# Secure Software Design: Verification and Testing

## Platform voor InformatieBeveiliging (PvIB)

**Gabriele Webber**

10 November 2016

# Contents

- Who is DNV GL
- Purpose of testing
- Our approach
- Device Health Test
- End-to-end System test
- Questions

# We are a global classification, certification, technical assurance and advisory company

OUR PURPOSE

## TO SAFEGUARD LIFE, PROPERTY AND THE ENVIRONMENT

# Global reach – local competence

**150**
years

**400**
offices

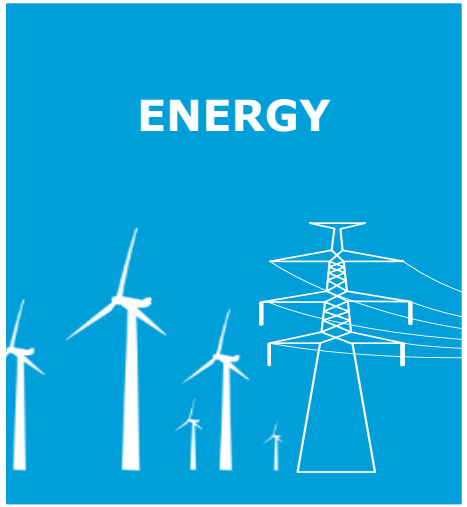
**100**
countries

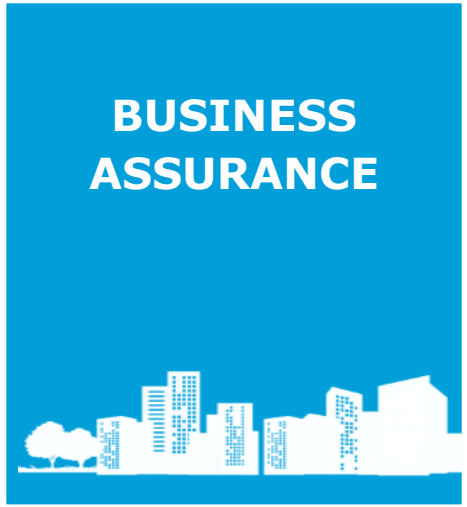
**15,000**
employees

**Ungraded**

# Our vision: global impact for a safe and sustainable future



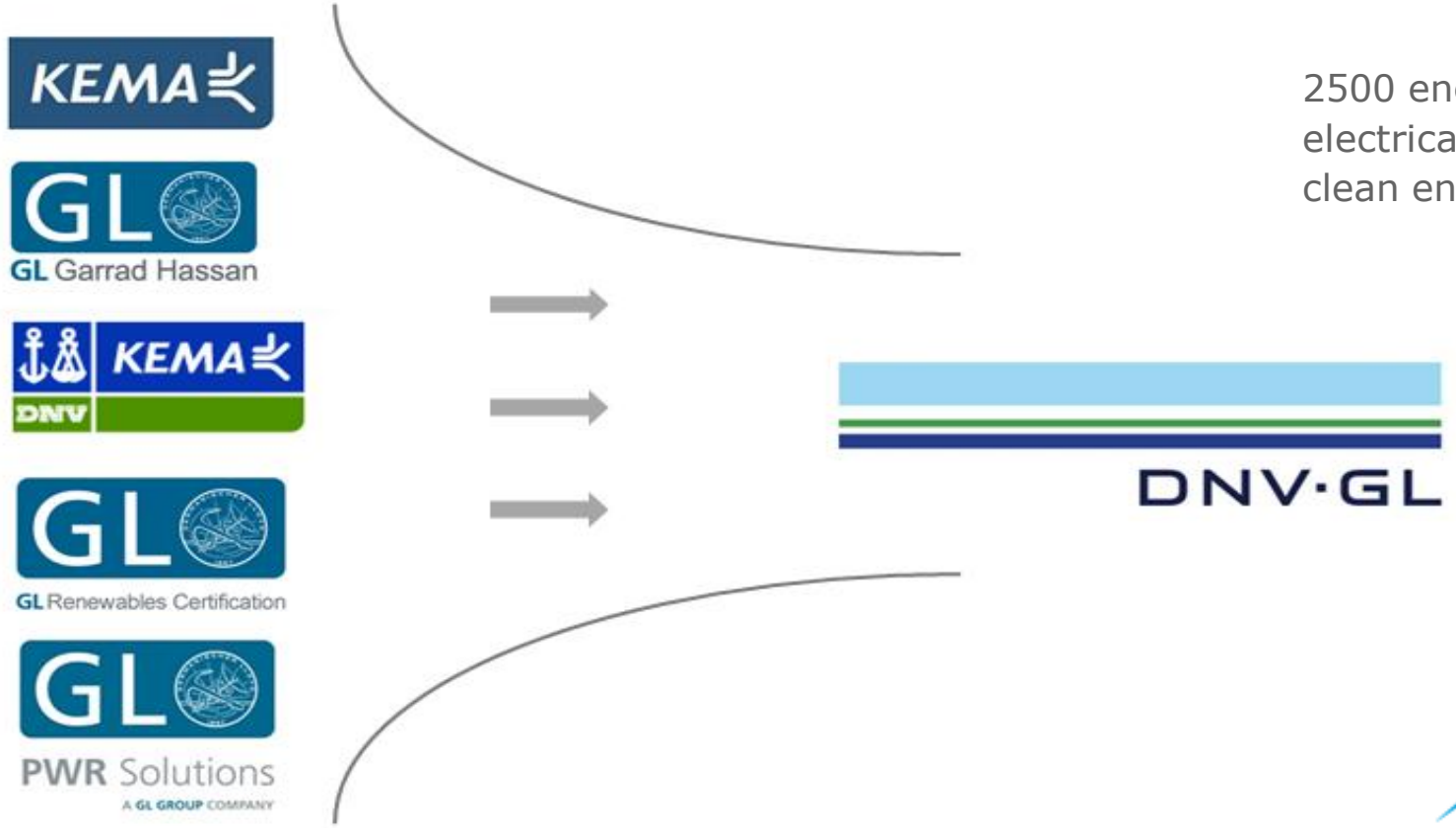




# COMBINING THE STRENGTH OF WELL-KNOWN BRANDS

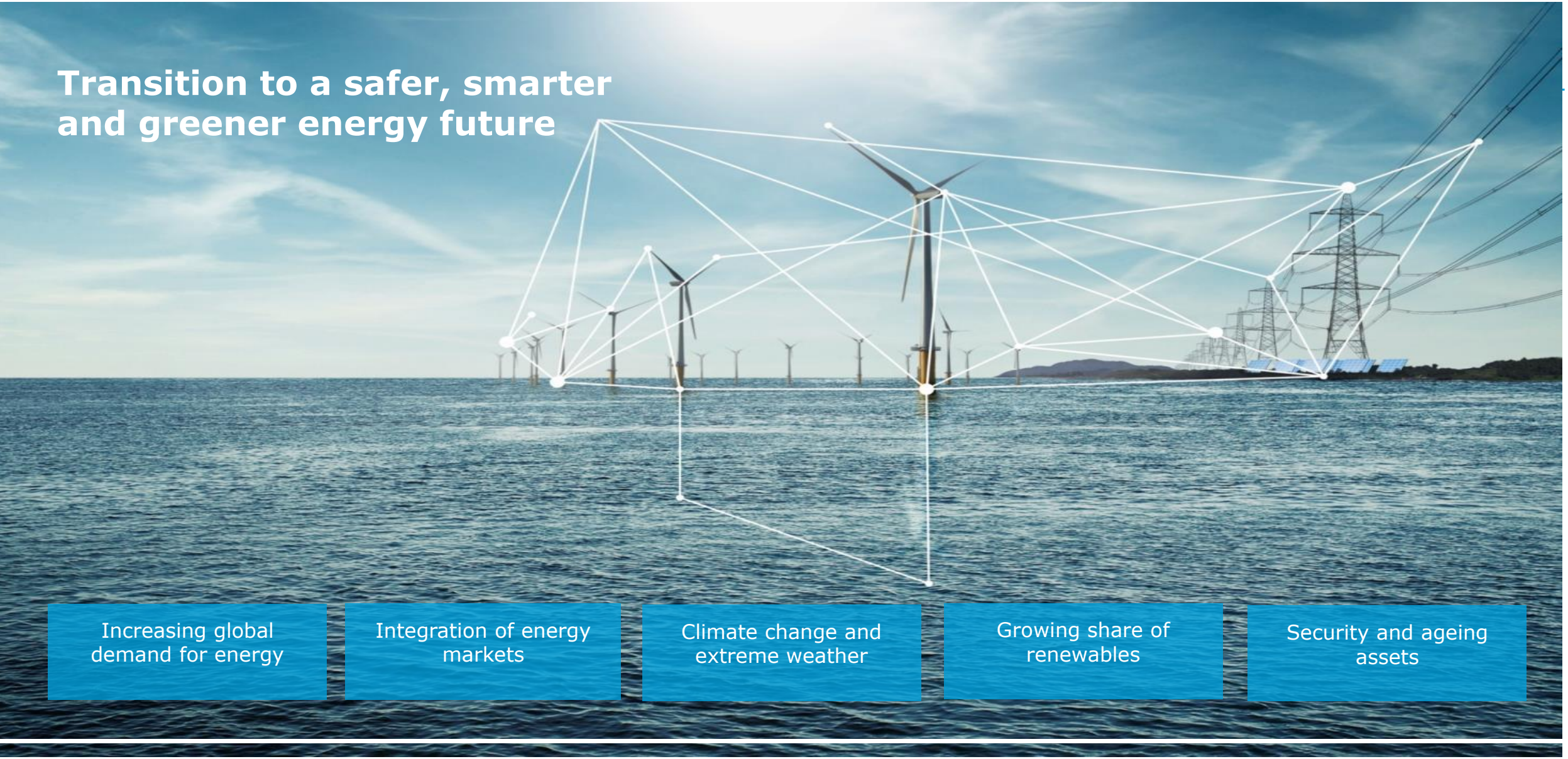
**DNV GL - Energy** combines the strengths and rich heritage of a couple well-known brands in energy, **KEMA, GL Garrad Hassan** and **GL Renewables Certification**.




