ITEA 2

INFORMATION TECHNOLOGY FOR EUROPEAN ADVANCEMENT

openETCS

InnoTrans 2014 - openETCS Workshop

Agile Methods meet Safety

supported by:

Federal Ministry of Education and Research

Liberté • Égalité • Fraternité
RÉPUBLIQUE FRANÇAISE
MINISTÈRE DE L'ENSEIGNEMENT SUPÉRIEUR ET DE LA RECHERCHE

INVESTISSEMENTS D'AVENIR

Région de Bruxelles-Capitale

GOBIERNO DE ESPAÑA
MINISTERIO DE CIENCIA E INNOVACIÓN

openETCS@ITEA2 Project

Jan Welte (TU Braunschweig)

Berlin, 24.09.2014

OpenETCS Project

3 Main innovative Aspects

- **Open Source – Open Proof**
- **Formal Methods**
- **Agile Development**

Agenda

1. Safety
2. Traditional Development
3. Agile Development
4. Agile for safety-relevant development
5. Conclusion

Safety and Safety-relevant Systems

The EN 50128 standard defines safety as the

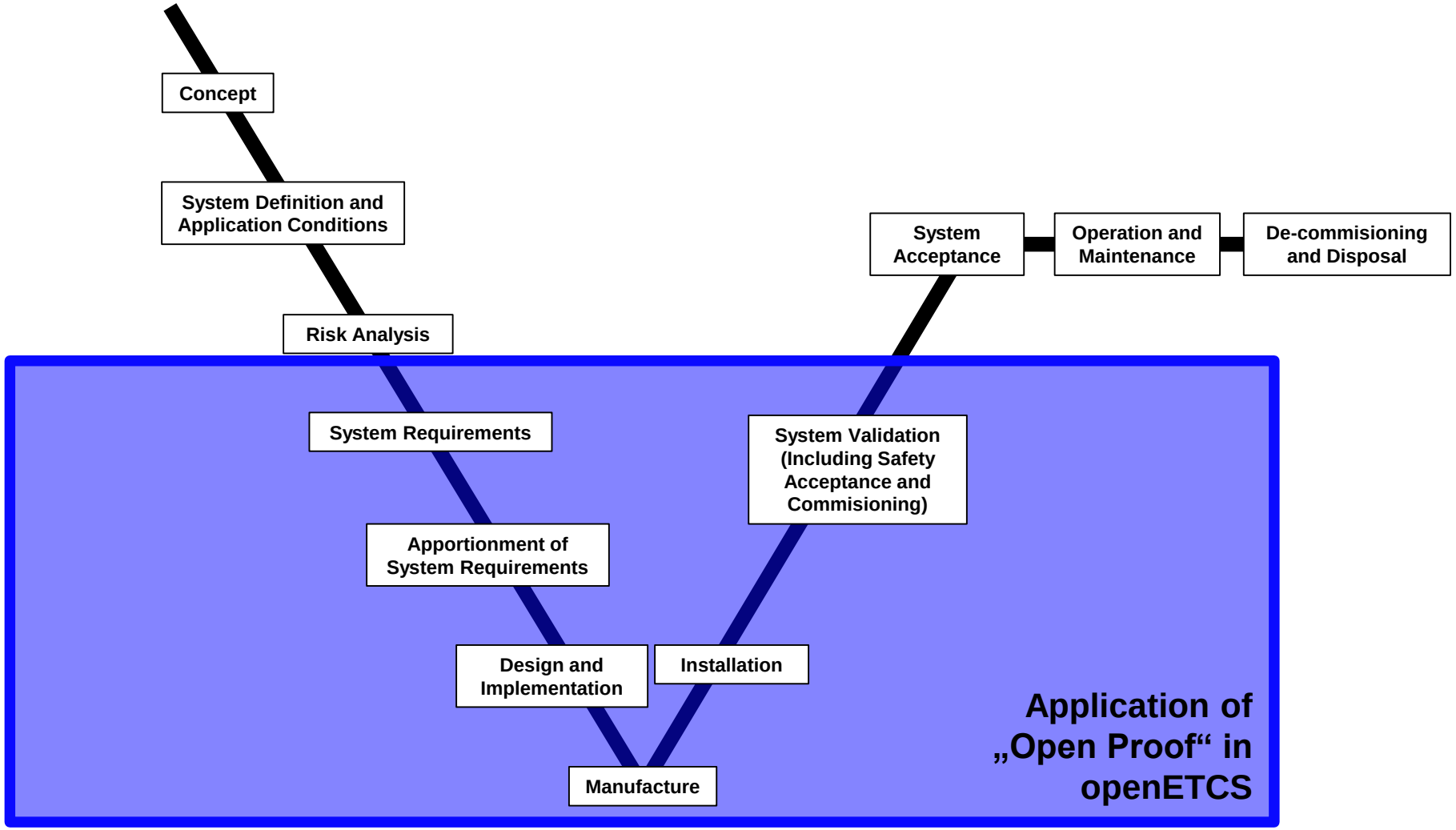
- **“freedom from unacceptable levels of risk of harm to people“**

