Cyber attacks on Process Plants

C de Salis

A safe world

DEKRA

About the presenter

Clive de Salis has been a member of the IEC committee from the beginning that writes the standards for Cyber (IEC62443) **and those for safety instrumented systems** (IEC61511, IEC61508 etc)**.**

- *Vice Chair of I.Chem.E Safety & Loss Prevention*
- *I.Chem.E Registered Safety Professional in 2006*
- *I.Chem.E Professional Process Safety Engineer since 2015*
- *I.Chem.E National and International Assessor for Professional Process Safety Engineer since 2015*
- *M.I.Chem.E since 1999 (and graduate member of I.Chem.E since 1980)*
- *M.Inst.M.C since 2007 (and Inst.M.C. London branch “Engineer of the Year” 2013)*
- *Expert witness to the Courts in both England & Wales and in Scotland since 2005*
- *1st Chair of the 61508 Association*

Misunderstandings and Where to start

Two projects fully done, one full project in progress.

Many smaller projects for specific processes

- Talking about misunderstandings encountered

- Talking about where to start

- **Understanding Cyber-hackers**

A Corporate response

Cyber attack risks are a very complex subject …..

Like most things …
you START by doing!

You cannot just be a headless chicken!

Which standard do I use?

- Confused by the standards

There are too many different Cyber standards! ….

I won't decide and do nothing instead!

Are you doing **PROCESS PLANT PROTECTION** or are you doing **OFFICE COMPUTER PROTECTIONS** ?

Here's the simple version ….

PROCESS PLANT PROTECTION – use the **IEC 62443** group of standards

OFFICE COMPUTER PROTECTION – use the **ISO 27001** group of standards

You can actually use both!

The available standards

None of the standards are mature yet and it is actually early days for all of them

There are two main groups of standards for cyber security and the government requirements

- ISO 27000 set of standards
- IEC 62443 set of standards
- Government requirements

In the UK the SRAM (what needs to be stated in a COMAH report) states OG0086 needs to be shown.

These actually overlap – *The clever thing is to limit what you apply and still cover everything that matters.*

Cyber Security – An effective approach

There are a number of standards and guidance documents all trying to achieve the same end.

The two main standards are the ISO standards and the IEC standards.

IEC62443 is now the European Norm

For EN62443

We have written a huge amount of words on how to protect your computer systems …. BUT … not very much on what is ***equally*** important

– how to use independence from Cyber attack

…..BUT….

…..from the perspective of publicity people have been bombarded with the problem of protecting computers, an I.T. network and data highway.

- Confused by misleading publicity

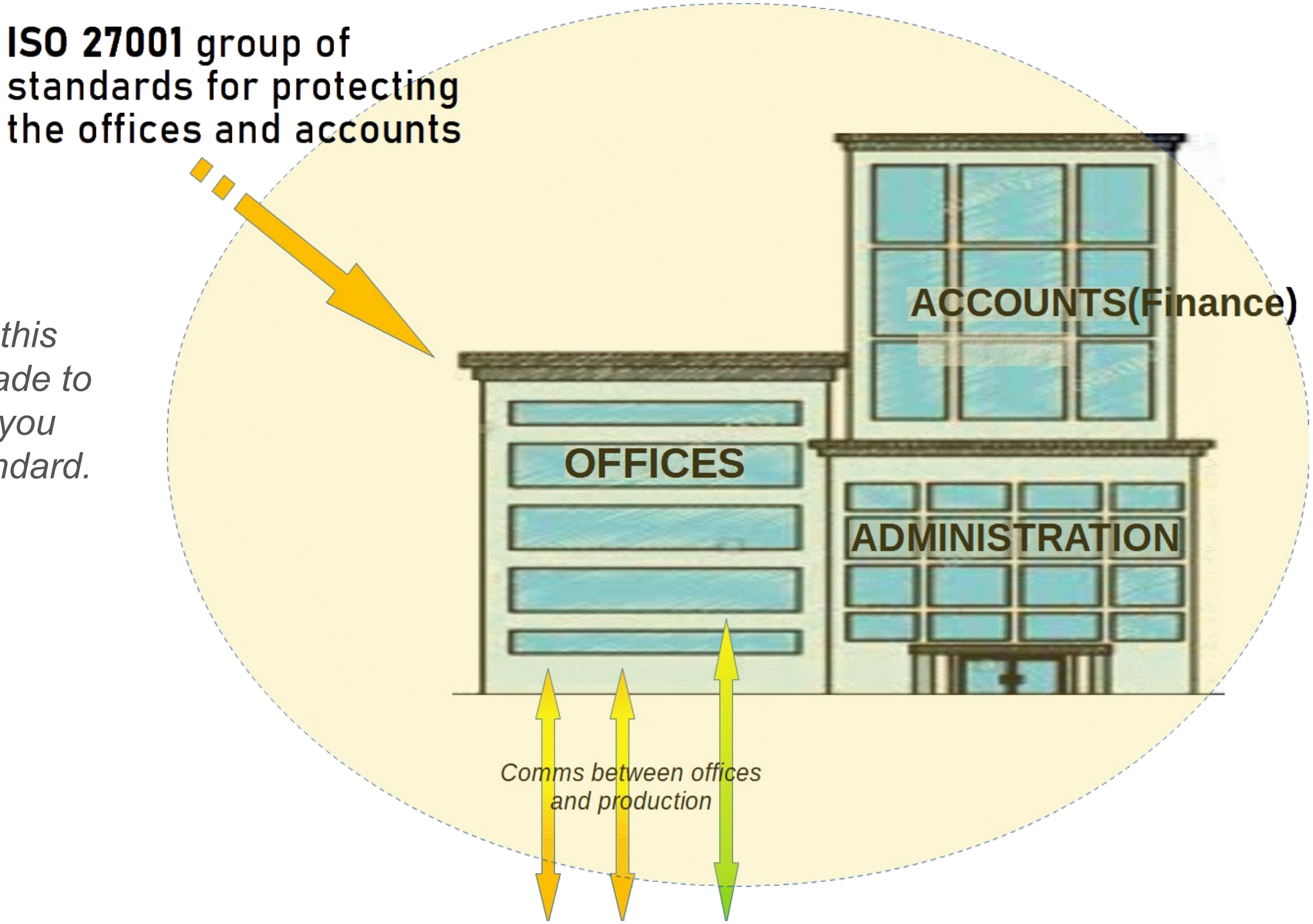
The truth is that the number of words in a standard is ***NOT*** proportional to how important the statement is.