2500 energy experts help customers throughout the electrical power industry realise efficient, reliable and clean energy for today and the future

**Ungraded**

# Transition to a safer, smarter and greener energy future



- Increasing global demand for energy
- Integration of energy markets
- Climate change and extreme weather
- Growing share of renewables
- Security and ageing assets

# Assisting companies to solve the energy trilemma


Ungraded



DNV·GL

# How we contribute to a safer, smarter and more sustainable world

Policy | Production | Transmission & distribution | Use

Examples of our project portfolio:

- ENISA smart grid cyber security certification study
- ENISA SCADA patching
- SCADA and substation automation conformity and interoperability testing
- 62351 Protocol test tools



**Ungraded**



DNV·GL


# Purpose of testing

## Critical Industrial Systems

**Gabriele Webber**

10 November 2016

**Ungraded**




SAFER, SMARTER, GREENER

# Not to scare you; but to make you think


**Ungraded**



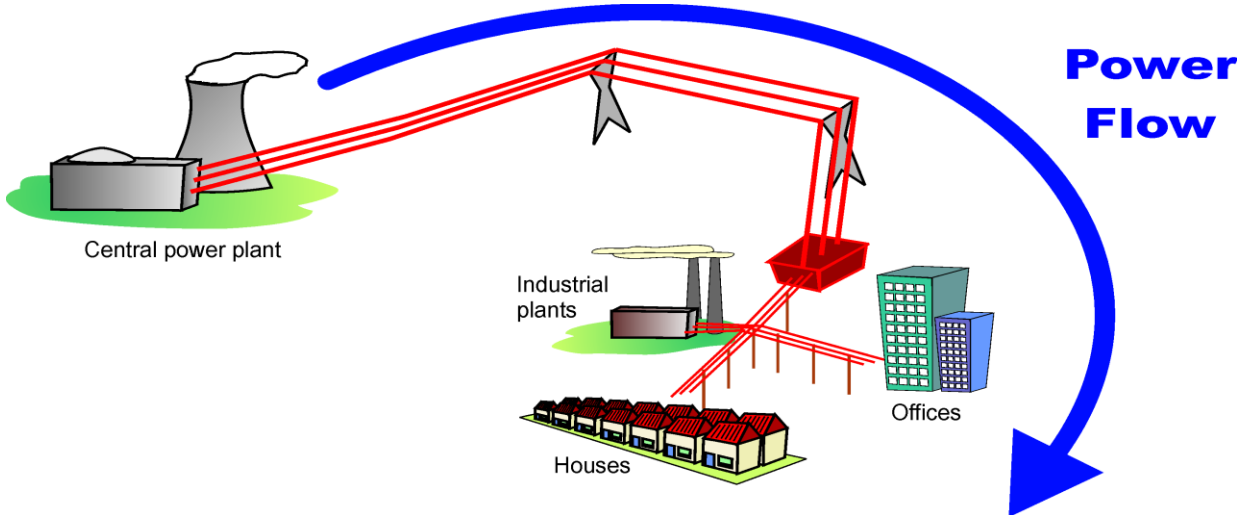
DNV·GL

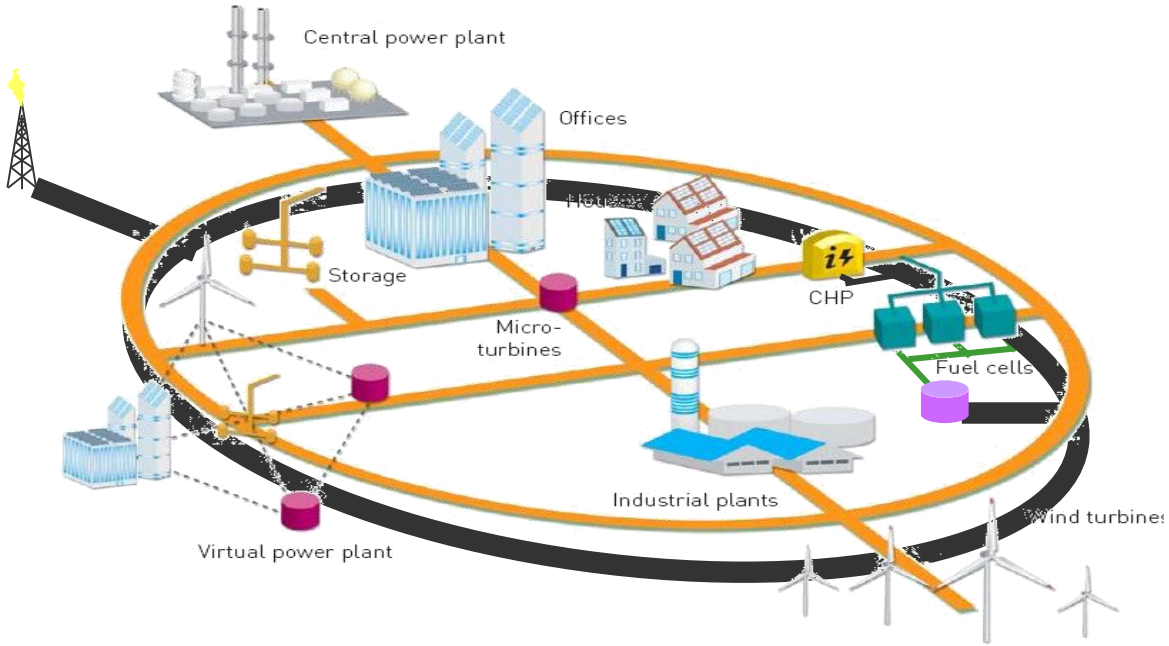
# IT vs OT

| | IT | OT |
|---|---|---|
| **Components** | Computers<br>Printers,…<br>Network components | Computers<br>Controllers<br>Actuators |
| **Incident implication** | Critical<br>On industry<br>On business | Limited<br>On business |
| **Incident management and maintenance** | Standard procedures | Emergency procedures |
| **Running software** | Dynamic, experimental | Static, conservative |
| **Applications and protocols** | Standard, many | Customized, few |
| **Attack vectors** | Generic | Customized |
| **Maintenance subjects** | Computer scientist | Engineer |

