DEIS

Evaluation of a Dependability Mechanism for Cyber Physical Systems

Dr. Gilbert Regan

EuroAsiaSPI 2019

Lero THE IRISH SOFTWARE RESEARCH CENTRE

University of Limerick Ollscoil Luimnigh

DCU

Trinity College Dublin Coláiste na Tríonóide, Baile Átha Cliath The University of Dublin

UCD Dublin

OÉ Gaillimh NUI Galway

Dundalk Institute of Technology

UCC University College Cork, Ireland Coláiste na hOllscoile Corcaigh

Maynooth University National University of Ireland Maynooth

Institute of Technology Tralee

Presentation overview

- DEIS project overview
- Assessment methodology
- Results/Conclusion

DEIS Project

- Increasingly interconnected world

- Why?
  - ...developed independently
  - ...data protection issues
  - ...cybersecurity

DEIS Goal

Development of technologies that:

1. facilitate the **efficient synthesis** of components and systems based on their dependability information, and
2. to enable the exchange of safety critical information in real time.

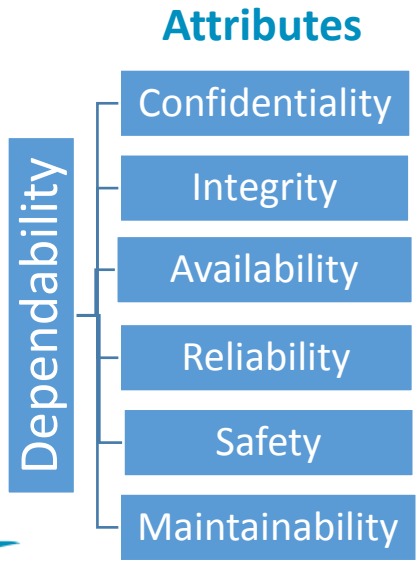
DEIS Consortium Partners

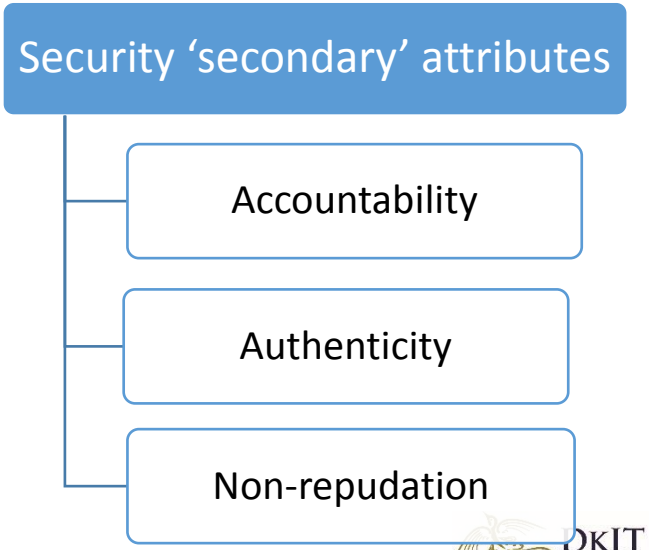
Figure 20: DEIS Consortium plus the advisory board partner AEV

Definition

Dependability

- Qualitatively defined as the ability to deliver service that can justifiably be *trusted*, and
- Quantitatively defined as 'the ability to *avoid service failures* that are more frequent and more severe than is acceptable to its user(s)'

