SIEMENS
Ingenuity for life

Industrial-Grade DevOps

Balancing Speed with Extreme Quality

Frank Buschmann w/ Joachim Fröhlich, Lars Gelbke, Fei Li, Marc Zeller, Peter Zimmerer
Siemens AG, Corporate Technology

DevOps is state-of-practice in enterprise IT software engineering

Leaders in DevOps experience measurable benefits

SIEMENS
Ingenuity for life

amazon

SAP

NETFLIX

„ **Market attractive product quality[1]**	§ 18% increase in revenue § 19% improvement in product quality and performance
„ **Short time-to-market[1]**	§ 21% reduction of time to market for product innovations
„ **Minimal cost of downtime[2]**	§ 60% decrease of deployment downtime costs per year
„ **IT performance[2]**	§ On demand product deployment § 3x lower deployment failure rate, 24x faster recovery from failure § >2000x shorter lead times for product changes

1) CA Technologies: DevOps: Enterprise Organizations‘ Newest Best Practice, July 2015 2) Puppet 2016 State of DevOps Report

The Digitalization of the industry requires an adoption of DevOps

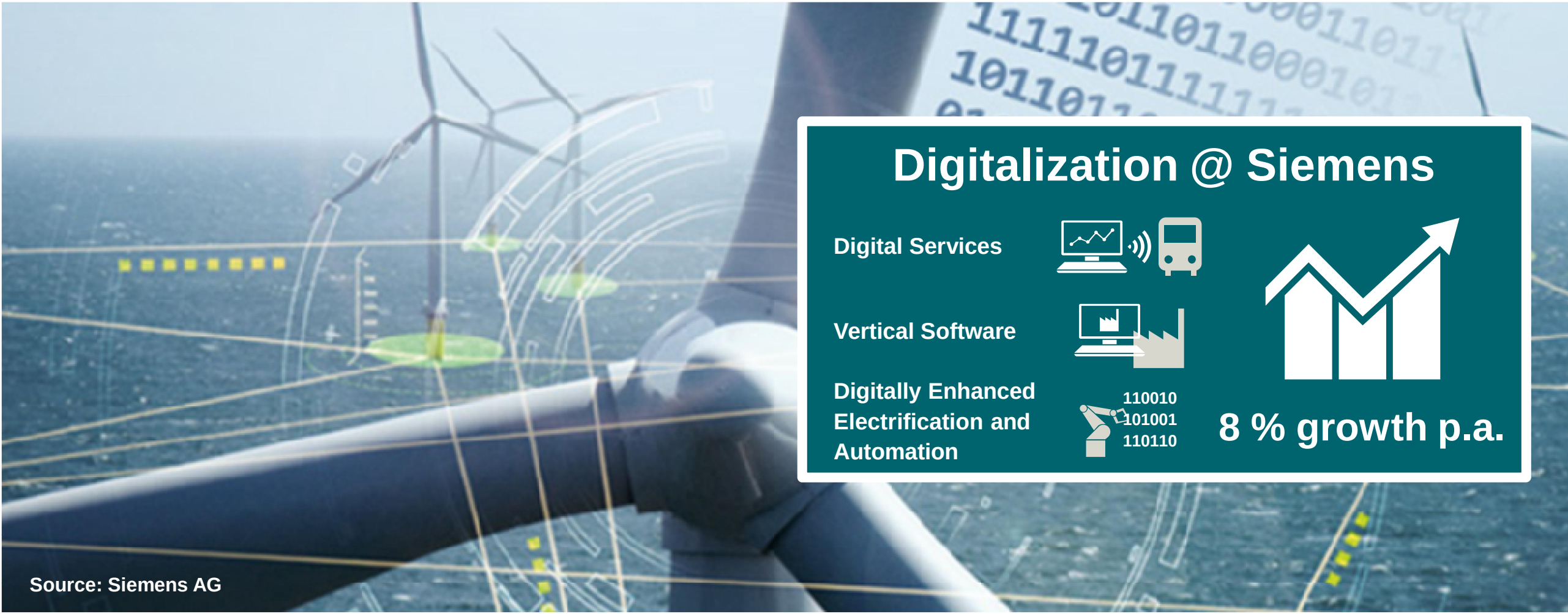
It is the "how" to achieving business agility

