Static Model Analysis

Checking Safety Related Functions in Simulink and Stateflow

Safety

Railway: EN 50126, EN 50128, EN 50129

Automotive: ISO 26262

Process industry: IEC 61511

IEC 61508

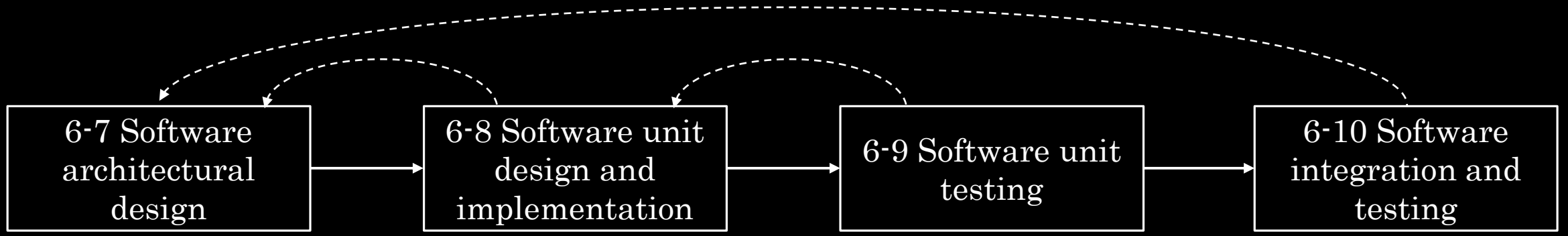
Medical: IEC 62304

Machines: IEC 62061, ISO 13849

Gas Measure Techniques: EN 50271, EN 50402

Automotive

ISO 26262



ISO 26262

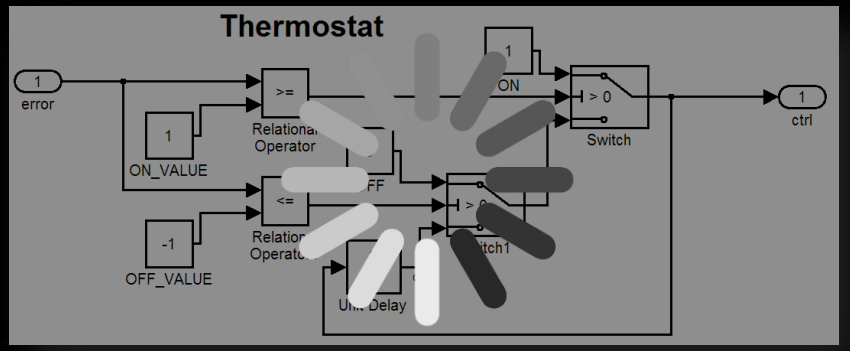
… software units are specified and implemented…
followed by static model verification.