# The electricity infrastructure evolution

## Yesterdays infrastructure: simple and straight forward

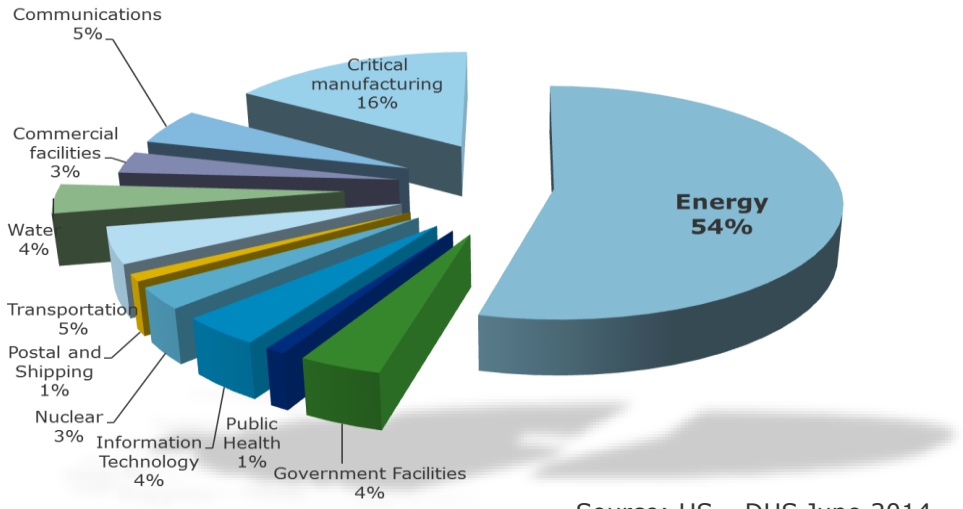


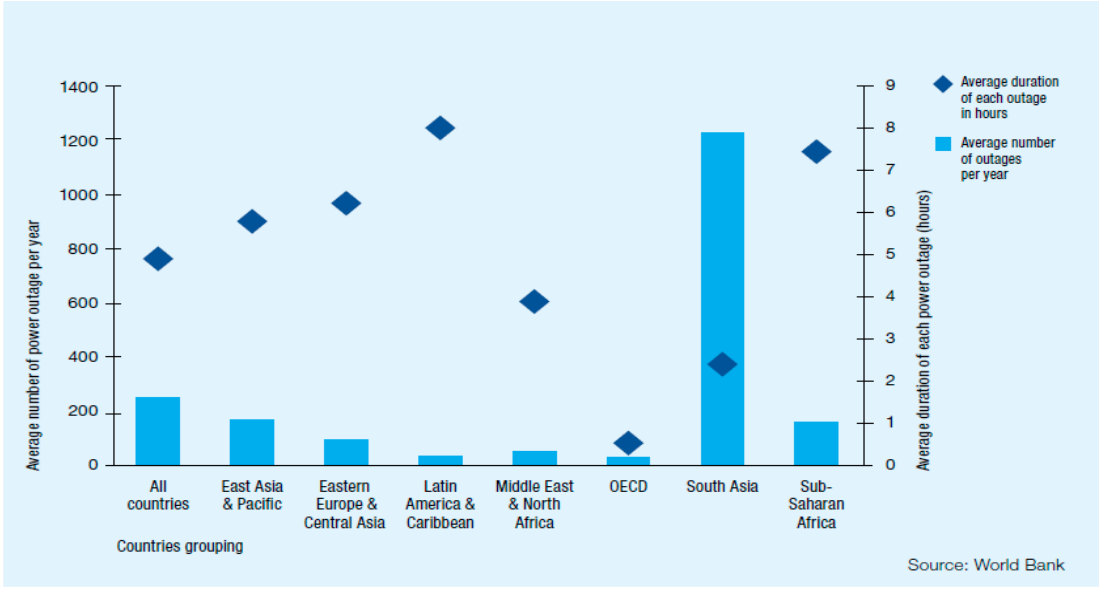

## Tomorrow: Smart Grids, highly intelligent fully integrated infrastructures

# Usage of common IT technologies comes at a price

1. Existing infrastructure is owned or used by parties that you do not have control over.
2. Multifunctional networks combine unrelated services on one network, causing conflicts.
3. Economic network designs interconnect unrelated systems on lower layers.
4. Low cost devices are more vulnerable to viruses, and easy to break.




Source: US – DHS June 2014




**Evolution in the smart grid also leads to more cyber vulnerabilities**

# Our approach

## A holistic approach to risk management and mitigation for critical infrastructures

**Gabriele Webber**

10 November 2016



# How to address the cyber security challenge?
# Security Management: A Holistic approach

**Holism** is the idea that a natural system (physical, biological, chemical, social, economic, mental, linguistic, etc.) and its properties should be viewed as a whole, not as a collection of parts

Systems function cannot be fully understood solely in terms of their component parts

Examples:
- Risk studied for a SCADA system as a whole (not only an RTU), with implications over a broad environment is holistic
- Involvement of engineers and management in the CS management is holistic
- V approach is holistic
- End 2 End test is holistic

# Information Security Management System (ISMS)

## International standards

- ISO/IEC 27001 and 27002
- IEC62351, IEC62443, ISA99
- ISF "The Standard of Good Practice for Information Security"
- NERC, NIST, IEC, WIB..