We need **BOTH** barriers that are genuinely INDEPENDENT **and** barriers to protect the data highway.

We can make INDEPENDENT barriers robust.
For the data highway and computer barriers we can put protection in place as well.

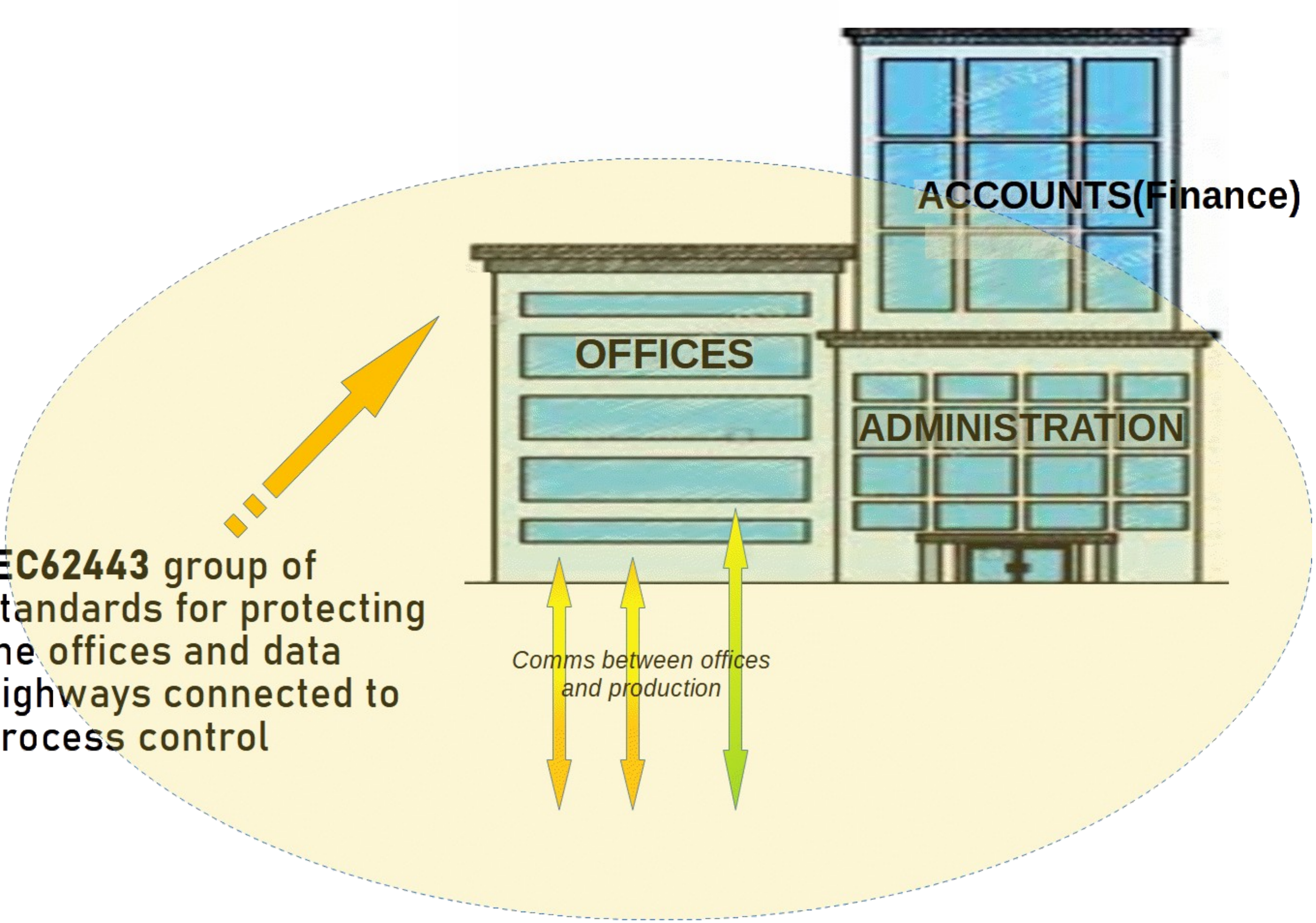
The ISO 27000 group of standards

There are sections within this ISO 27000 that can be made to cover more than this, but you risk going outside the standard.


ISO 27001 group of standards for protecting the offices and accounts
ACCOUNTS(Finance)
OFFICES
ADMINISTRATION
Comms between offices and production

Some company's corporate standards use the ISO 27000 series so they protect the accounts, the offices and the data highways going out to the process plant *but do not properly protect the process plant itself !*