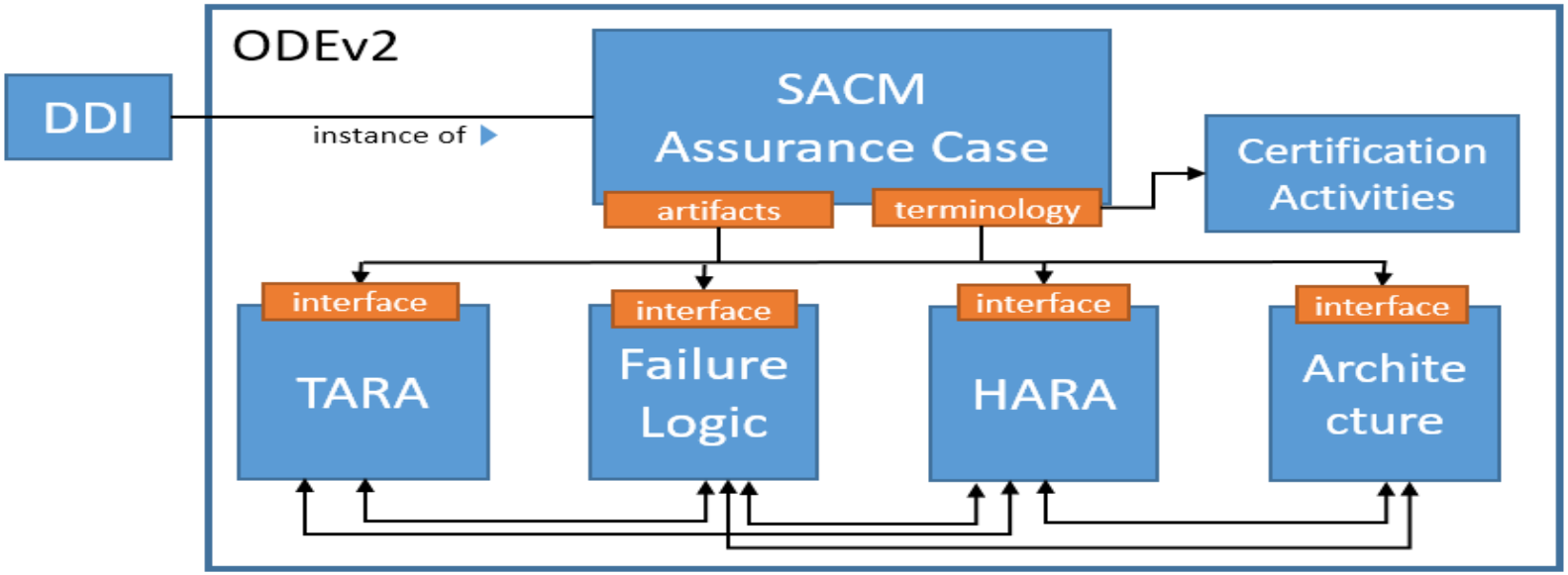




DKIT | REGULATED SOFTWARE RESEARCH CENTRE

DDI Overview

DEIS concept……. **Digital Dependability Identity (DDI)** of a component or system. A DDI contains information that uniquely describes all the dependability characteristics of a system which are required for certifying the system's dependability



Why SACM?

- SACM defines a metamodel for representing structured assurance cases and provides corresponding means for modularisation.
- SACM is **already standardised and relatively mature**, which might help us get the DDI concept / ODE meta-model accepted and adopted eventually.

DKIT REGULATED SOFTWARE RESEARCH CENTRE

DDI Target

The DDI targets:

1. **improving the efficiency** of generating consistent dependability argumentation over the supply chain **during design time**;
2. laying the foundation for **runtime certification** of ad-hoc networks of embedded-systems.

The DDI of a system contains:

1. **claims about the dependability guarantees** given by a system to other systems and derived system dependability requirements;
2. **supporting evidence** for those claims in the form of various models and analyses.

DEIS Tools ?