CENELEC standards safety approach is risk-based

A safety case is “the documented demonstration that the product complies with the specified safety requirements.” [EN 50129]

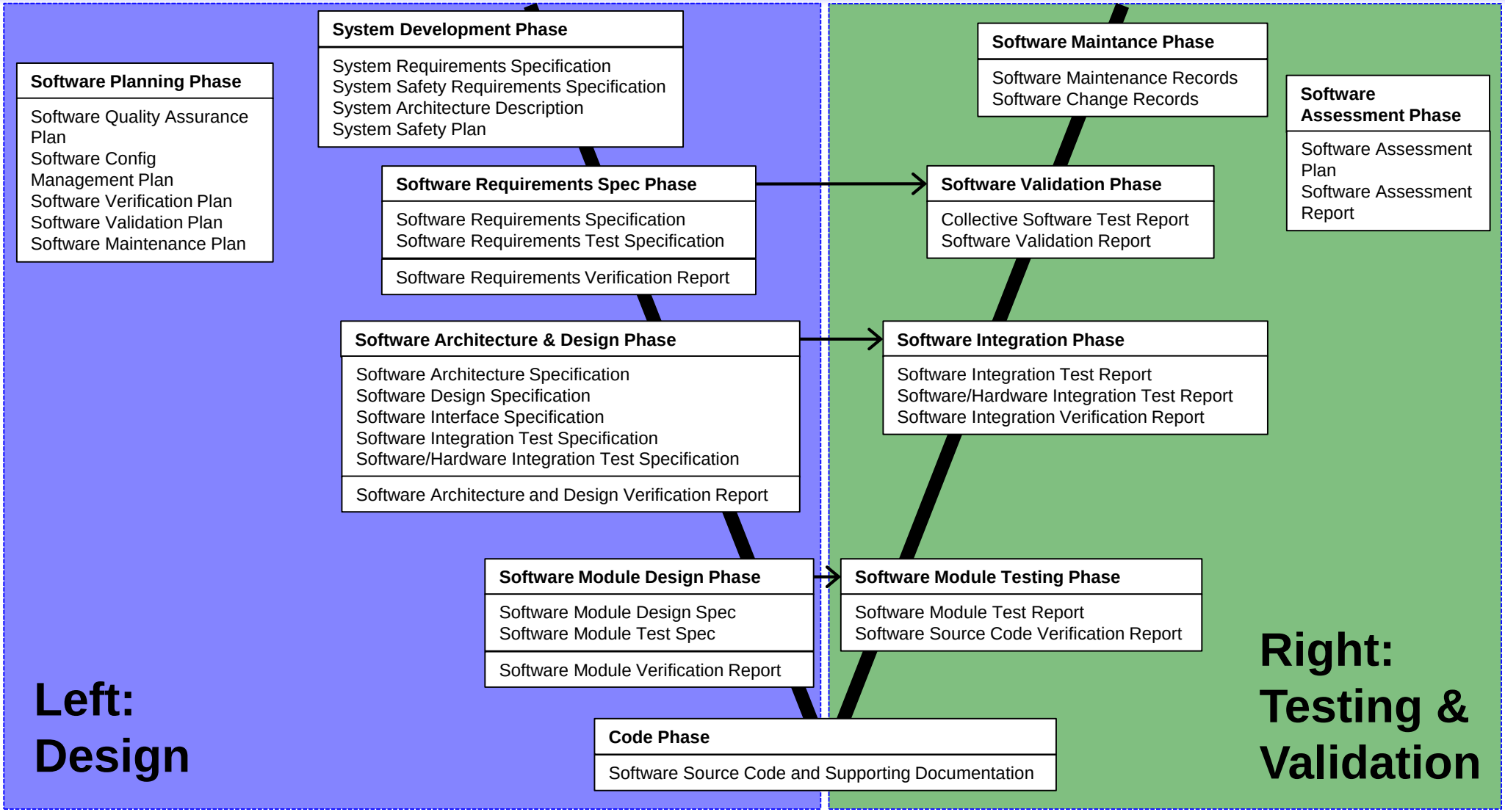
Traditional Development

System Lifecycle according to EN 50126



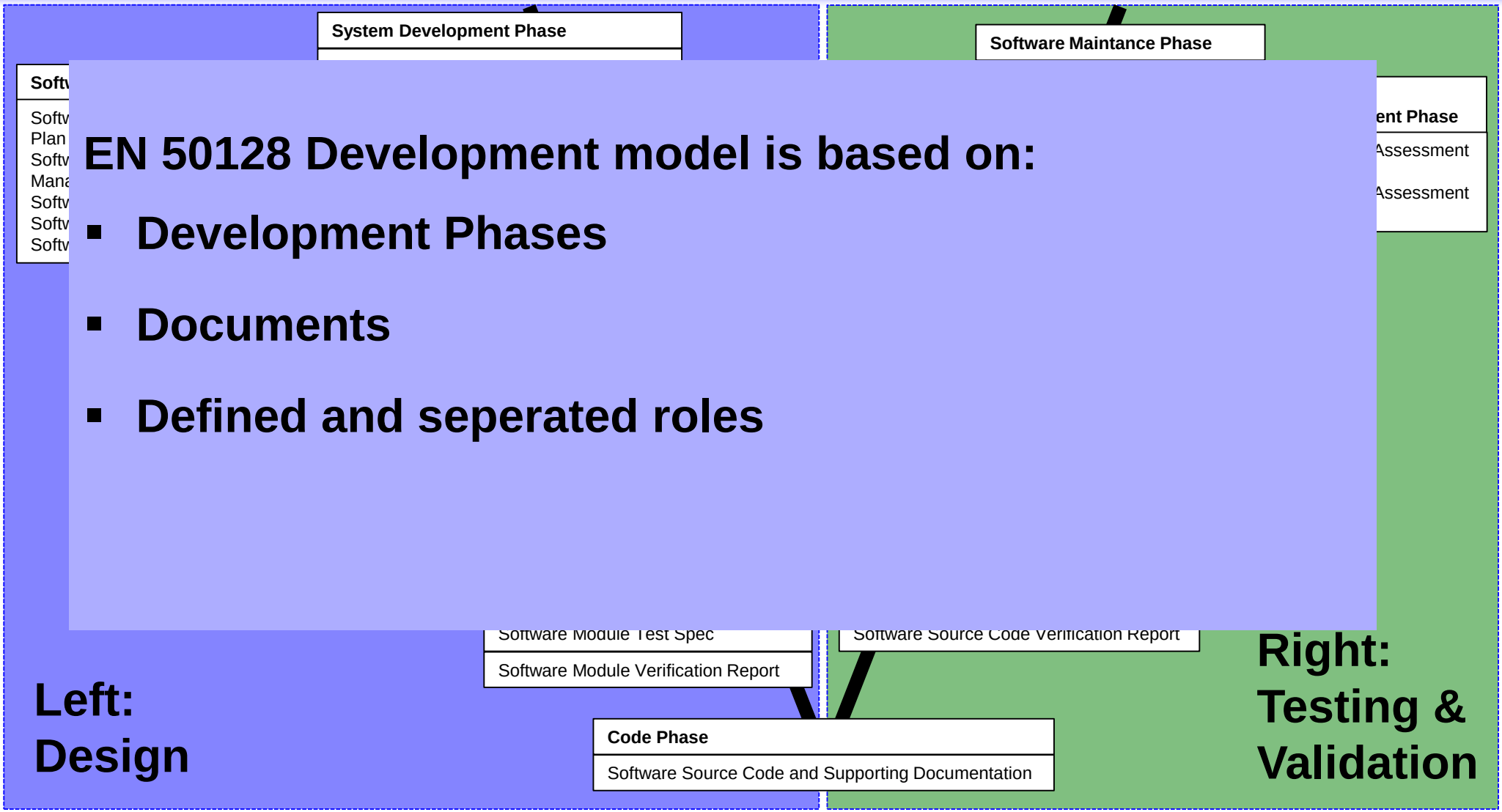
Traditional Development