Static Model Verification

Modeling Guidelines

Model Modifications

Check List

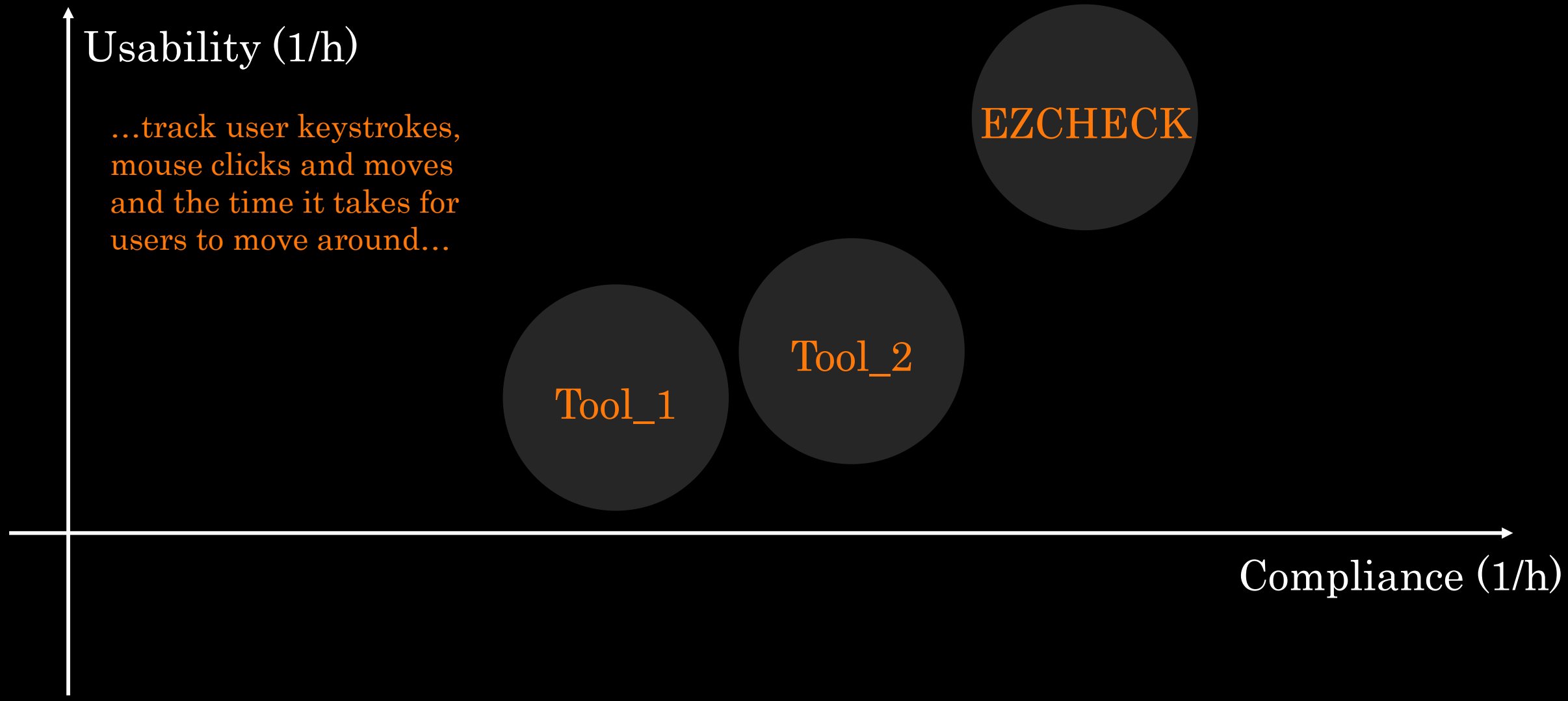


Multiple Iterations

Deviation Procedures

Verification Report

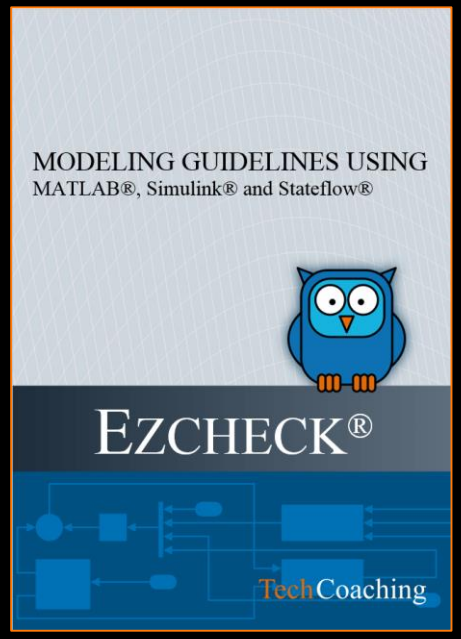
Tool Criteria

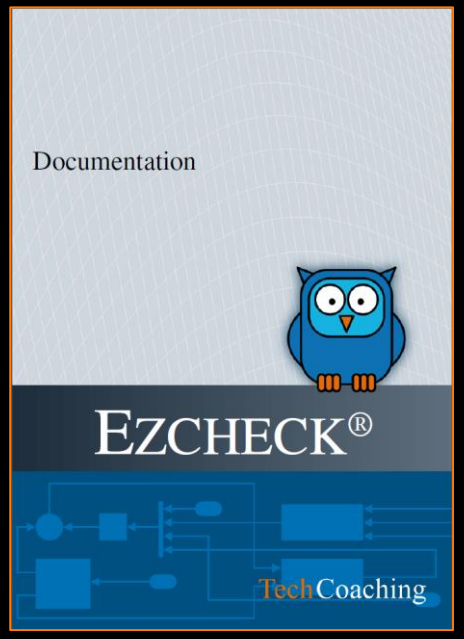


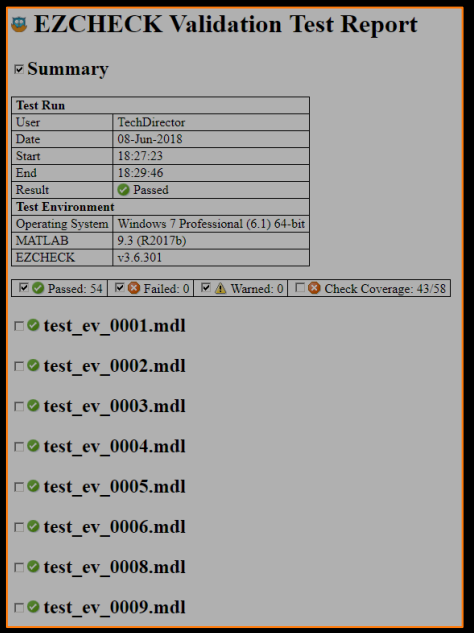
Modeling Guidelines

Methods (ISO 26262-6, 5.4.7 Table 1)		ASIL				Tool Support
		A	B	C	D	
1.1a	Enforcement of low complexity	++	++	++	++	EZCHECK
1.1b	Use of language subsets	++	++	++	++	EZCHECK
1.1c	Enforcement of strong data typing	++	++	++	++	EZCHECK
1.1d	Defensive implementation techniques	o	+	++	++	EZCHECK
1.1e	Use of established design principles	+	+	+	++	EZCHECK
1.1f	Unambiguous graphical representation	+	++	++	++	EZCHECK
1.1g	Use of style guides	+	++	++	++	EZCHECK
1.1h	Use of naming conventions	++	++	++	++	EZCHECK

Tool Qualification Kit







EZCHECK Validation Test Report

Summary

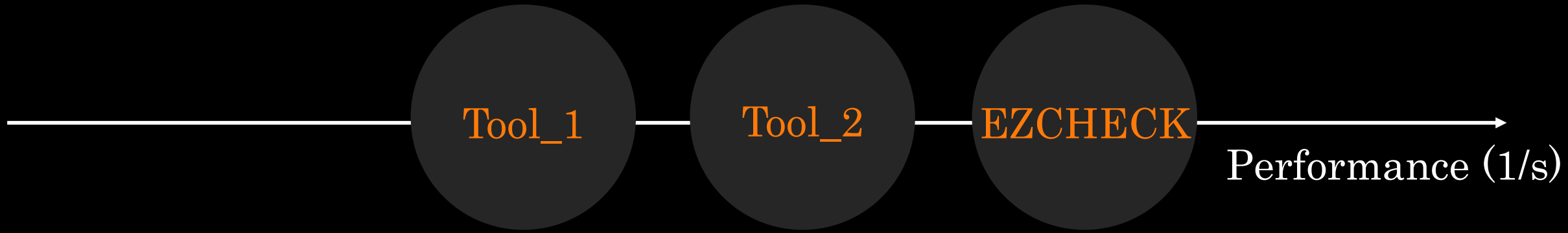
Test Run	
User	TechDirector
Date	08-Jun-2018
Start	18:27:23
End	18:29:46
Result	Passed
Test Environment	
Operating System	Windows 7 Professional (6.1) 64-bit
MATLAB	9.3 (R2017b)
EZCHECK	v3.6.301

Passed: 54 | Failed: 0 | Warned: 0 | Check Coverage: 43/58

- test_ev_0001.mdl
- test_ev_0002.mdl
- test_ev_0003.mdl
- test_ev_0004.mdl
- test_ev_0005.mdl
- test_ev_0006.mdl
- test_ev_0008.mdl
- test_ev_0009.mdl

Compliance Checking

Model (blocks)	Tool_1 (s)	Tool_2 (s)	EZCHECK (s)
AU.. (27)	58	36	8
FA..1 (94)	65	42	15
FA..2 (58)	47	33	16
FA..3 (228)	126	58	30
SO.. (420)	115	31	10
sf_car (32)	92	40	11



Tool Features Summary

- Modeling guidelines for safety related applications
- Qualification kit with validation tests
- Compliance checking for modeling guidelines
- Automated report renaming and relocation
- Automated guideline-based model correction
- Model web view generator with a search capability
- Kontext-based exclusion handling and documentation
- Programmable scripting interface for check automation