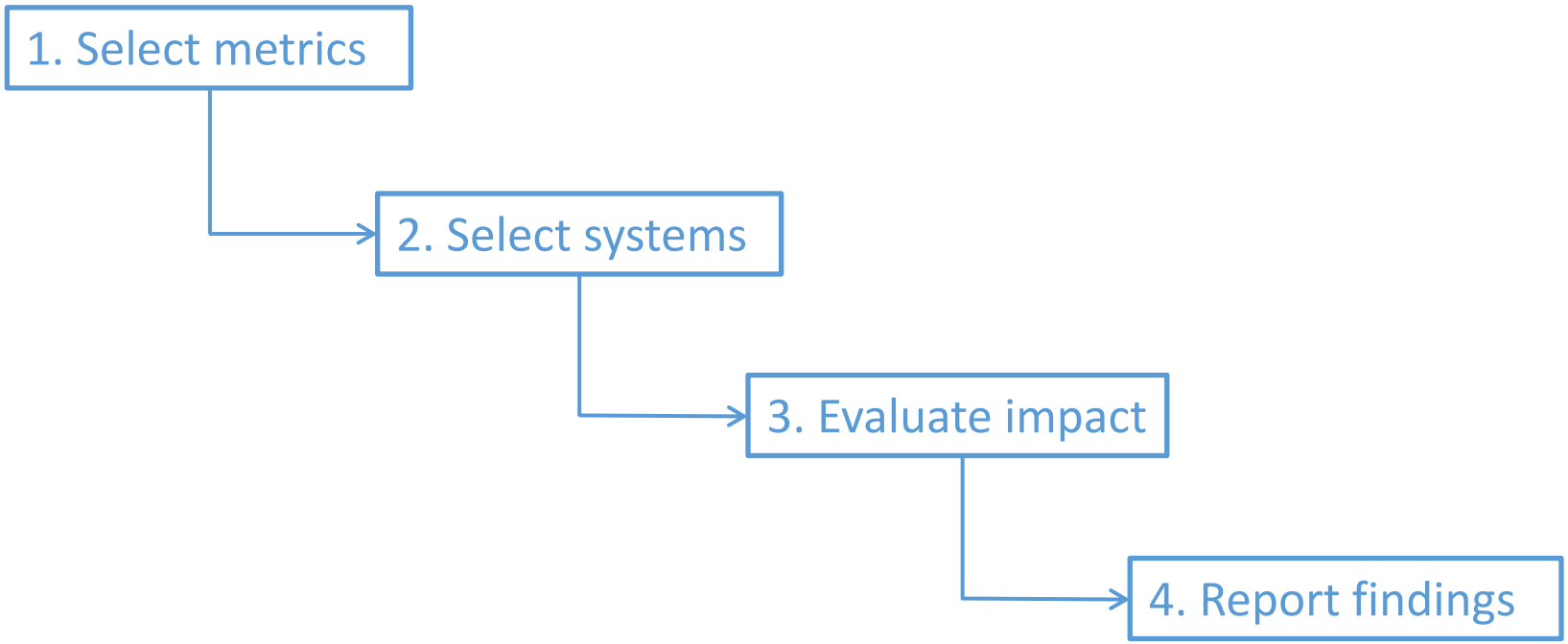
- ACME
- HIP-HOPS
- etc

Presentation overview

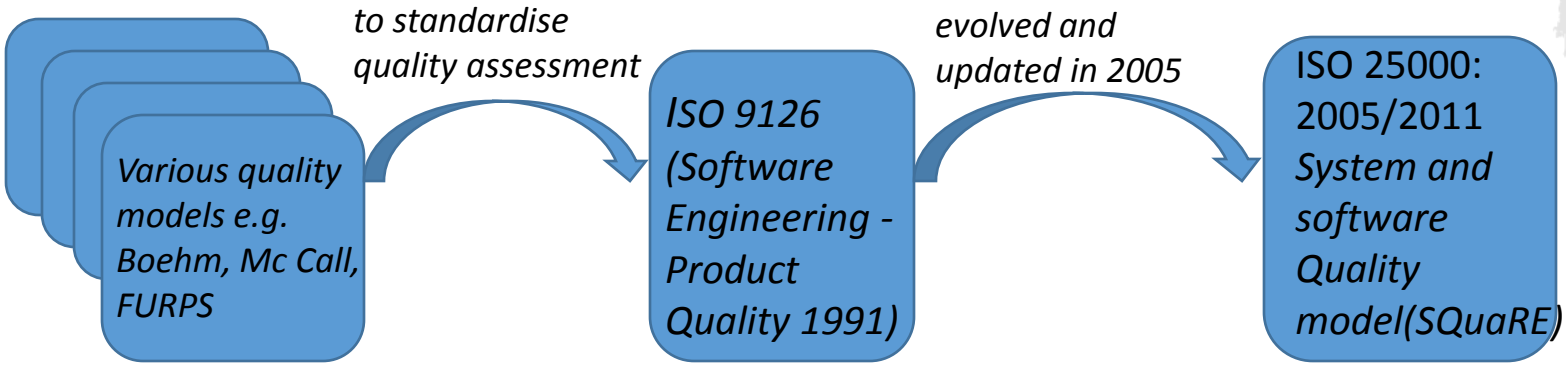
- DEIS project overview
- **Assessment methodology**
- Results/Conclusion

Research Methodology

- 4 stage approach

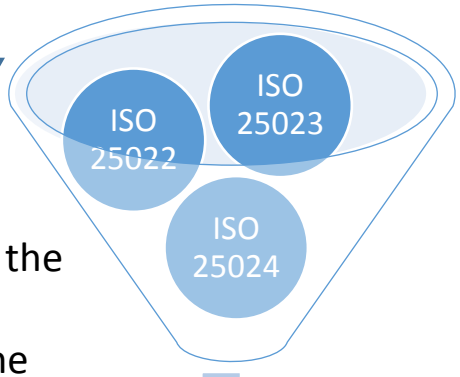


Research Methodology – Stage 1 Select metrics



4 Industrial Partners + DKIT

analysis



1) its relevance to assessing the impact of the DDI;
2) practicality for each partner to make the measurement
3) Agreement reached by general consensus

21/28 Quality characteristics

58/185 measures

ISO 25000 Characteristics and Measures Example

Characteristic	Sub-Characteristis	Measure	Measurement Function
Compatability	Co-existence Measures	Co-existence with other products	X = A/B A = Number of other specified software products with which this product can co-exist B = Number of other software products specified to co-exist with this product in theoperation environment
	Interoperability measures	Data formats exchangeability	X = A/B A = Number of data formats exchangeable with other software or systems B = Number of data formats specified to be exchangeable
		Data exchange protocol sufficiency	X = A/B A = Number of data exchange protocols supported B = Number of data exchange protocols specified to be supported
		External interface adequacy	X = A/B A = Number of external interfaces that are functional B = Number of external interfaces specified