## Balanced approach

- People
- Technology
- Organisation

## The entire lifecycle of IT

- Requirements
- Design
- Development
- Commissioning
- Operations
- Decommissioning

## Organisation

- Policy
- Roles and Responsibilities
- Ownership

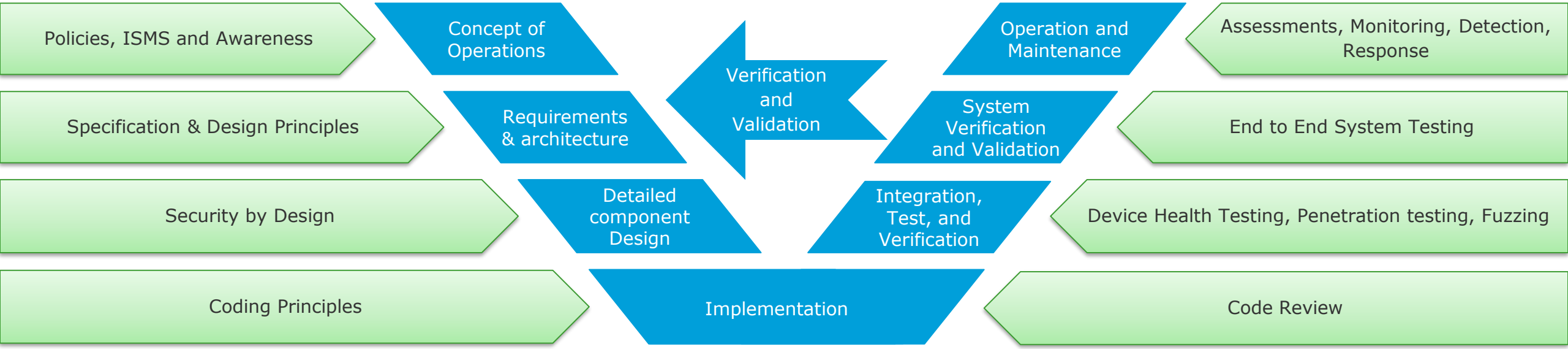
## Processes

- Incident, Problem and Change
- Monitoring & measuring
- Response
- Business Continuity

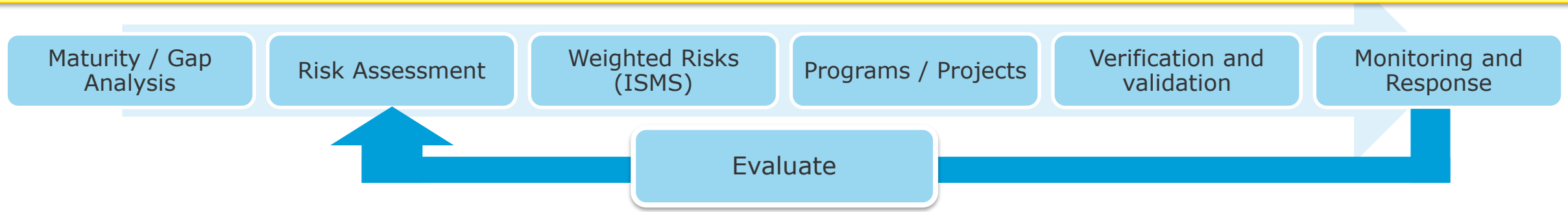
## Technical

- Architecture
- Security functionality
- Robustness
- Hardware and software maintenance

# Cyber Security portfolio




V model applied to cyber security aspects




Risk-based approach

# Use case: Health testing (device level)

## A path for a cyber secure environment

**Gabriele Webber**

10 November 2016

**Ungraded**

# Cyber Security Health Test

## Comprehensive, cost effective testing for energy IT systems and smart grids

- Independent security **assessment of IT/smart grid devices**, and a means to asses the **implemented** level of security within the product
- Aspects of the test process:
  - White box testing (pen testing)
  - DNV GL Test specification based on industry international standards
  - Methodology based on (international accepted) Common Criteria
  - Test against globally known vulnerabilities

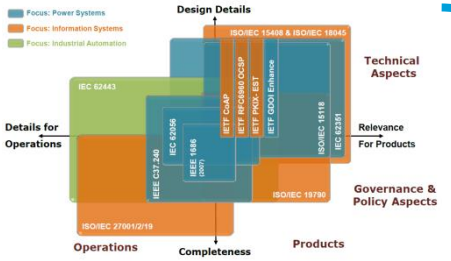
Deliverable: Test report assessing the implemented level of security

| Standard | Requirements | Testable requirements | Detailed | Testcases that can be defined |
|---|---|---|---|---|
| IEC62351 | 105 | 100% | 100% | 100% |
| IEEE 1686 | 50 | 100% | 90% | 80% |
| WIB | 102 | 49% | 35% | 30% |
| NERC-CIP | 85 | 38% | 25% | 20% |
| NIST IR 7628 | 147 | 35% | 20% | 10% |
| **Total** | **489** | **289** | **231** | **207** |