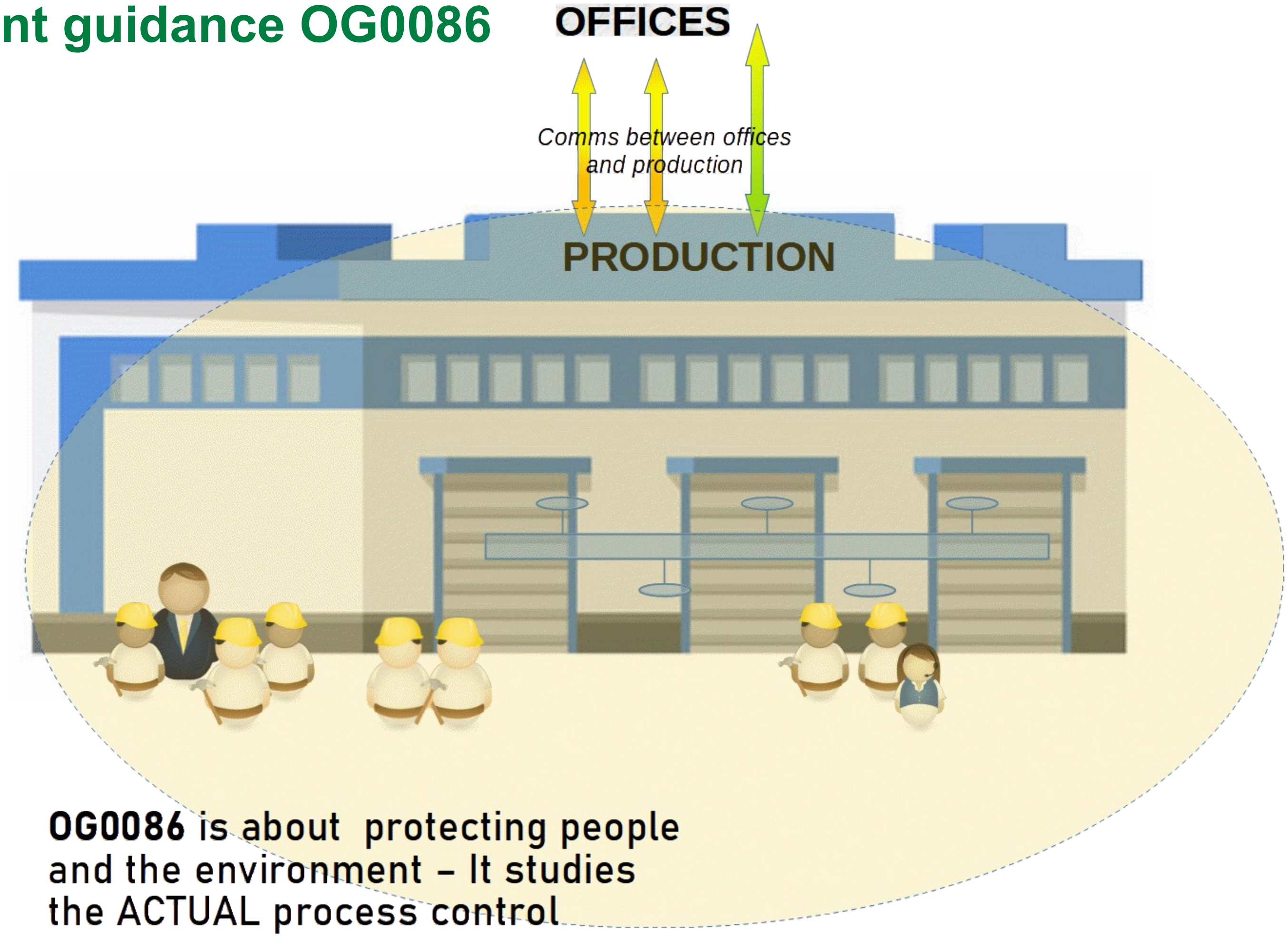
The IEC 62443 group of standards



IEC62443 group of standards for protecting the offices and data highways connected to process control

There are similarly sections within this IEC 62443 group that can be made to cover more than this, but you again risk going outside the standard.

