2nd Annual review
Florence 14th November 2013

nSHIELD Run through

September 1st 2012 – August 31st 2013
by: Josef Noll
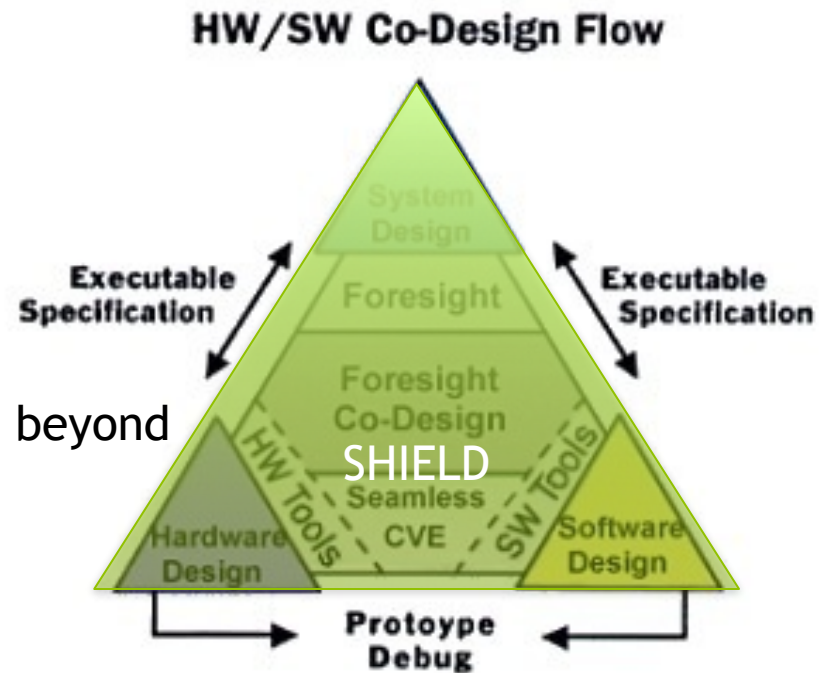
nSHIELD - Run Through Use case Exercise

SHIELD Methodology to create SPD Devices

SHIELD Methodology =
 pSHIELD (Security requirements)
 nSHIELD (Metrics-based analysis)
 nSHIELD (Ontology descriptions)
—> SHIELD (security assessment/ composability)

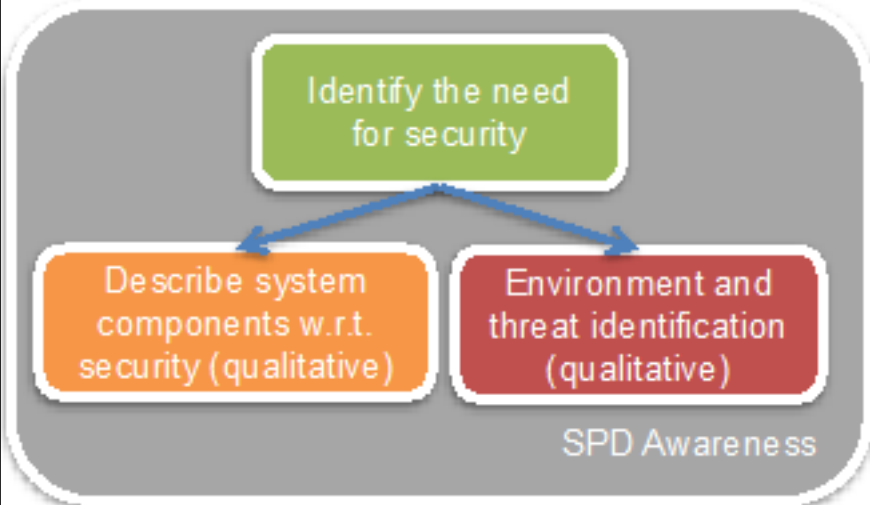Integrated industrial implementation beyond nSHIELD