**Great for code review and re-design!**

# Cyber Security Health Test approach

Smart grid and security standards




Requirements

test pack tailored to the specific device

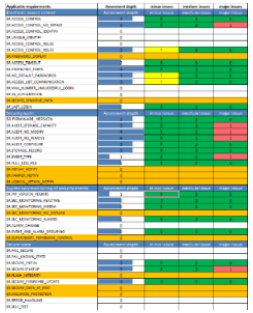
In-site, smart grid equipment

**Common criteria methodology**

## Testing scope

1. Functional testing
2. Protocols testing
3. Negative and robustness testing (fuzzing)
4. Known vulnerability testing, leveraging global vulnerability database

Findings and recommendations



**Ungraded**



DNV·GL

# Use case: End-to-end testing (system level)

## A path for a cyber secure environment

**Gabriele Webber**

10 November 2016

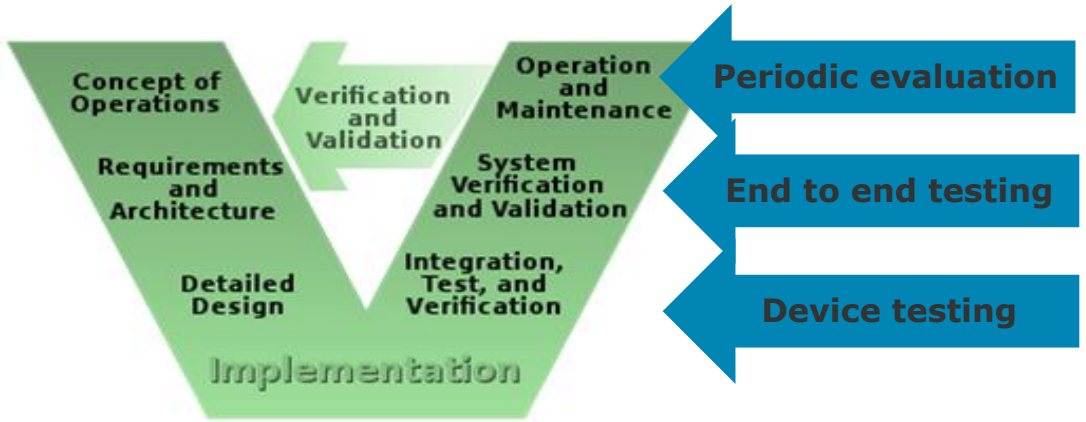


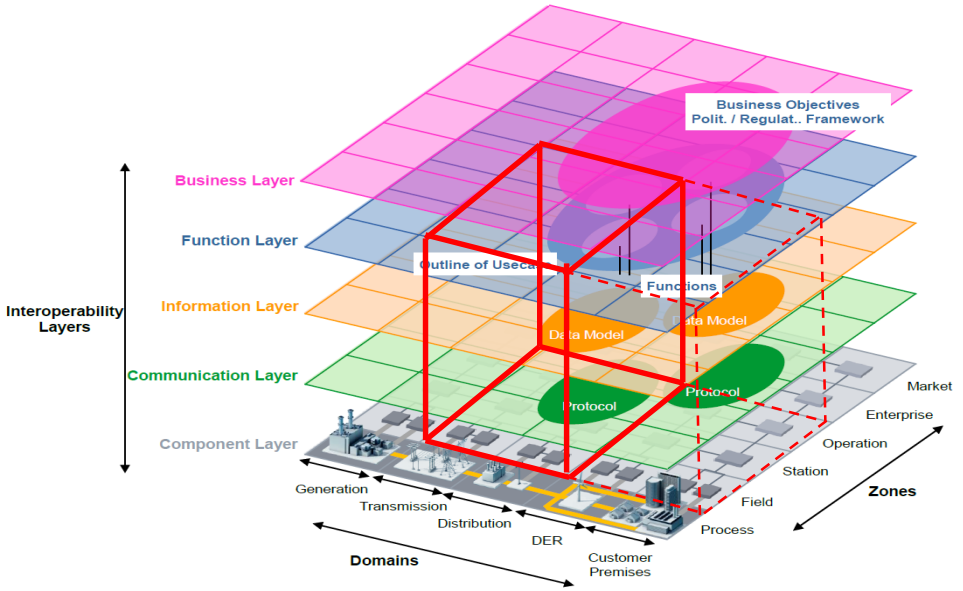
 

# End-To-End Test

## Comprehensive, cost effective testing for energy IT systems and smart grids

- 3rd party technical validation services to provide bottom-up proof that proper security measures have been taken for a complete system from an end to end perspective.
- We assess your system regarding
  - Secure network design principles
  - Physical cyber defences and intrusion prevention
  - Data stream analysis
  - Policy and procedures for prevention, detection, mitigation and recovery
- Deliverable:
  Report describing the cyber secure state of your OT / ICS / smart grid system.