The Government guidance OG0086

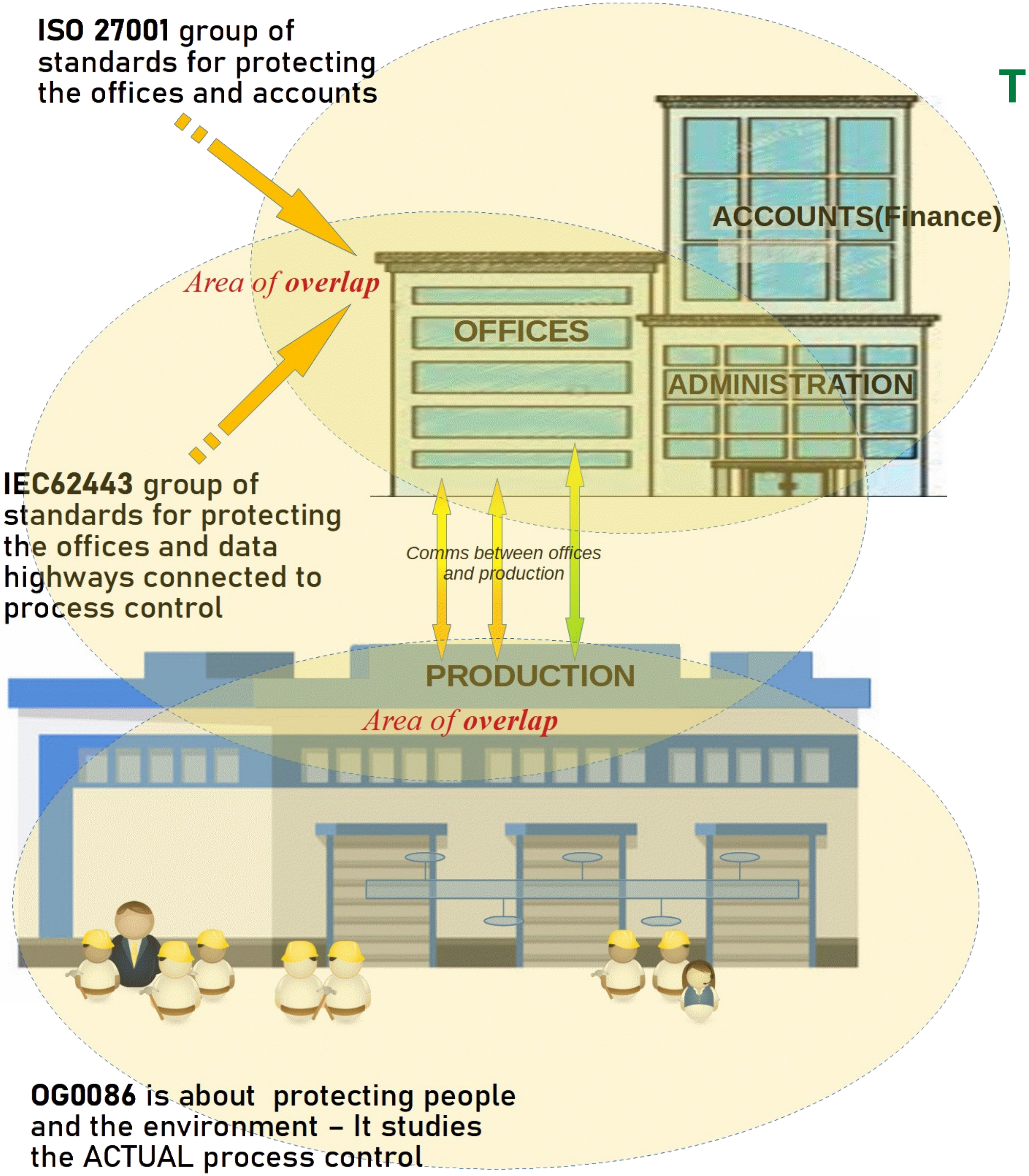


OG0086 is about protecting people and the environment – It studies the ACTUAL process control

Not surprisingly, the government document is about protecting people and the environment.

….and yet there are overlaps between all of these standards as shown below:

These standards overlap in parts



ISO 27001 group of standards for protecting the offices and accounts

IEC62443 group of standards for protecting the offices and data highways connected to process control

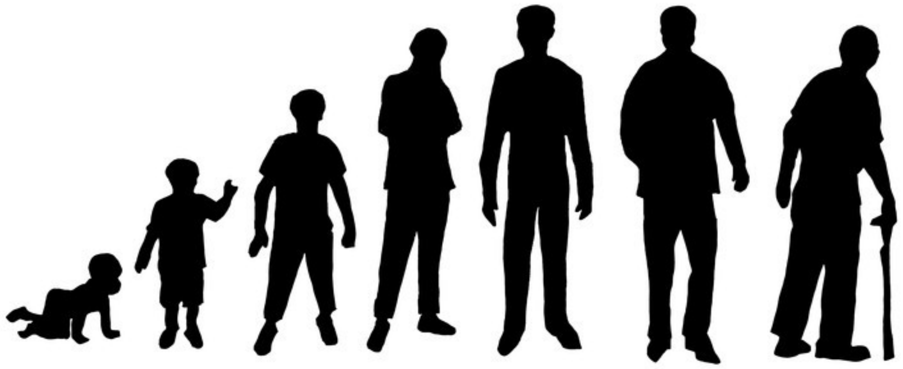
OG0086 is about protecting people and the environment – It studies the ACTUAL process control

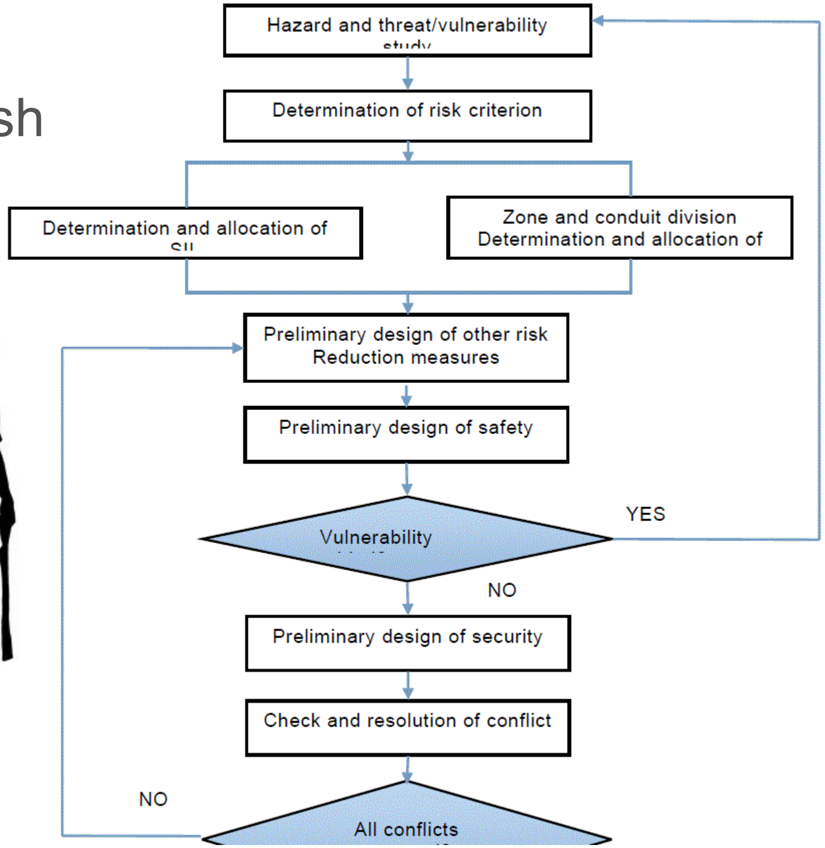
Yet it is a waste of time and money trying to do them all

The lifecycle

Start at the beginning of the lifecycle

A lifecycle concept is from start to finish





Hazard and threat/vulnerability study

Determination of risk criterion

Determination and allocation of SIL

Zone and conduit division
Determination and allocation of

Preliminary design of other risk
Reduction measures

Preliminary design of safety

Vulnerability

YES

NO

Preliminary design of security

Check and resolution of conflict

NO

All conflicts

***IEC63325** is to be published shortly and is the lifecycle for the **IEC62443** Cyber standards for process plants*

Where to start….