SIEMENS
Ingenuity for life

The Digitalization of the industry requires an adoption of DevOps

It is the "how" to achieving business agility

SIEMENS
Ingenuity for life



Yet the adoption of DevOps in industry is challenging

Stringent industry-specific constraints and requirements apply

SIEMENS
Ingenuity for life

Source: Siemens AG

Yet the adoption of DevOps in industry is challenging

Stringent industry-specific constraints and requirements apply

SIEMENS
Ingenuity for life

Source: Siemens AG

Yet the adoption of DevOps in industry is challenging

Stringent industry-specific constraints and requirements apply

SIEMENS
Ingenuity for life

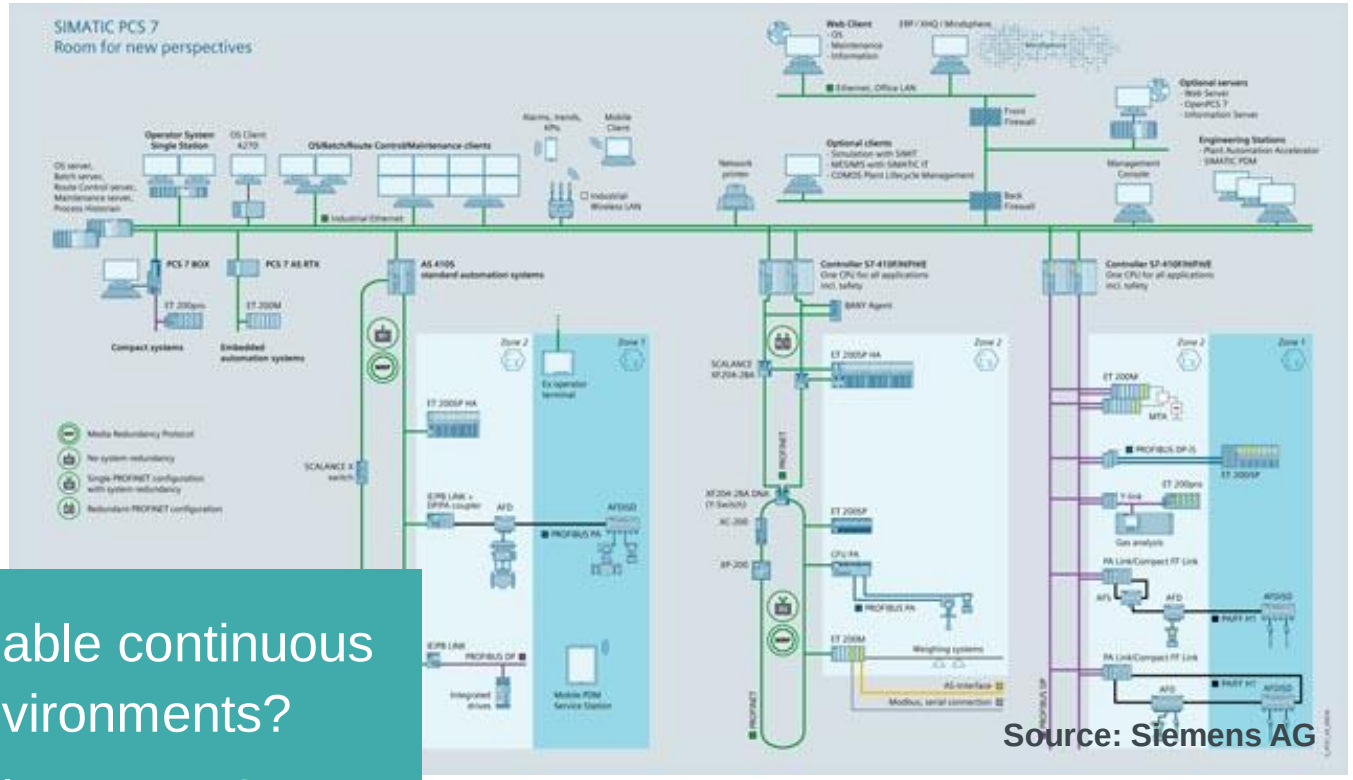
Source: Siemens AG

Ops environment complexity complicates continuous deployment

Operations environments are often polyglot, critical infrastructures

SIEMENS
Ingenuity for life

- „ Multiple IT, OT and field networks
- „ Restricted network access
- „ Multi-platform execution environments
- „ Federated cloud to edge deployments
- „ Flexible deployment demands