HW/SW Co-Design Flow

nSHIELD Design Flow first year focus

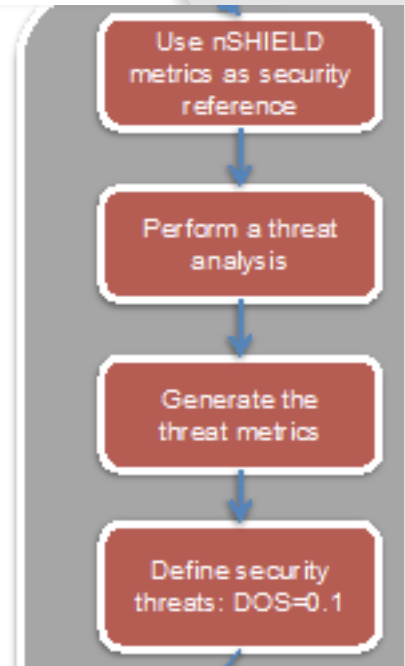| STEP	INPUT	OUTCOME
Environment and threats identification		Awareness
SPD Assessment	Application case *	SPD Guidelines
Metrics Implementation	SPD Guidelines and Tools*	Metrics (security measure)
Ontology Definition	Application case *, Tools*	Ontology (OWL)
Technological Injection	Software Module*, IP *, Template*, Trusted run time environment *	Software/Firmware customized modules (SPD SF Module)
Integration	SPD SF Modules + Design files	E.S. physical Implementation
Validation/Verification	SPD Validation tools*	Validation Report
Deployment	Market impact?	E.S physical Implementation + end user application note

* From nSHIELD

nSHIELD

nSHIELD Design Flow **2nd** year focus

STEP	INPUT	OUTCOME
Environment and threats identification		*Awareness*
SPD Assessment	*Application case*	*SPD Guidelines*
Metrics Implementation	*SPD Guidelines and Tools*	*Metrics (security measure)*
Ontology Definition	*Application case, Tools*	*Ontology (OWL)*
Technological Injection	*Software Module, IP, Template, run time environment*	*Software/Firmware customized modules (SPD SF Module)*
Integration	*SPD SF Modules + Design files*	*E.S. physical Implementation*
Validation/Verification	*SPD Validation tools*	*Validation Report*
Deployment	**Market impact**	*E.S physical Implementation + end user application note*

* From nSHIELD

nSHIELD

The SHIELD run-through blocks

1) Identification and description

Identify the need for security

Describe system components w.r.t. security (qualitative)

Environment and threat identification (qualitative)

SPD Awareness

2) Metrics based assessment

Use nSHIELD metrics as security reference

Perform a threat analysis

Generate the goal metrics

Set security goals: privacy=0.8

Use nSHIELD metrics as security reference

Perform a threat analysis

Generate the threat metrics

Define security threats: DOS=0.1
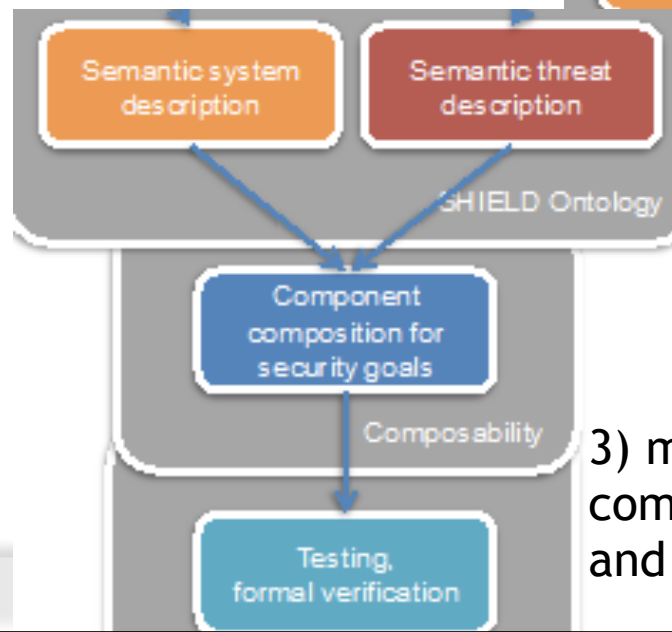
3) measures/ composition and verification