We'll come to the question of "hierarchy" shortly …..

1. Identify MAH caused by Cyber

   MAH = MAJOR accident hazards

2. Identify the barriers and safeguards that prevent the MAH

   Barriers = ISO17776 and COMAH language

   Safeguards = HAZOP and IEC61882 language

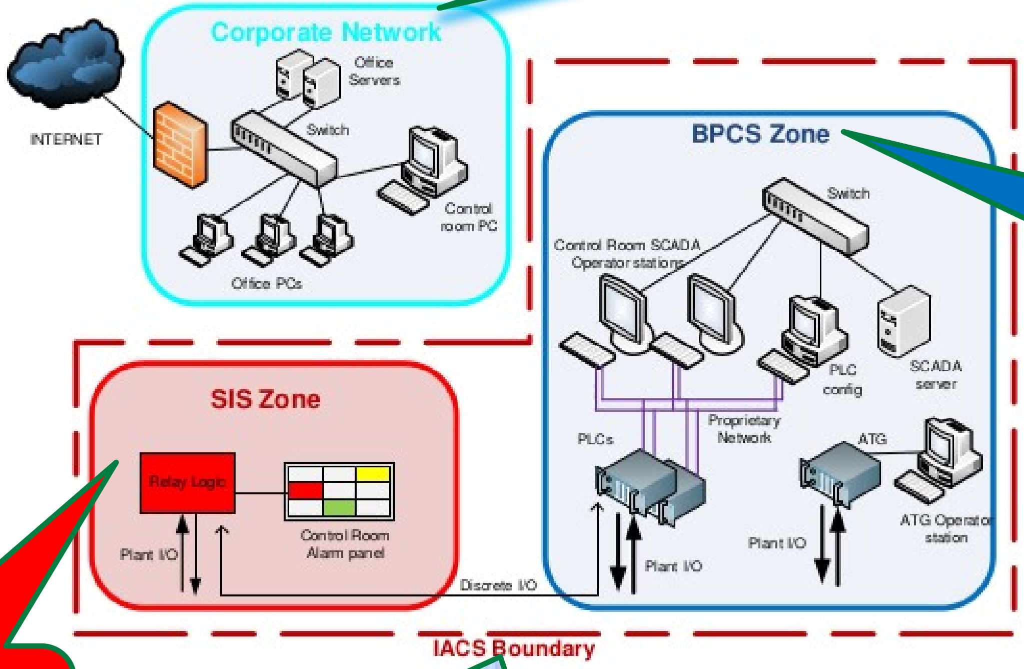
3. Collate the barriers and safeguards together into Zones to understand them holistically

   "Zones" are NOT the barriers and safeguards

OG0086 requires a diagram of the control network for the Cyber assessment

The HSE example includes:

Figure 2-1 Small Site



- Office computers and network

- Basic Process Control System (PLCs, DCS controllers etc)

- Safety Instrumented Systems

Industrial Automated Control system – **The TOTAL plant control system**

This diagram is from the 1st edition

Identify MAH caused by Cyber

You CANNOT do just a HAZOP

….that isn’t right at all

Cyber attacks I/O
…but can attack multiple I/O.

Cyber causes MAH
…we protect against the MAH and NOT just the Cyber attack

Identify barriers and safeguards

Your risk assessment does want to list all the barriers and safeguards that prevent the MAH

….INCLUDE the barriers and safeguards you already have and label them CYBER CRITICAL

…INCLUDE existing Cyber protections like firewalls and improve them

…significantly!

Identify barriers and safeguards that prevent the MAH and keep us safe

If the barriers and safeguards have a COMMON basis, then any cyber hacker that attacks that common basis can get through every barrier and safeguard that you have.

It is NOT the quantity of barriers and safeguards that matter ….

What matters is that all the barriers and safeguards are <u>different</u>, and that some barriers are genuinely independent of the computer systems.

DIVERSITY

You CANNOT do just a HAZOP

….that isn't right at all

….the number of words in a standard is NOT proportional to how important the statement is.

OG0086 states:

No single security countermeasure provides absolute protection as new threats and vulnerabilities can be identified at any time. To reduce these risks, implementing multiple protection measures in series, i.e. defence in depth, avoids single point failures.

OG0086 has a section requiring DIVERSITY of barriers and safeguards

OG0086 also states:

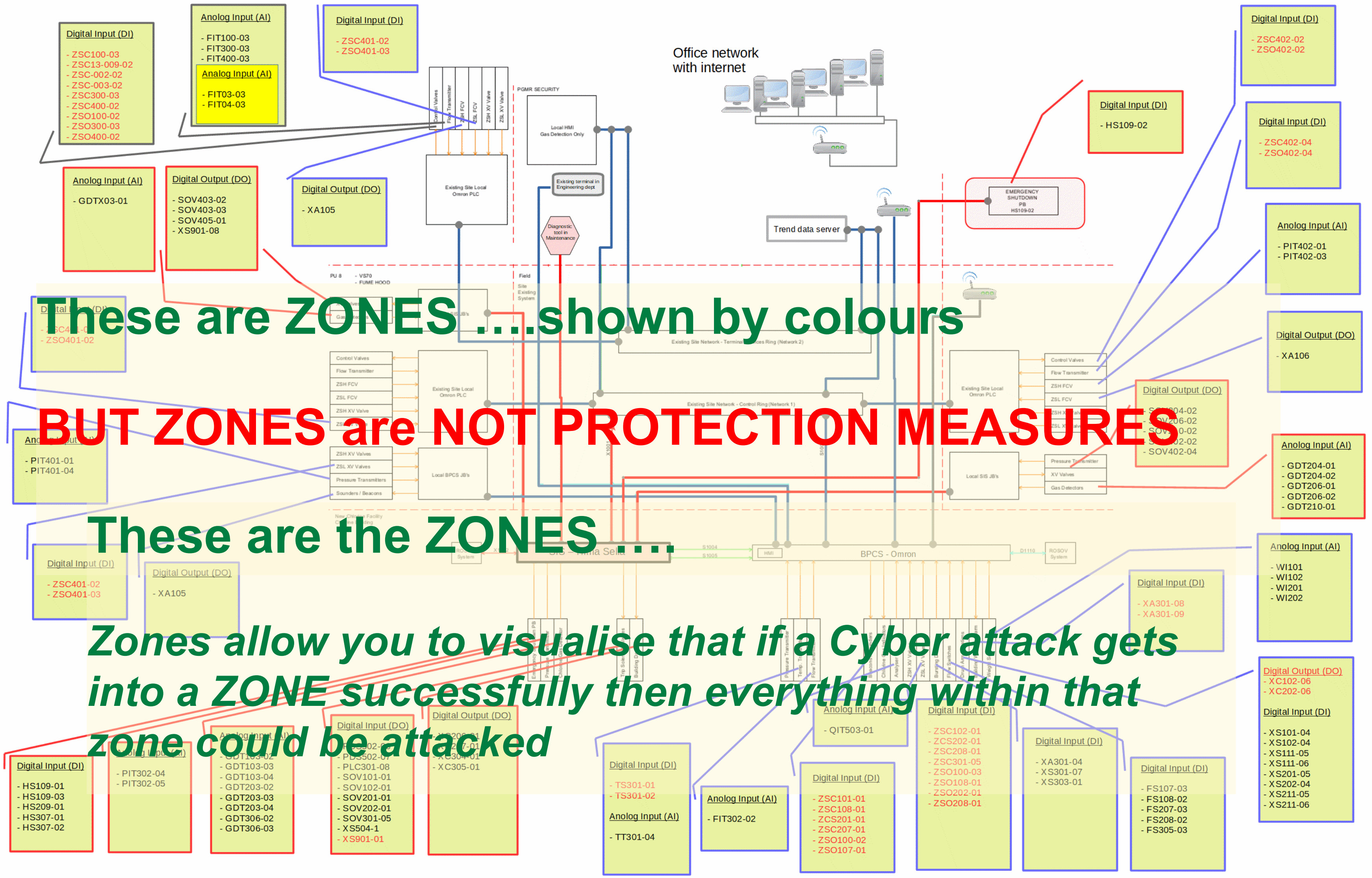
As the SIS normally contains significant risk reduction control measures, it is usually appropriate to apply stronger controls to the SIS than the rest of the IACS.

CYBER CRITICAL **SIL rating** of INDEPENDENT barriers and safeguards is also needed

…. We need BOTH barriers that are genuinely INDEPENDENT and barriers to protect the data highway

For OG0086 transform the diagram into this:

This diagram matches the requirements from OG0086



These are ZONES ….shown by colours

BUT ZONES are NOT PROTECTION MEASURES

These are the ZONES …

Zones allow you to visualise that if a Cyber attack gets into a ZONE successfully then everything within that zone could be attacked

Digital Input (DI)
- ZSC100-03
- ZSC13-009-02
- ZSC-002-02
- ZSC-003-02
- ZSC300-03
- ZSC400-02
- ZSO100-02
- ZSO300-03
- ZSO400-02

Anolog Input (AI)
- FIT100-03
- FIT300-03
- FIT400-03

Analog Input (AI)
- FIT03-03
- FIT04-03

Digital Input (DI)
- ZSC401-02
- ZSO401-03

Anolog Input (AI)
- GDTX03-01

Digital Output (DO)
- SOV403-02
- SOV403-03
- SOV405-01
- XS901-08

Digital Output (DO)
- XA105

Digital Input (DI)
- HS109-02

Digital Input (DI)
- ZSC402-02
- ZSO402-02

Digital Input (DI)
- ZSC402-04
- ZSO402-04

Anolog Input (AI)
- PIT402-01
- PIT402-03

Digital Output (DO)
- XA106

Digital Output (DO)
- SOV204-02
- SOV206-02
- SOV210-02
- SOV402-02
- SOV402-04

Anolog Input (AI)
- GDT204-01
- GDT204-02
- GDT206-01
- GDT206-02
- GDT210-01

Digital Input (DI)
- ZSC401-0
- ZSO401-02

Anolog Input (AI)
- PIT401-01
- PIT401-04

Digital Input (DI)
- ZSC401-02
- ZSO401-03

Digital Output (DO)
- XA105

Anolog Input (AI)
- WI101
- WI102
- WI201
- WI202

Digital Input (DI)
- XA301-08
- XA301-09

Digital Output (DO)
- XC102-06
- XC202-06

Digital Input (DI)
- XS101-04
- XS102-04
- XS111-05
- XS111-06
- XS201-05
- XS202-04
- XS211-05
- XS211-06

Digital Input (DI)
- HS109-01
- HS109-03
- HS209-01
- HS307-01
- HS307-02

Anolog Input (AI)
- PIT302-04
- PIT302-05

Anolog Input (AI)
- GDT103-02
- GDT103-03
- GDT103-04
- GDT203-02
- GDT203-03
- GDT203-04
- GDT306-02
- GDT306-03

Digital Input (DO)
- PDS502-06
- PDS502-07
- PLC301-08
- SOV101-01
- SOV102-01
- SOV201-01
- SOV202-01
- SOV301-05
- XS504-1
- XS901-01

Digital Output (DO)
- XC206-01
- XC207-01
- XC304-01
- XC305-01

Digital Input (DI)
- TS301-01
- TS301-02

Anolog Input (AI)
- TT301-04

Anolog Input (AI)
- FIT302-02

Anolog Input (AI)
- QIT503-01

Digital Input (DI)
- ZSC101-01
- ZSC108-01
- ZCS201-01
- ZSC207-01
- ZSO100-02
- ZSO107-01

Digital Input (DI)
- ZSC102-01
- ZCS202-01
- ZSC208-01
- ZSC301-05
- ZSO100-03
- ZSO108-01
- ZSO202-01
- ZSO208-01