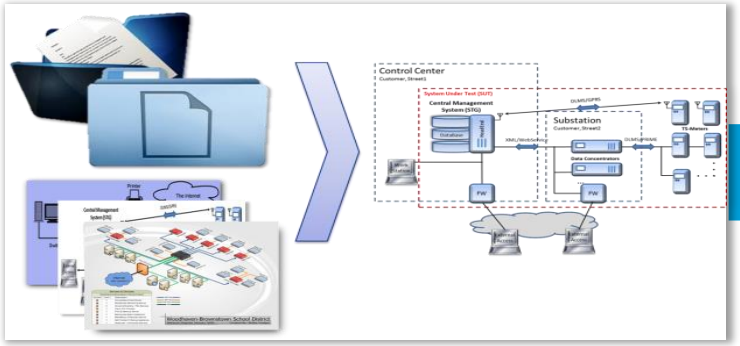


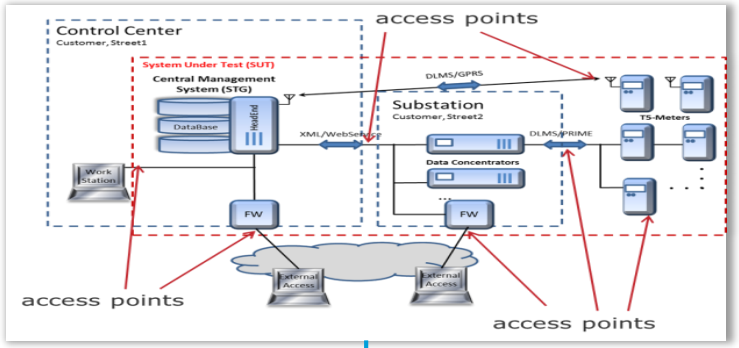

**Ungraded**

# End to end system testing approach

Data aggregation & scope definition

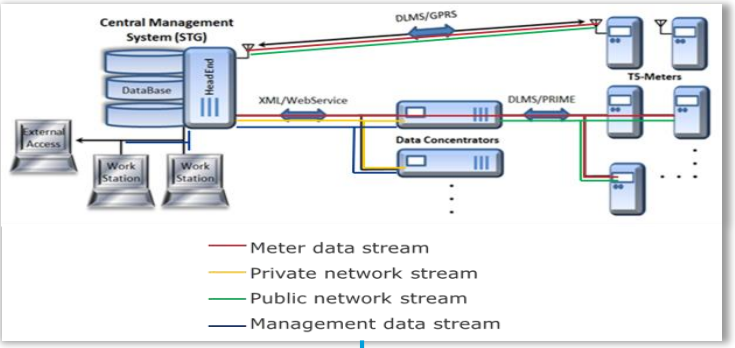


Perimeter access points




&

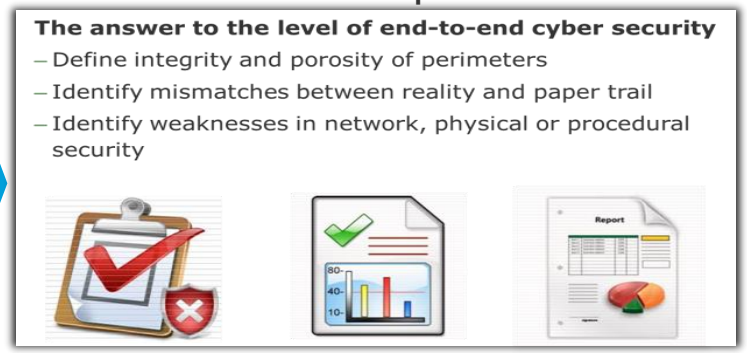
Network data streams




Test book definition


Test execution


Final report




**Ungraded**



DNV·GL

# DNV GL Cyber Security

**Gabriele Webber**
gabriele.webber@dnvgl.com
+31 26 3 56 6031

**www.dnvgl.com**

**SAFER, SMARTER, GREENER**

**Ungraded**



DNV·GL