Semantic system description

Semantic threat description

SHIELD Ontology

Component composition for security goals

Composability

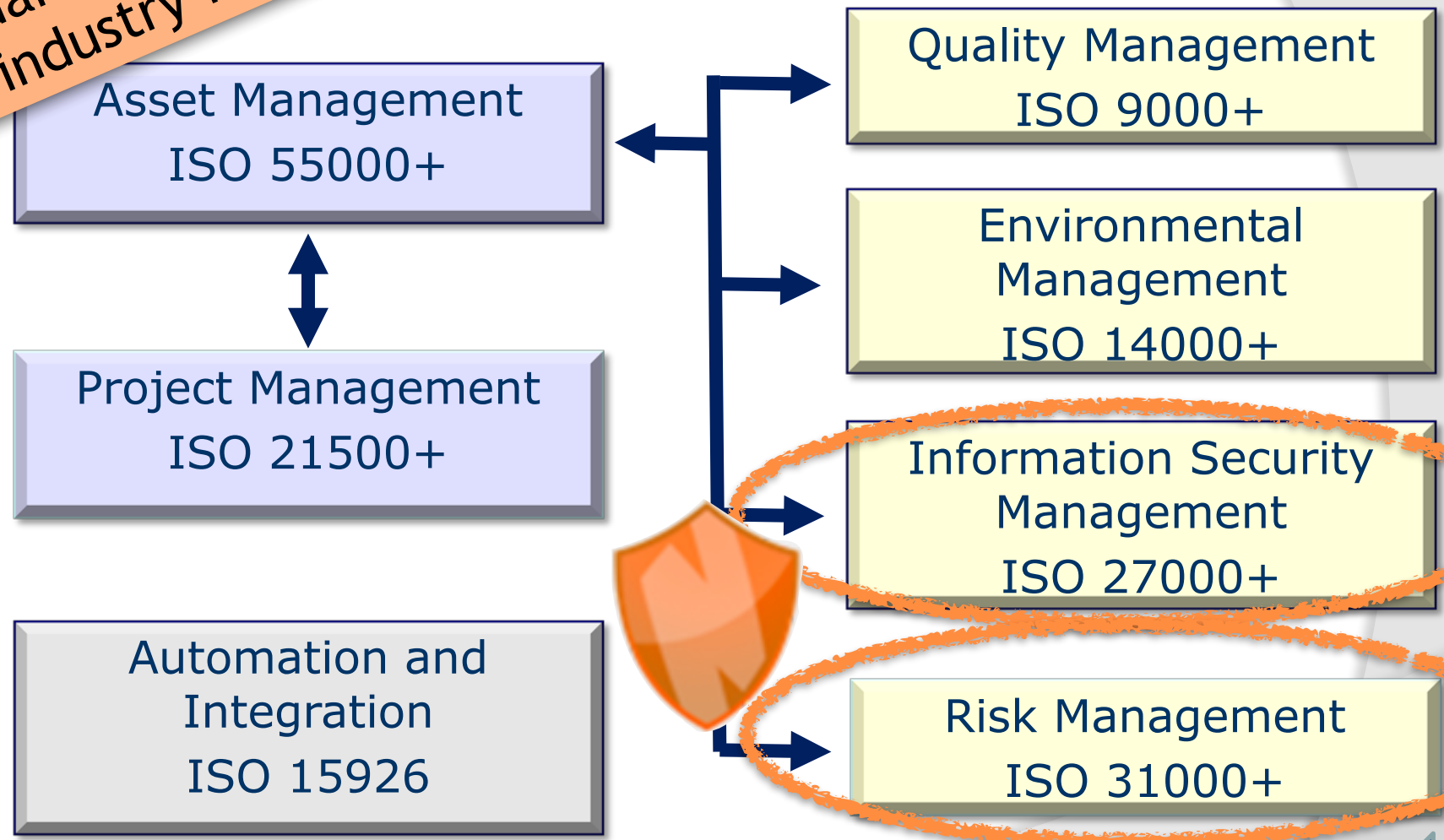Testing, formal verification

5

SHIELD – Market Impact

- Measurable security is not a issue in the actual market
  - IFEA (ABB, GE, …): "how to add security"
  - oil industry: "reliability", "software is new for oil industry (adoption)"
- SPD value not intuitive

nSHIELD

Market Impact for Process automation

- Focus on oil and gas
  - security framework
  - clearly identified business values
- Challenges
  - separation of logic, on- versus offshore
  - delay <4 ms for energy processes, <10 ms for compressor adjustments
  - lifetime of components > 10 years
- add-on security
  - old components (replace, modular design?)
  - variety of HW, SW and OS
  - critical to extra delays

nSHIELD

Management in ISO

Asset Management
ISO 55000+

Project Management
ISO 21500+

Automation and Integration
ISO 15926

Quality Management
ISO 9000+

Environmental Management
ISO 14000+

Information Security Management
ISO 27000+

Risk Management
ISO 31000+

[source: Thor Langeland, 2013]

Concluding remark

SHIELD methodology, consisting of

- metrics assessment,

- security ontology descriptions, and

- measured / composed security

Ready for validation in three use-cases, assessment in 4th use case