Source: Siemens AG

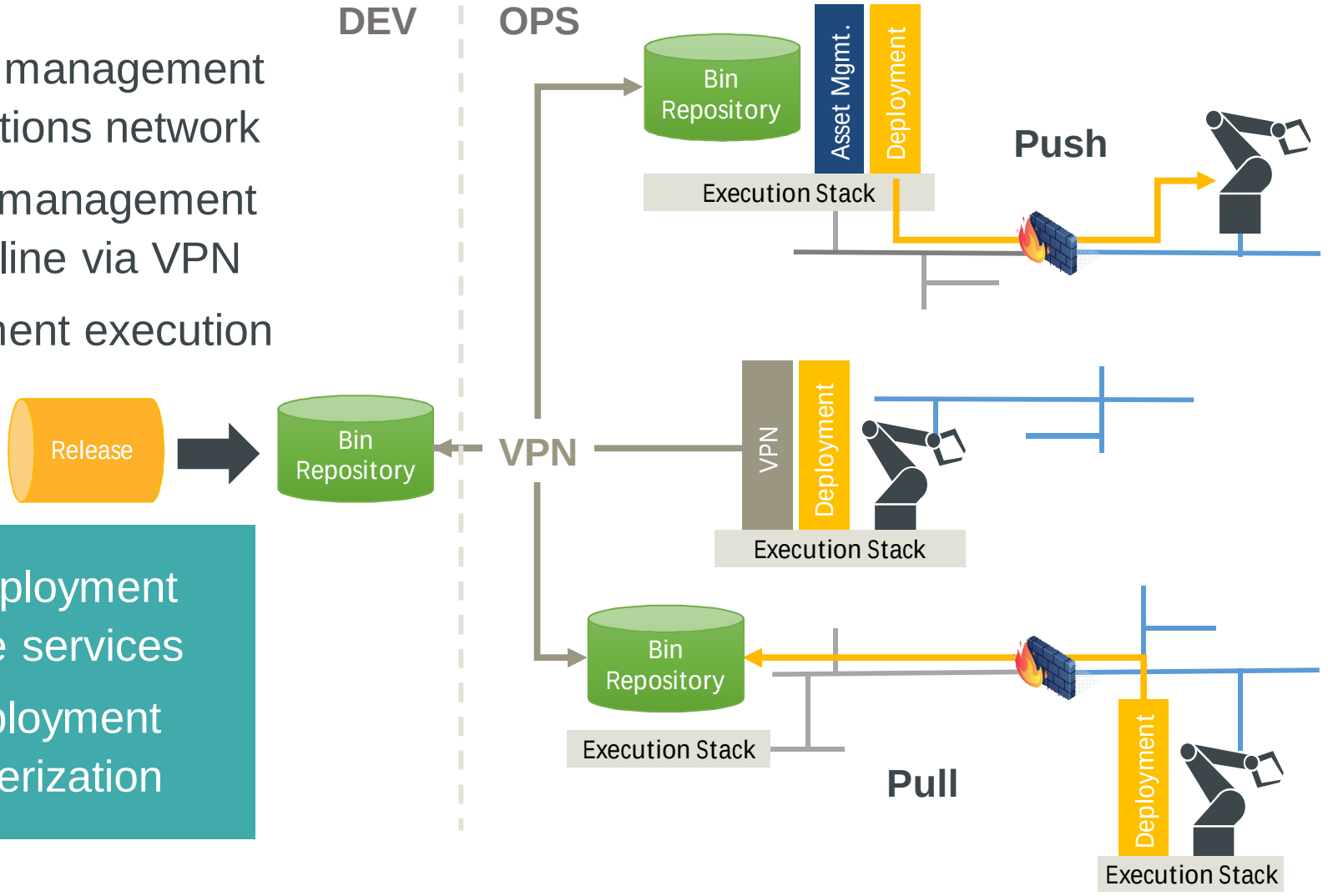
- „ What delivery pipeline architectures enable continuous deployment into industry operations environments?
- „ What technologies support flexible deployment of features to multi-platform execution environments?

