

Sicherheitskritische Software mit dem V-Modell

Michael Erskine, Volker Stucky
LFK-Lenkflugkörpersysteme GmbH

Hintergrund

- Verteidigungssysteme (HW/SW) mit Schwerpunkt Flugkörper
- Geschäftssystem konform mit dem V-Modell XT
- Große, langjährige, internationale Entwicklungsprojekte
- Eingebettete Echtzeitsoftware

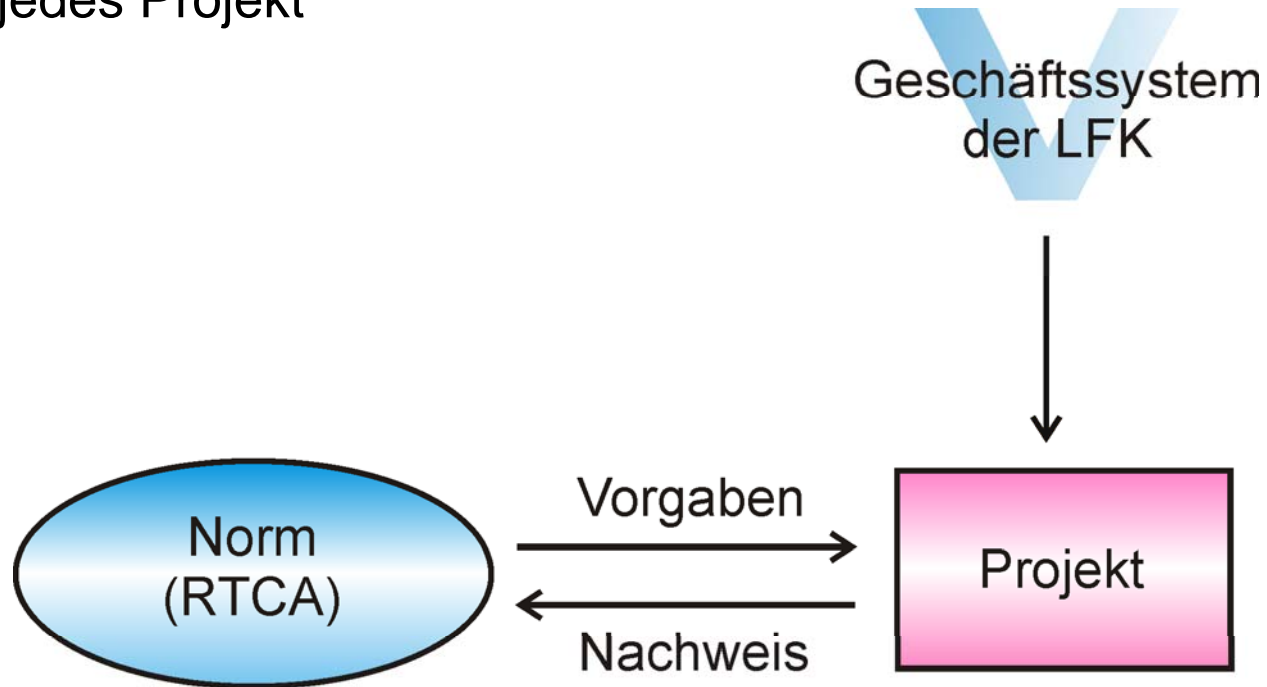
Ausgangspunkt:

- Systemanalyse in SE1/2 stuft Software als sicherheitskritisch ein
- Betrachtet wird Softwareentwicklung SE3-SE7

