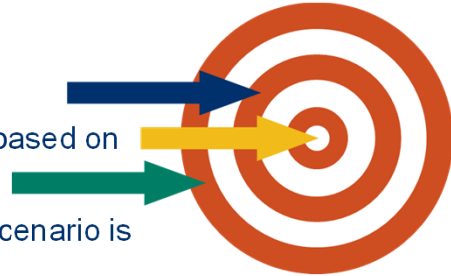
YOKOGAWA ◆ Co-innovating tomorrow™

EPSC Safety Congress | December 14, 2023 | © Yokogawa Electric Corporation 27

27

Risk Assessment

- Assessment based on scenarios
- Risk = Likelihood * Impact
- Yokogawa consultant selects the likelihood based on identified vulnerabilities.
- Yokogawa explains what will happen if the scenario is executed.
- Customer to judge what the impact is.



28

Scenario example

Intended manipulation of SIS Logics by Remote Hack

- Hacker can remotely manipulate the logic with the intention of creating a disaster

Vulnerabilities contributing to increasing likelihood

- No write protect key switch
- No antivirus on engineering station
- No whitelisting on engineering station
- Missing access control on engineering station
- Firewall rules missing or wrong

If the hacker is successful, the safety control will no longer functions correctly

Only mechanical safety barriers can be relied upon (relief valves, etc.)

Customer to judge what is the impact.

29

Risk Matrix

					Likelihood						
					Chance	Chance	Virtually improbable and unrealistic	Conceivably possible, but very unlikely to occur	Unusual but possible	Quite possible or not unusual	Event expected to occur more than once per year
					Frequency	Frequency	Event could occur at some time greater than 100 years	Event could occur at some time within 10 to 100 years	Has occurred or is expected to occur within 5 to 10 years	Has occurred or is expected to occur within 1 to 5 years	Event expected to occur more than once per year
							Improbable	Rare	Unlikely	Possible	Likely
							1	2	3	4	5
Impact	Safety	Environment	Financial	Reputation	Trivial	1	1	2	3	4	5
	Medical Treatment, Minor Health Effects, First Aid Case, or Less	No off site impact	Potential equipment or asset damage or financial loss < \$100K USD	No harm or slight client concern	Minor	2	2	4	6	8	10
	Medical Treatment with Restricted Duty or Medium Health Effects	One odor or noise complaint from event	Potential equipment or asset damage or financial loss \$100K to \$ 1M	Minor harm to the Company's public reputation, or client concern	Moderate	3	3	6	9	12	15
	Serious illness or injury resulting in days away from work (LTI), or a permanent partial Disability	On-site or off-site environmental release to soil/ground or multiple odor or noise complaints from event	Potential equipment or asset damage or financial loss \$1M to \$10M	Harm to the Company's reputation limited to the local area via local public media reports or local industry news; significant client concern	Major	4	4	8	12	16	20
	Illness or injury resulting in one fatality, or permanent full disability	On-site or off-site environmental release to surface water	Potential equipment or asset damage or financial loss \$10M to \$100M	Harm to the Company's reputation extends to the region through regional or national public media outlets or national industry or financial news; multiple significant client concerns	Critical	5	5	10	15	20	25
Illness or injury resulting in multiple (2+) fatalities	Major off-site impact (vapor cloud explosion, fire, major toxic gas release, major off-site environmental release, wildlife kill)	Potential equipment or asset damage or financial loss >\$100M	Harm to the Company's reputation extends internationally through public media outlets or negative publicity in international industry or financial news; global client concerns								

YOKOGAWA ◆ Co-innovating tomorrow™ | EPSC Safety Congress | December 14, 2023 | © Yokogawa Electric Corporation 30

30

Key Take Aways

Seveso directive: Analyse and Manage your risks!

Analyse

- HAZOP and Risk Analysis for Process Safety Functions (SIFs with SIL levels)
- Risk Analysis for Cyber Security (Risk report with criticality levels)
- During safety risk assessment, make shortlist of most important SIFs
- Make most important SIFs un-hackable

Manage

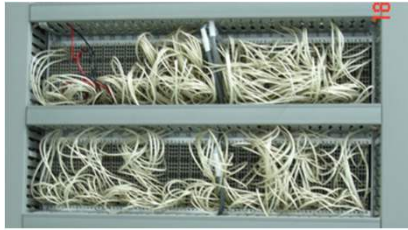
- Functional Safety Management systems
- Cyber Security Management systems

YOKOGAWA ◆ Co-innovating tomorrow™ | EPSC Safety Congress | December 14, 2023 | © Yokogawa Electric Corporation 31

31

Ultimate Cyber Secure Safety Logic Solvers

- You remember your shortlist with most important SIFs, make them hardwired!
- There are hardwired safety logic solvers available, they are not obsolete at all!
- They consist of solid-state elements to process your functional safety logic
- Even with physical access, any change will lead to a (partial) shutdown



Very fast, very reliable,
completely insensitive for
hackers, viruses, malware etc.

Co-innovating tomorrow™

Free downloads:

Yokogawa.com/nl/**safety**
Yokogawa.com/nl/**securitysan**
Yokogawa.com/nl/**securityebook**