Delivery pipelines extend to the field

Centrally managed, federated on-premise deployment infrastructure

SIEMENS
Ingenuity for life

- „ Dedicated (restricted) DevOps management networks per (restricted) operations network
- „ Secure connection of DevOps management networks with the delivery pipeline via VPN
- „ Dedicated on-premise deployment execution stacks per DevOps management network



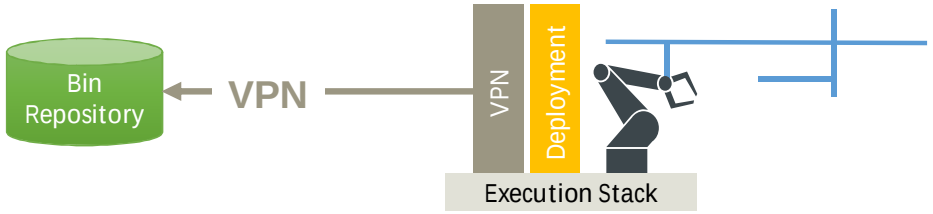
- „ Management of on-premise deployment execution stacks as deployable services
- „ Provisioning of on-premise deployment execution stacks using containerization

Diverse deployment scenarios

No two operations networks are likely to be the same

SIEMENS
Ingenuity for life

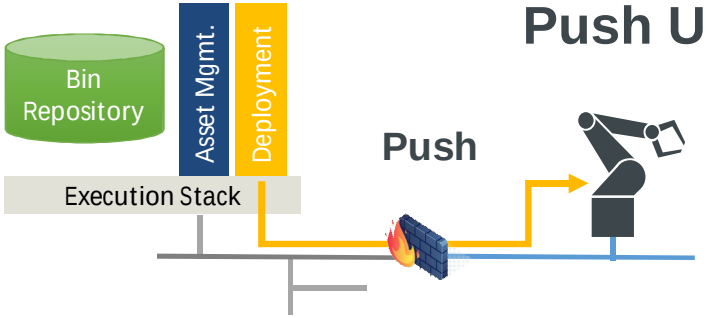
Direct Connection (for open Ops networks)



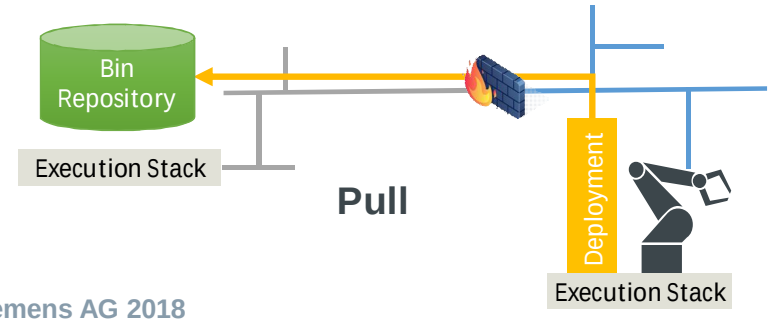
- „ On-premise deployment service directly accesses the main repository via Internet
- „ On-premise deployment service runs on edge device and updates it via feature pull

Push Update

- „ Repository mirror with the latest feature versions
- „ Asset management to orchestrate devices for update
- „ Deployment service updates devices via feature push



Pull Update



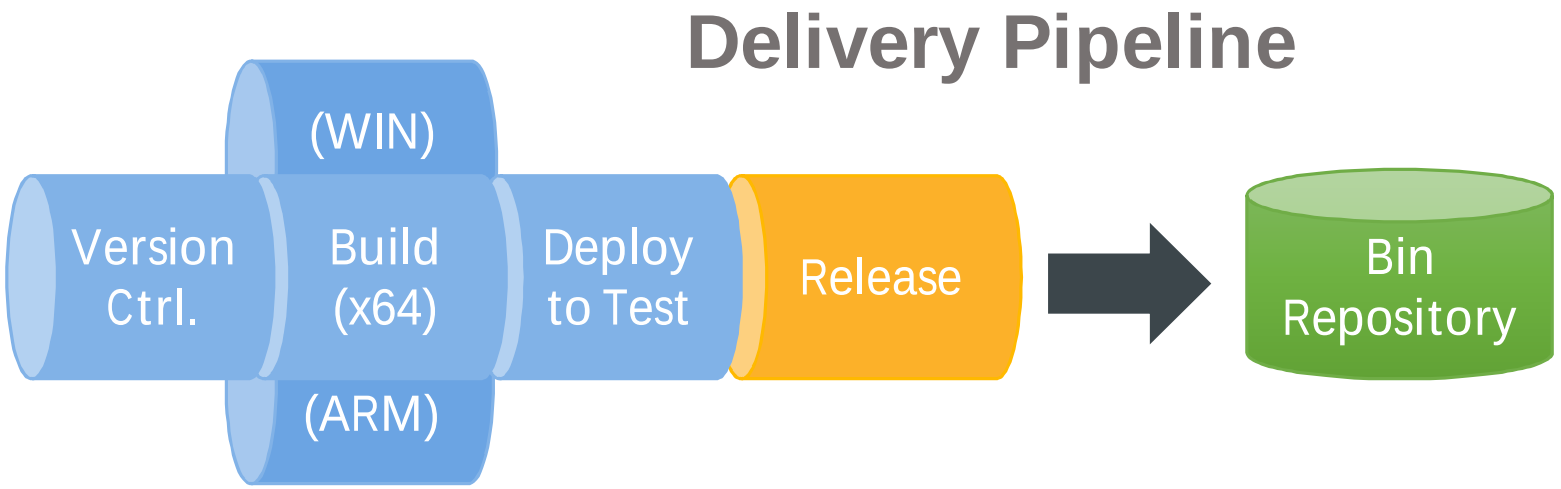
- „ Repository mirror with the latest product features
- „ Deployment service runs on edge device and updates it via feature pull