Research Methodology – Stage 2 - Select Systems

Automotive - physiological parameter monitoring

GM

SIEMENS

Railway - European Train Control System

Automotive – Truck platoon

AVL

Healthcare – app for oncology professionals

portablemedical TECHNOLOGY LTD

DKIT REGULATED SOFTWARE RESEARCH CENTRE

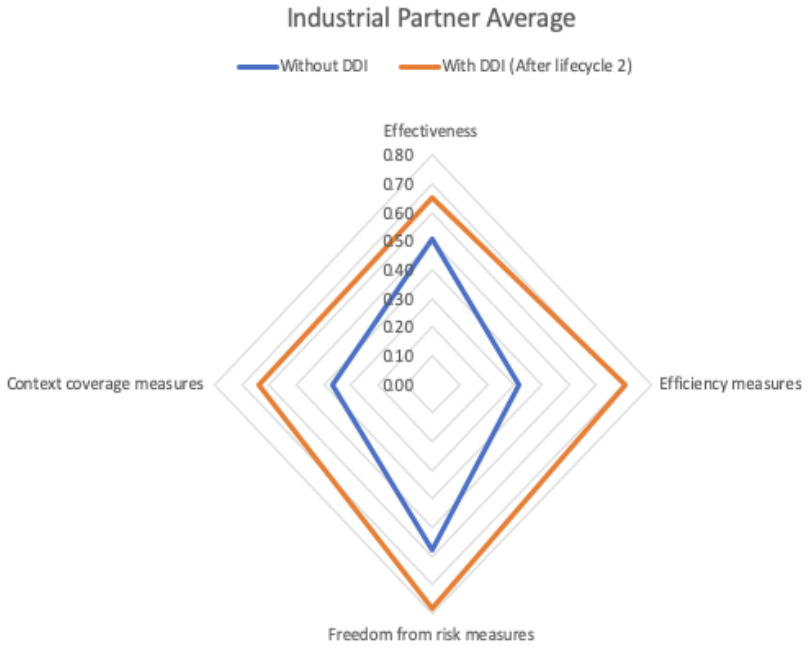
Presentation overview

- DEIS project overview
- Assessment methodology
- **Results/Conclusion**

DDI impact findings

Quality in Use (ISO 25022)

Characteristic (4)	Sub characteristic (3)	GM	GM	AVL	AVL	PMT	PMT	SAG	SAG	AVG% imp.
Effectiveness	n/a	0.39	0.56	0.5	0.63	0.5	0.58	0.64	0.83	14.2
Efficiency	n/a	0.44	0.62	0.25	0.44	0.53	0.82	0.05	0.95	39.0
Freedom from Risk	Economic risk mitigation	0.61	0.73	0.65	0.85	0.33	0.68	0.73	0.87	20.3
Context Coverage	Context completeness, and Flexibility measures	0.2	0.2	0.42	0.67	0.5	1.0	0.35	0.69	27.3

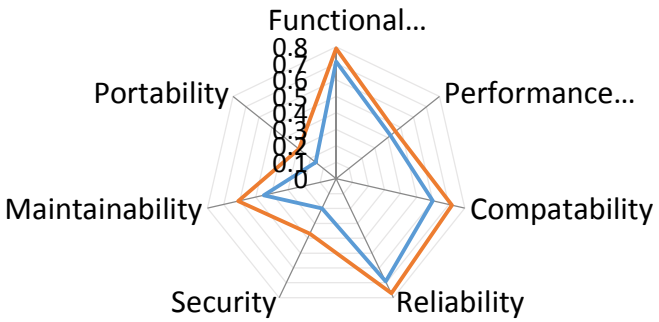


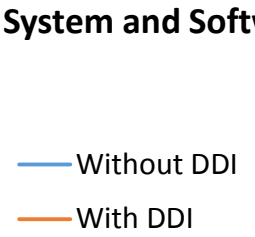
Siemens

'We are expecting a significant increase of the number of the objectives achieved for the same period of time by introducing DDI. Furthermore, we are expecting a significant decrease in the cost for carrying out the task for the same amount of objects in ETCS use case'.