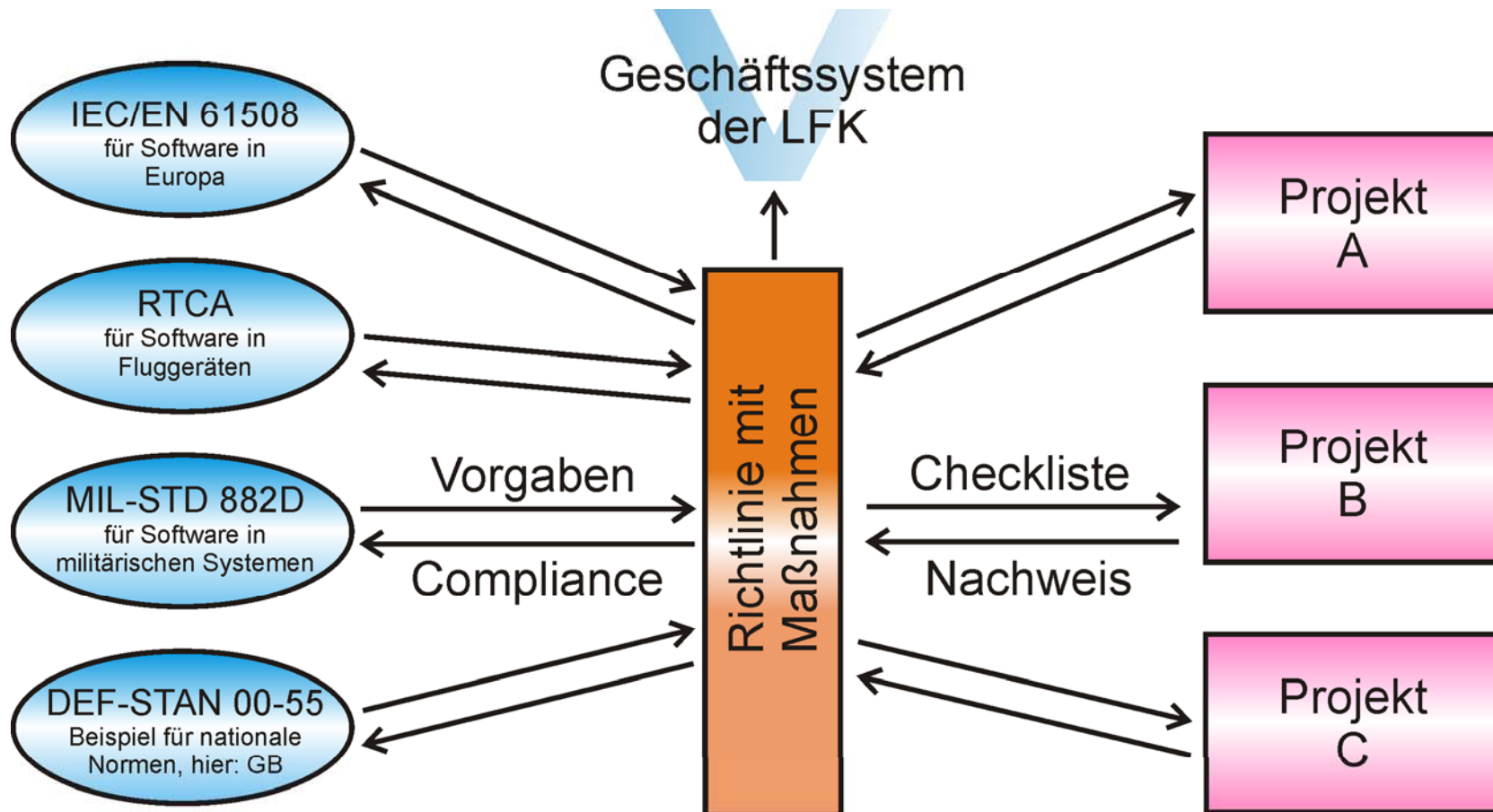
„Was muß ich tun, damit meine Software zertifizierbar wird?“