Software Development Lifecycle according to EN 50128



Traditional Development

Software Development Lifecycle according to EN 50128



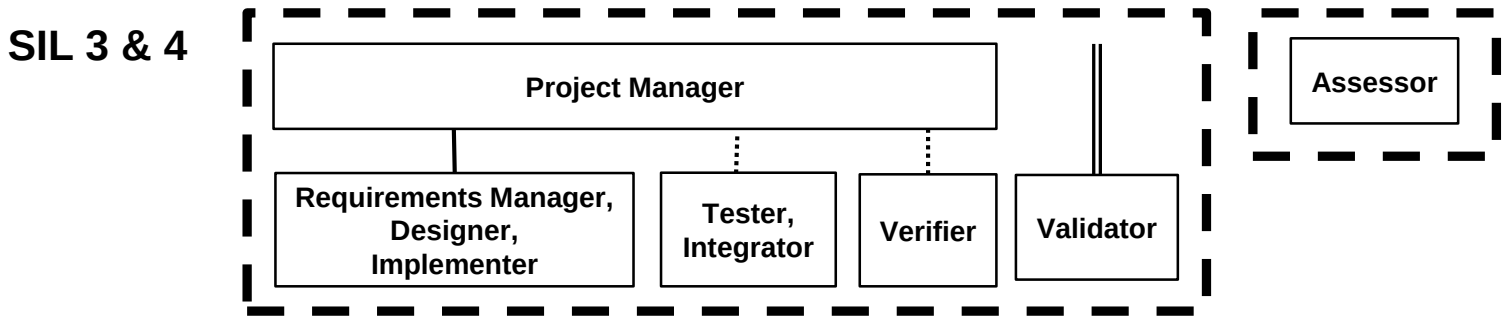
EN 50128 Development model is based on:

- **Development Phases**
- **Documents**
- **Defined and seperated roles**

Traditional Development
Roles

EN 50128 Development process:

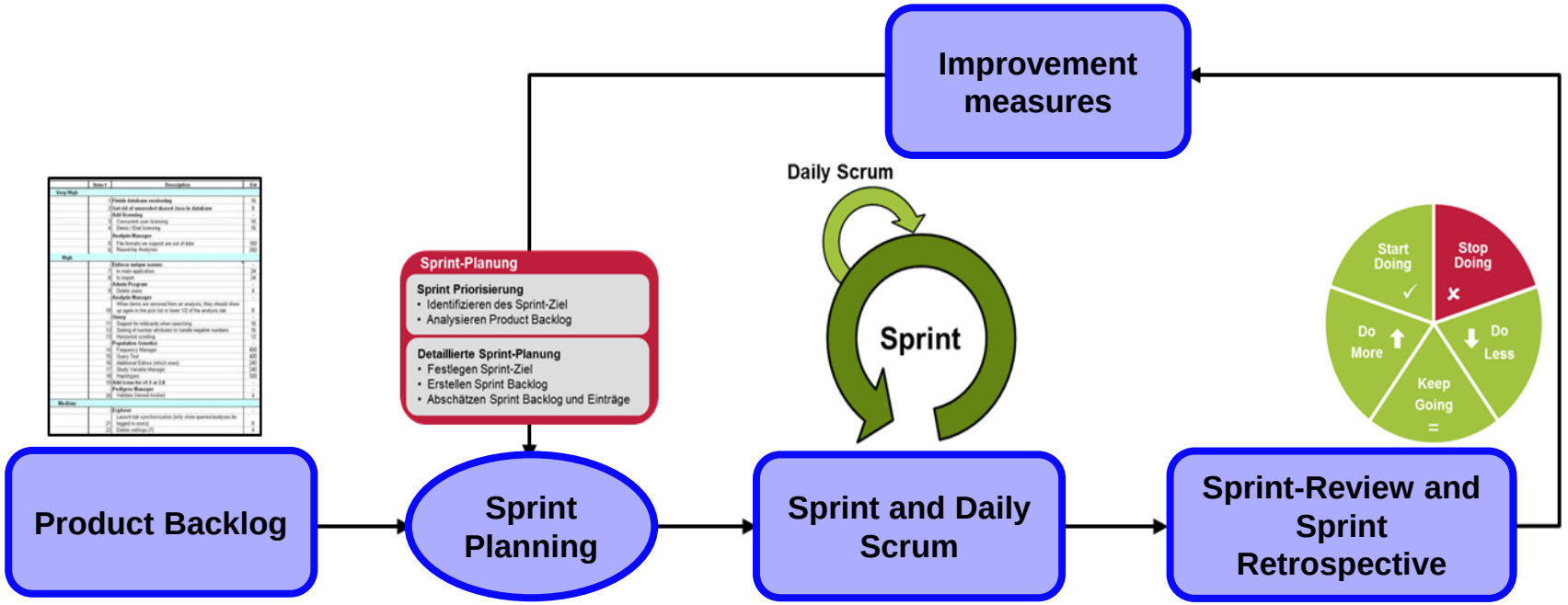
- Clearly distinguishes between a number of roles
- Requires proof of qualification for roles



Agil Development

SCRUM Software Development

Scrum has been developed to focus on costumer needs



Agil Development

SCRUM Software Development

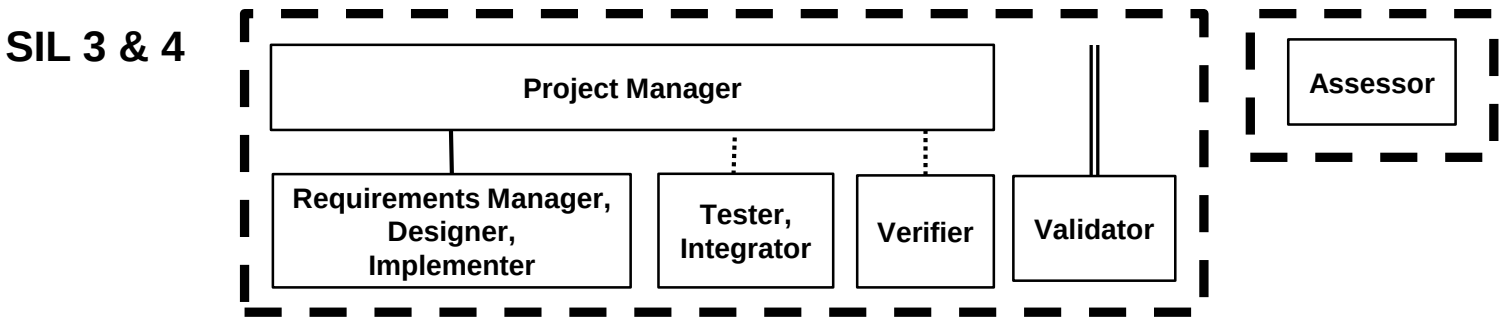
Sc

SCRUM Development is based on:

- **Focus on Design**
- **Iterative Process**

  (Every Sprint runs through all phases)
- **Team members are generalists**

Agile for safety-relevant development
Roles

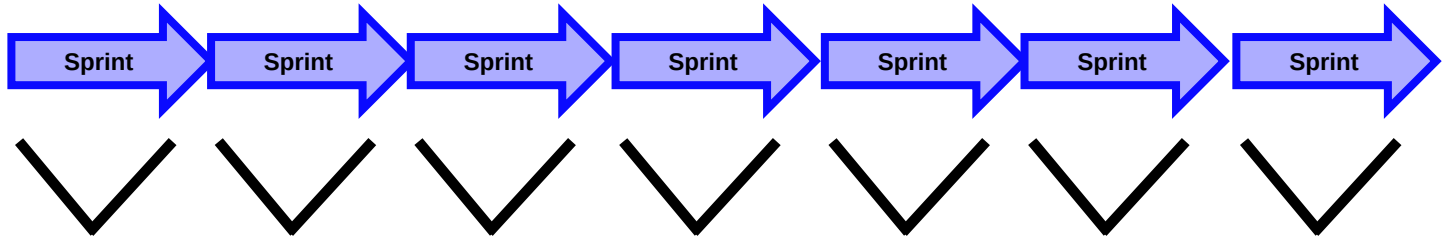


SCRUM roles:

- **Product owner = Project Manager**
- **SCRUM Master = Team Leader**
- **Scrum Team = Designer, Implementer, (Tester, Integrator Verifier) – seperated teams or personal roles**
- **Need new roles: Validator Team, Assessor**