DKIT REGULATED SOFTWARE RESEARCH CENTRE

DDI impact findings





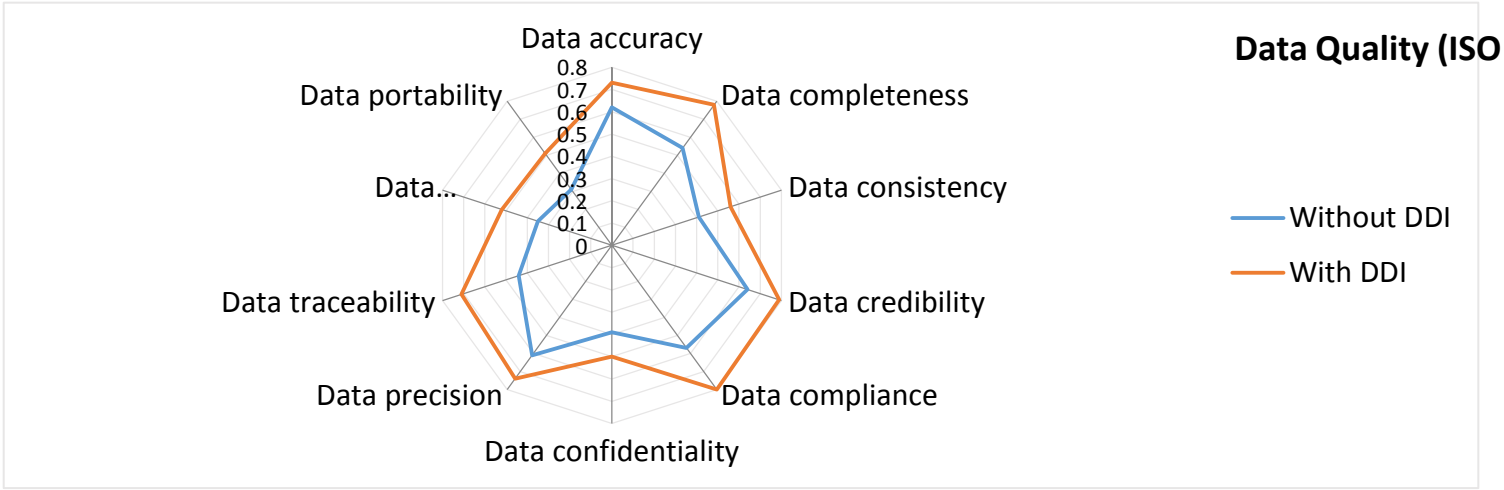
Performance Efficiency: Resource utilization: Siemens:*'for mean processor utilisation and bandwidth utilisation, we could not observe any improvement by use of DDI. Both mean processor utilisation and bandwidth utilisation remain low for railway safety-critical system'*

Portability: GM stated *'No improvement here, considering that no other scenario has been evaluated outside the GM architecture ecosystem',* while **AVL** stated *'No portability related implementation has been done'.*

Functional suitability: Siemens: *Our ETCS* products *have 1% of missing intended usage of the system without DDI (99% of usage completeness).....This estimation is also true for the correctness of functions'*

There are occasions where some metrics may not apply to some systems. For example the 'portability' metric only showed improvement in the PMT system.

DDI impact findings



Siemens indicated no improvement in a number of metrics (all at 100%). *For the **data completeness, data credibility, data precision and data compliance**,* Siemens state that *'their ETCS system has to be certified according to relevant safety standards and that these values are at 100% regardless of whether the DDI is applied or not'.*

GM indicated no improvement in the data confidentiality metric. However GM further state that *'the DDI can help in selecting at design time the best security solution to satisfy confidentiality requirements'.*

While the majority of the selected data quality metrics are applicable to most of the use cases, there were occasions where some metrics may not apply to some systems

Conclusion

- DDI has made significant improvements in the quality of each system. Dependability increased due to the harmonised exchange of safety argumentation.

  Average Improvement:

  Quality in Use… 25.2%
  System/software Quality….10.9%
  Data Quality….17.5%

- Not all metrics may apply to all systems and we need to review our metric selection before next round of evaluation, for example:

  - ‘Portability’ only showed improvement in one of the four systems.
  - For a small number of metrics one partner already considered themselves to be at 100%

- Results shown are for lifecycle 2 of the DEIS project. Next lifecycle involves tool development that allows for the automatic generation and integration of DDI, which should help improve metrics further and thus improve dependability

Lero THE IRISH SOFTWARE RESEARCH CENTRE

Thank you
Questions and feedback welcome

gilbert.regan@dkit.ie

http://deis-project.eu/

Science Foundation Ireland sfi For what's next
Southern Regional Assembly
Ireland's European Structural and Investment Funds Programmes 2014-2020
Co-funded by the Irish Government and the European Union
European Union
European Regional Development Fund