Digital Input (DI)
- XA301-04
- XS301-07
- XS303-01

Digital Input (DI)
- FS107-03
- FS108-02
- FS207-03
- FS208-02
- FS305-03

DEKRA Process Safety	Chilworth Technology Ltd Phi House, Southampton Science Park, Southampton SO16 7NS United Kingdom	Drawing / Sketch Title: Sample Control System diagram for Cyber assessment	Client: DEKRA Process Safety Project no. 20190715 Drawing / Sketch no. 20190715-SK1	By: C de Salis Date: 20th April 2020 Peer reviewed: Date:	3		
					2		
					1		
					Rev no.	Date	Revision / Change details

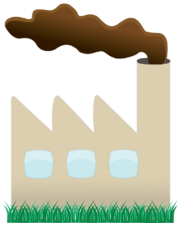
What the DEKRA approach offers

The **DEKRA CyberSafe PS** system provides a systematic process for clearly defining safeguards that require controls (cyber-security) to prevent remote access.

The **DEKRA CyberSafe PS** approach guides clients through protection for:

You choose {

- People
- The environment
- Assets



In the end you must have the right balance between:

INDEPENDENT barriers and

computer and data highway **PROTECTION**

You need to go through protection for:

People and the environment ….not just money

You choose

- People

= essential.

OG0086 states:

Key issues that are specific to cyber security of IACS are: ….. recognising that people are one of, if not the most, significant vulnerability.

- The environment

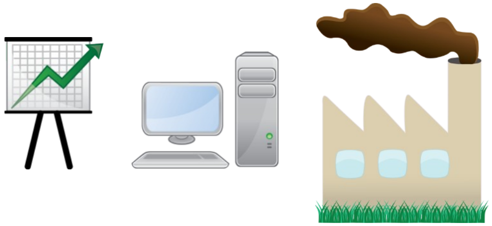
= second essential.

OG0086 also states:

CA / HSE regulated major hazard workplaces where cyber- security could pose a major accident risk to the health and / or safety of employees and / or members of the public and / or environment.

- Assets

= optional.



Cyber SIL assessment

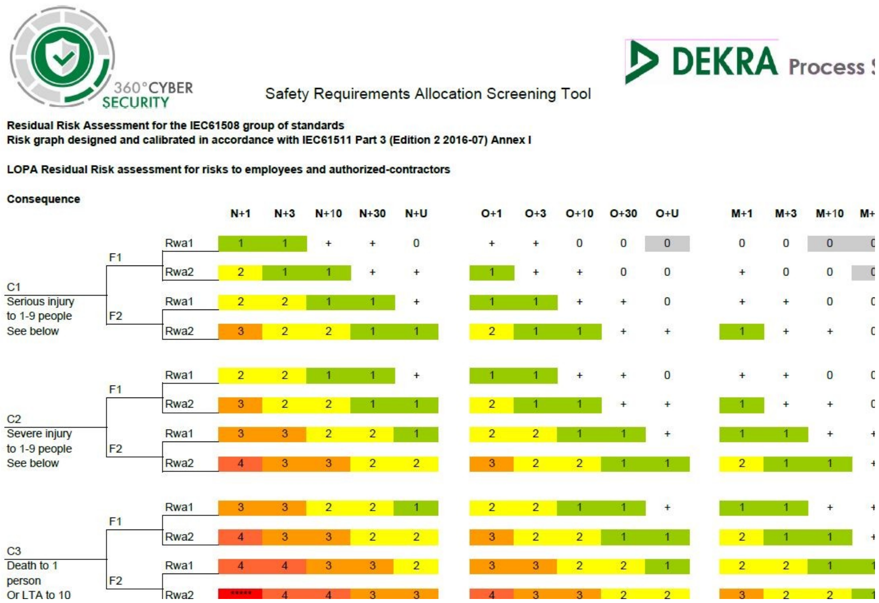
The same report shows Cyber-SIL ratings needed.

Note that the requirement to address cyber security threats for SIS in clause 8.2.4 of **BS EN 61511** (edition 2)

There is NOT enough data to do a quantitative SIL assessment.

You can only do a qualitative SIL assessment.

…be prepared to update it from time to time.



360°CYBER
SECURITY
DEKRA Process S

Safety Requirements Allocation Screening Tool

Residual Risk Assessment for the IEC61508 group of standards
Risk graph designed and calibrated in accordance with IEC61511 Part 3 (Edition 2 2016-07) Annex I

LOPA Residual Risk assessment for risks to employees and authorized-contractors

Consequence			**N+1**	**N+3**	**N+10**	**N+30**	**N+U**	**O+1**	**O+3**	**O+10**	**O+30**	**O+U**	**M+1**	**M+3**	**M+10**	**M+**
C1 Serious injury to 1-9 people See below	F1	Rwa1	1	1	+	+	0	+	+	0	0	0	0	0	0	0
		Rwa2	2	1	1	+	+	1	+	+	0	0	+	0	0	0
	F2	Rwa1	2	2	1	1	+	1	1	+	+	0	+	+	0	0
		Rwa2	3	2	2	1	1	2	1	1	+	+	1	+	+	0
C2 Severe injury to 1-9 people See below	F1	Rwa1	2	2	1	1	+	1	1	+	+	0	+	+	0	0
		Rwa2	3	2	2	1	1	2	1	1	+	+	1	+	+	0
	F2	Rwa1	3	3	2	2	1	2	2	1	1	+	1	1	+	+
		Rwa2	4	3	3	2	2	3	2	2	1	1	2	1	1	+
C3 Death to 1 person Or LTA to 10	F1	Rwa1	3	3	2	2	1	2	2	1	1	+	1	1	+	+
		Rwa2	4	3	3	2	2	3	2	2	1	1	2	1	1	+
	F2	Rwa1	4	4	3	3	2	3	3	2	2	1	2	2	1	1
		Rwa2	*****	4	4	3	3	4	3	3	2	2	3	2	2	1