Agile for safety-relevant development

Agile safety-related development

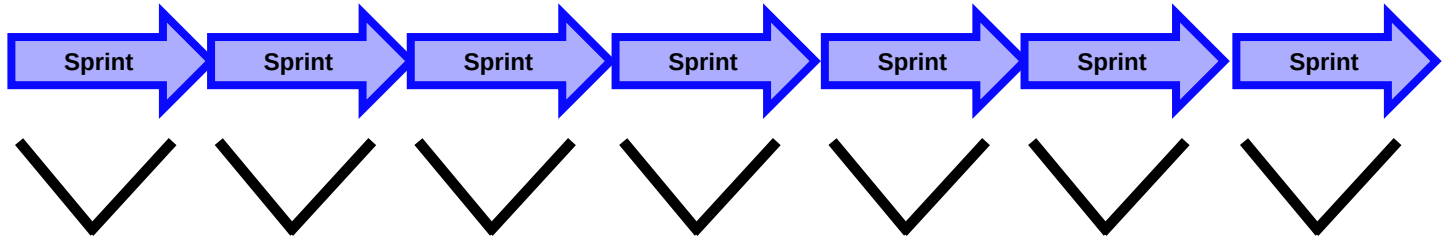


Agile for safety-relevant development

Agile safety-related development

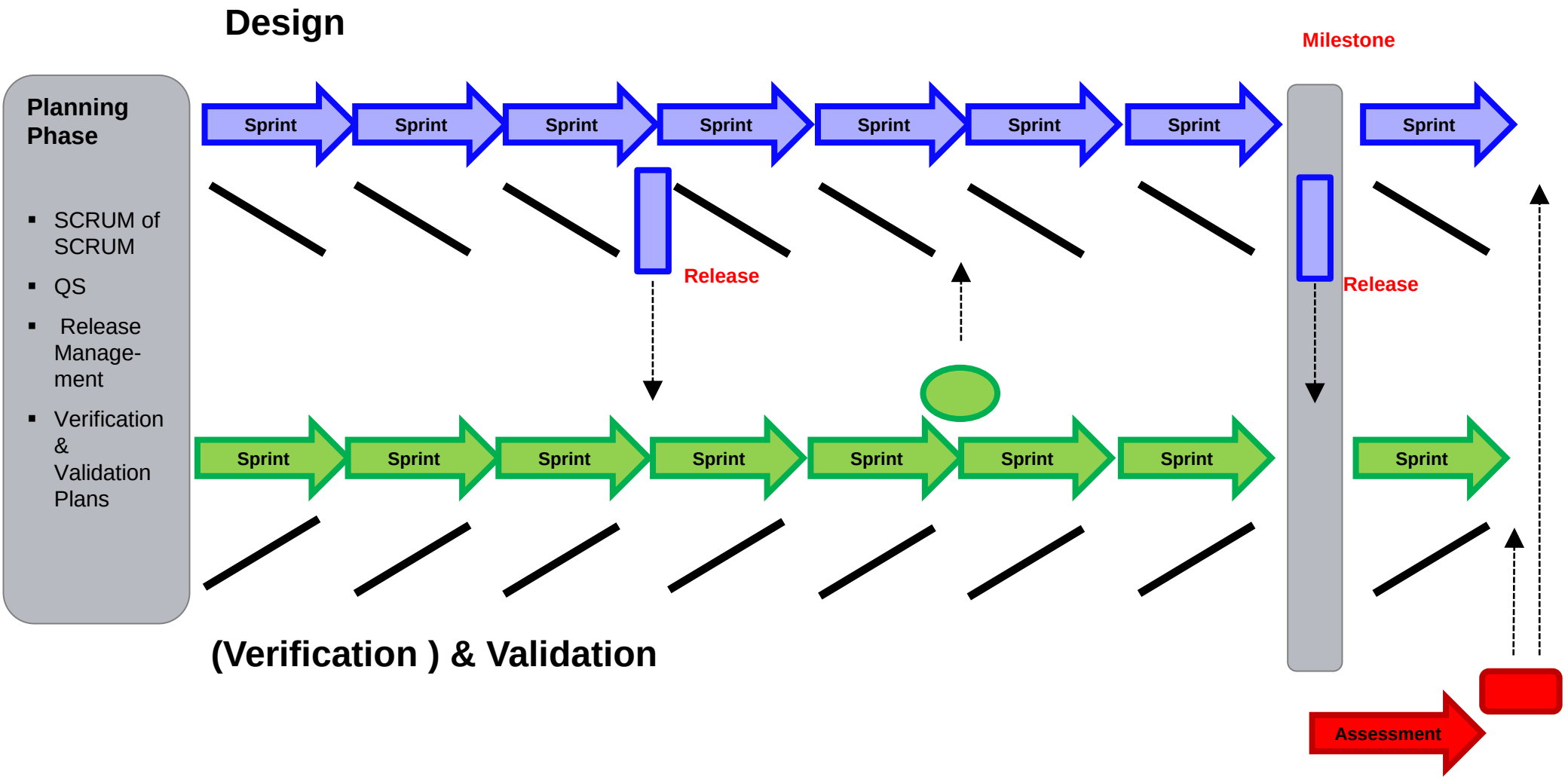
Planning Phase

- SCRUM of SCRUM
- QS
- Release Manage-ment
- Verification & Validation Plans



Agile for safety-relevant development

Agile safety-related development



Conclusion

Realisation of Scrum Development

- **Modified SCRUM can used for safety-relevant development**
- **Steps needed to confirm to EN 50128:**
  - **Independent roles for Project Management, Validation, Assessor**
  - **Overall Software Planning Phase to fill project backlog**
  - **Plan to incrementally write documents**
  - **Coordination of exchanged releases between Scrum Teams (Design, Verification/Validation)**
  - **Defined Change and Failure Management**
  - **Defined Release Management for Assessment and Validation**

Questions and Discussion

Technische Universität Braunschweig

Institut für Verkehrssicherheit und Automatisierungstechnik iVA

Prof. Dr.-Ing. Dr. h.c. mult. E. Schnieder

Jan Welte

Tchnische Universität Braunschweig

Institute for Traffic Safety and Automation Engineering
welte@iva.ing.tu-bs.de