Bisheriges Vorgehen

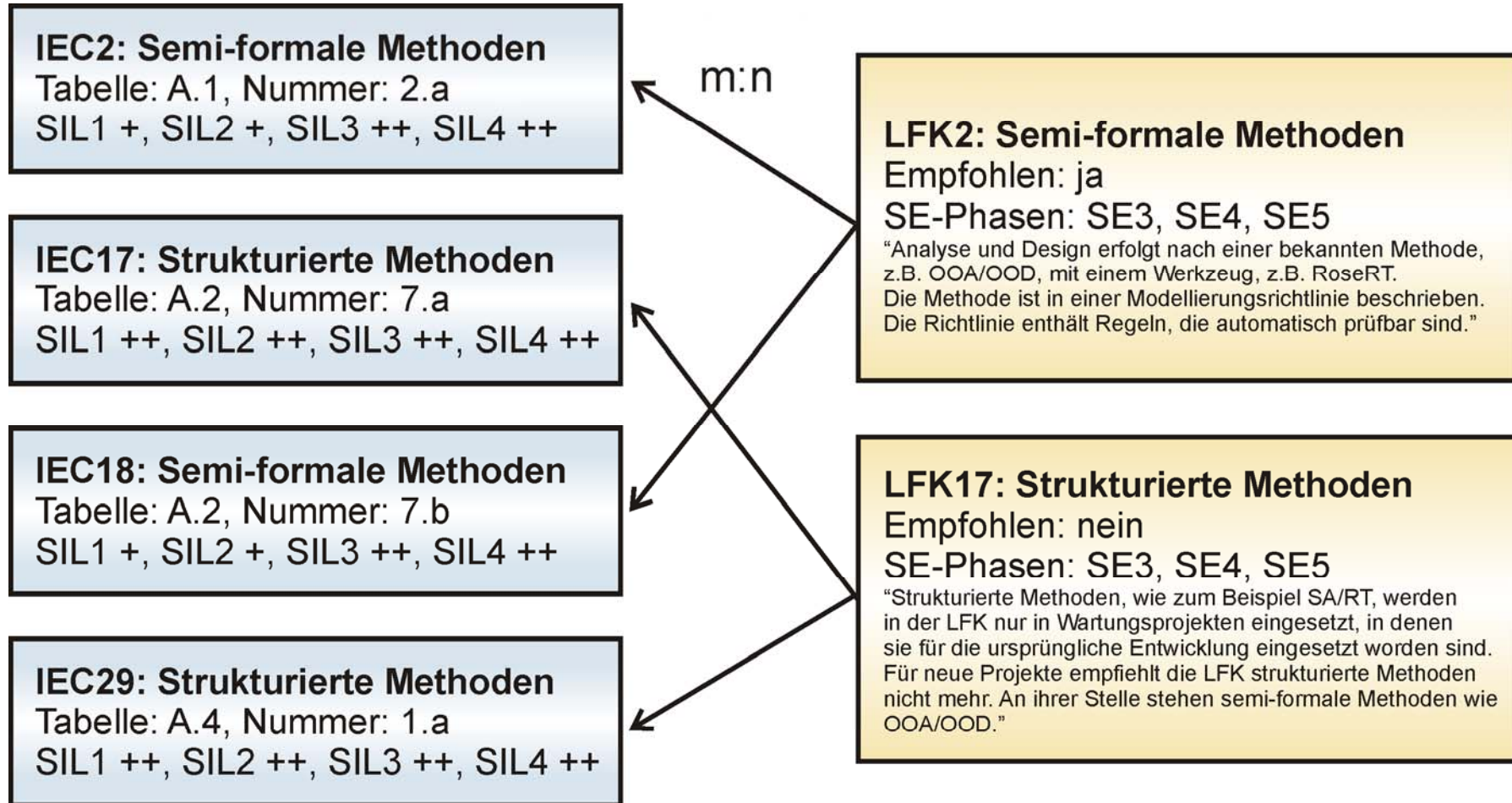
- Für jedes Projekt



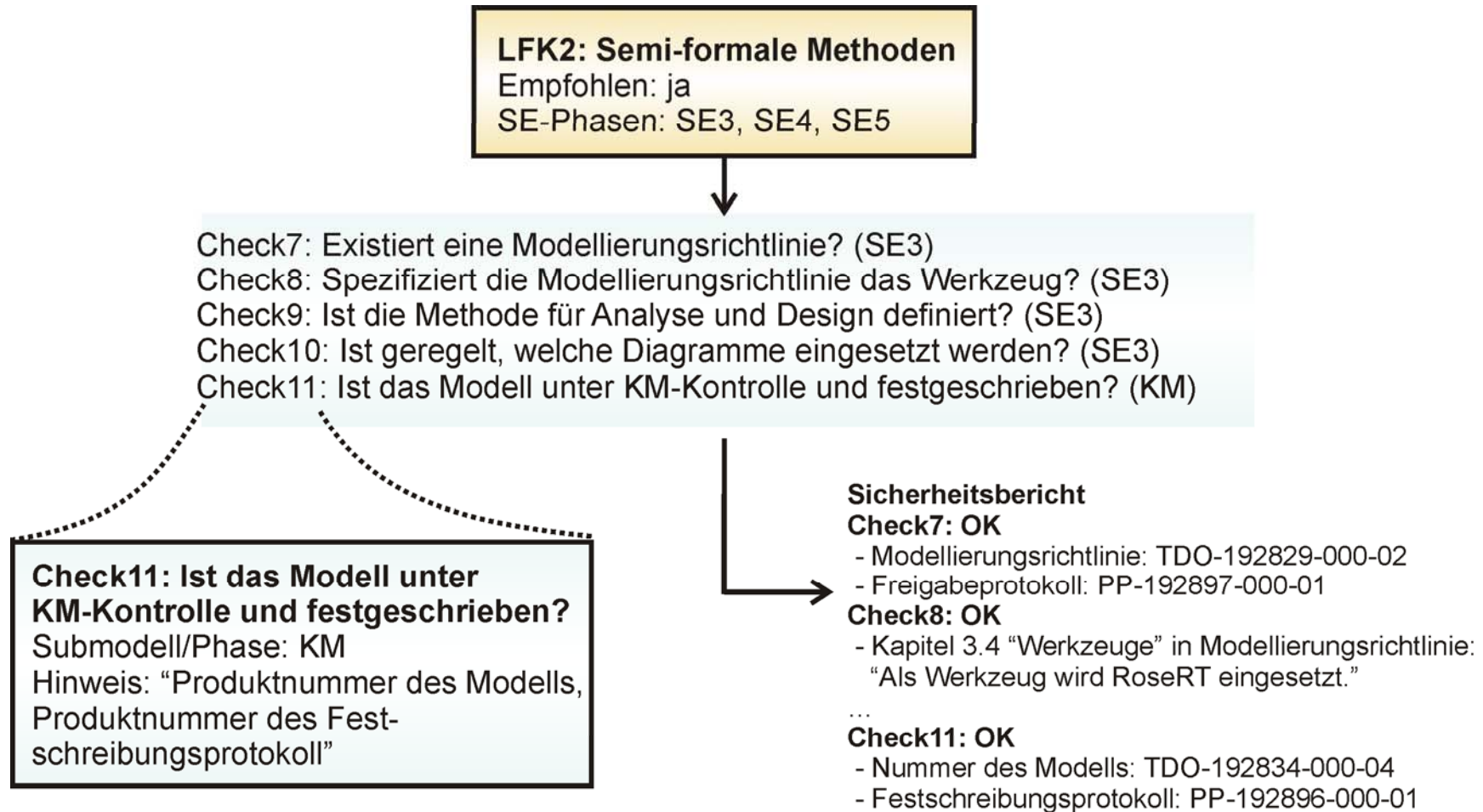
Strategie heute



Compliance zwischen Norm und LFK-Richtlinie



Erfüllung der LFK-Maßnahmen durch das Projekt



Resümee

- Werkzeuggestütztes „Anforderungsmanagement“:
 - Leichtere Verwaltung mehrerer Normen gleichzeitig
 - Sortierbar, filterbar, verknüpfbar
- Nachweis der Norm in zwei Schritten:
 - Allgemein: LFK-Richtlinie bildet Normen ab (Übernahme von empfohlenen Maßnahmen, Begründung bei nicht-empfohlenen Maßnahmen)
 - Projektspezifisch: Checkliste weist Erfüllung der LFK-Maßnahmen nach
- Maßnahmen in der Sprache der Firma:
 - Begriffe aus dem Geschäftssystem der Firma
 - Transparenz und Akzeptanz für Experten und Nicht-Experten
- Zusatzaufwand ermittelbar:
 - V-Modell-Produkte: Hinweis auf notwendige Regelungen
 - Nicht-V-Modell-Produkte explizit gefordert (z.B. Programmierrichtlinie)