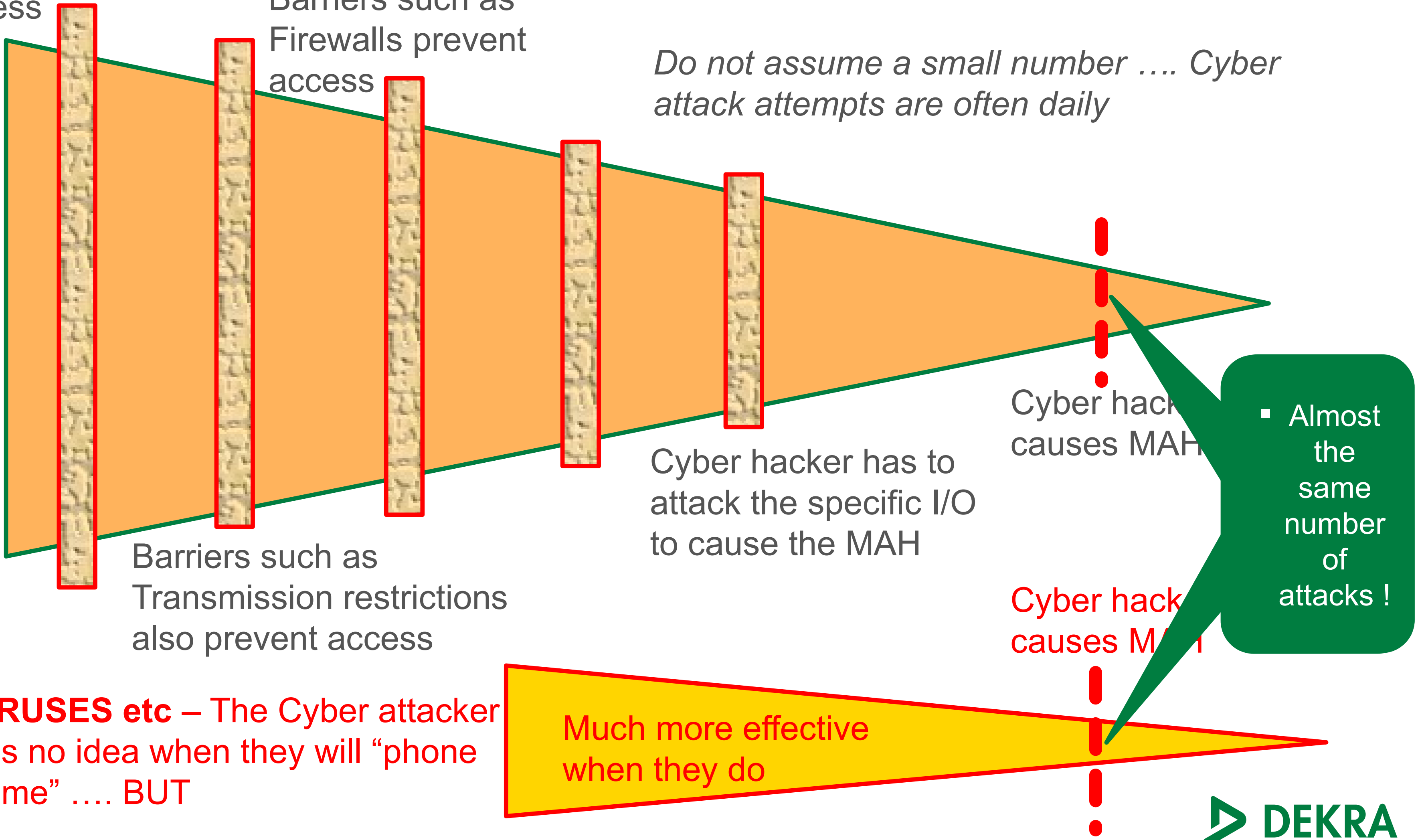
The likelihood is NOT the same as conventional LOPA SIL assessments.

The addition of two SIL rated SIFs to achieve the specified value is also different to conventional SIL rated systems – but is NOT complicated, *just different!*

Likelihood

You get a large number of Cyber attacks attempting to get into your network!

Do not assume a small number …. Cyber attack attempts are often daily



Barriers such as Firewalls prevent access

Barriers such as Firewalls prevent access

Barriers such as Transmission restrictions also prevent access

Cyber hacker has to attack the specific I/O to cause the MAH

Cyber hack
causes MAH

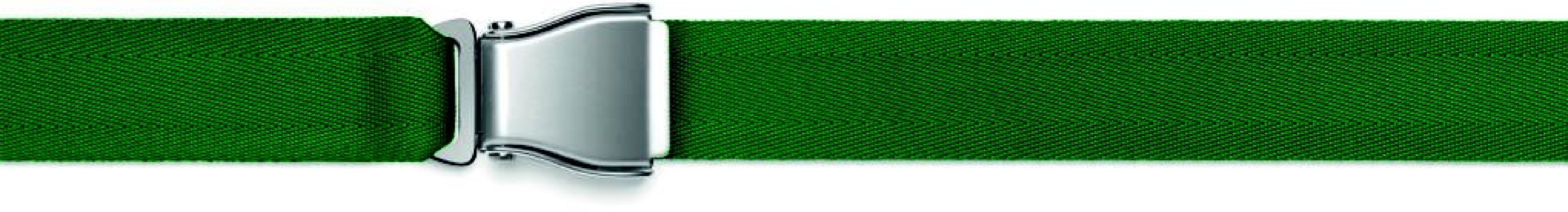
- Almost the same number of attacks !

Cyber hack
causes M

VIRUSES etc – The Cyber attacker has no idea when they will “phone home” …. BUT

Much more effective when they do

Thank **you!**



MISSION

SAFETY

DEKRA

DEKRA process safety