Delivery pipelines support multi-platform build, test, and release

Parallelization of build, integration and test in virtual, emulated environment

SIEMENS
Ingenuity for life

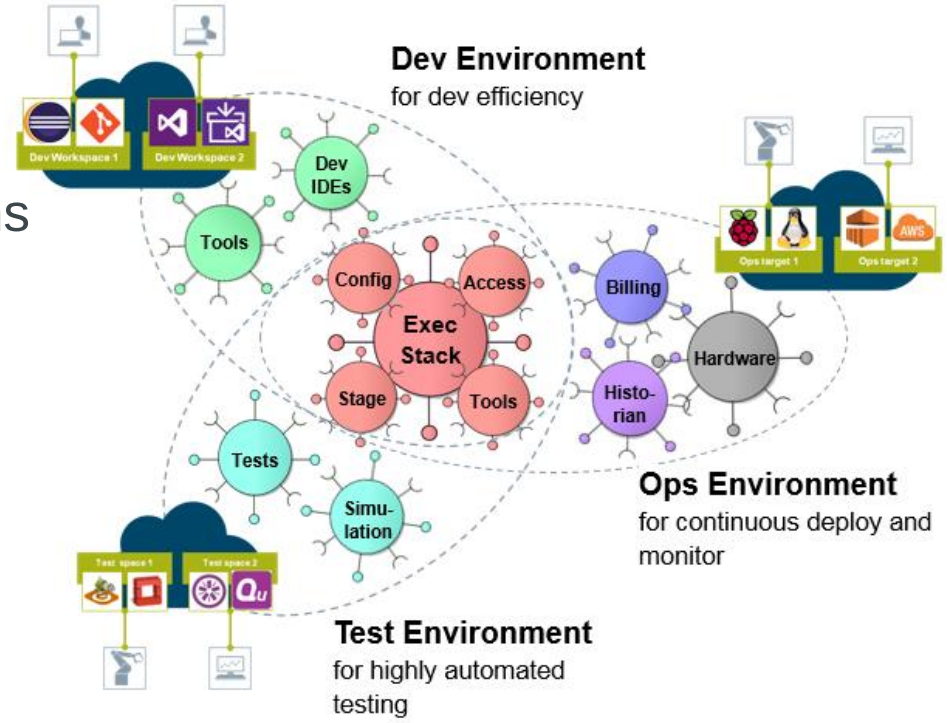
- Versioning and release management strategies for products with flexible deployment demands
- Parallel build stage with dedicated build infrastructure per product execution platform
- Features w/ deployment flexibility packed for all execution environments on which they can run
- Common integration and test stage based on virtualization and emulation
- Repository with images for all deployment platforms available to the deployment service



Environment orchestration in industrial context
Always different, always specific, always something new

SIEMENS
Ingenuity for life

- Leveraging modern orchestration and provision technologies simplify the creation and management of industrial DevOps environments
  - Most state-of-the-art technology need (some) adaption to fulfill industry-specific needs
- Ops environment complexity enforces tailored solutions
  - Single enterprise standard does not work
  - Orchestration requires proper tooling
  - Secure networking required to bridge dev and ops
- “Environment as asset” is a key mindset change!
  - Suggests role and practice extensions in existing scaled agile frameworks, e.g., SAFe



Regulated domains challenge agility and cycle time

Regulatory compliance like functional safety is often mandatory

SIEMENS
Ingenuity for life

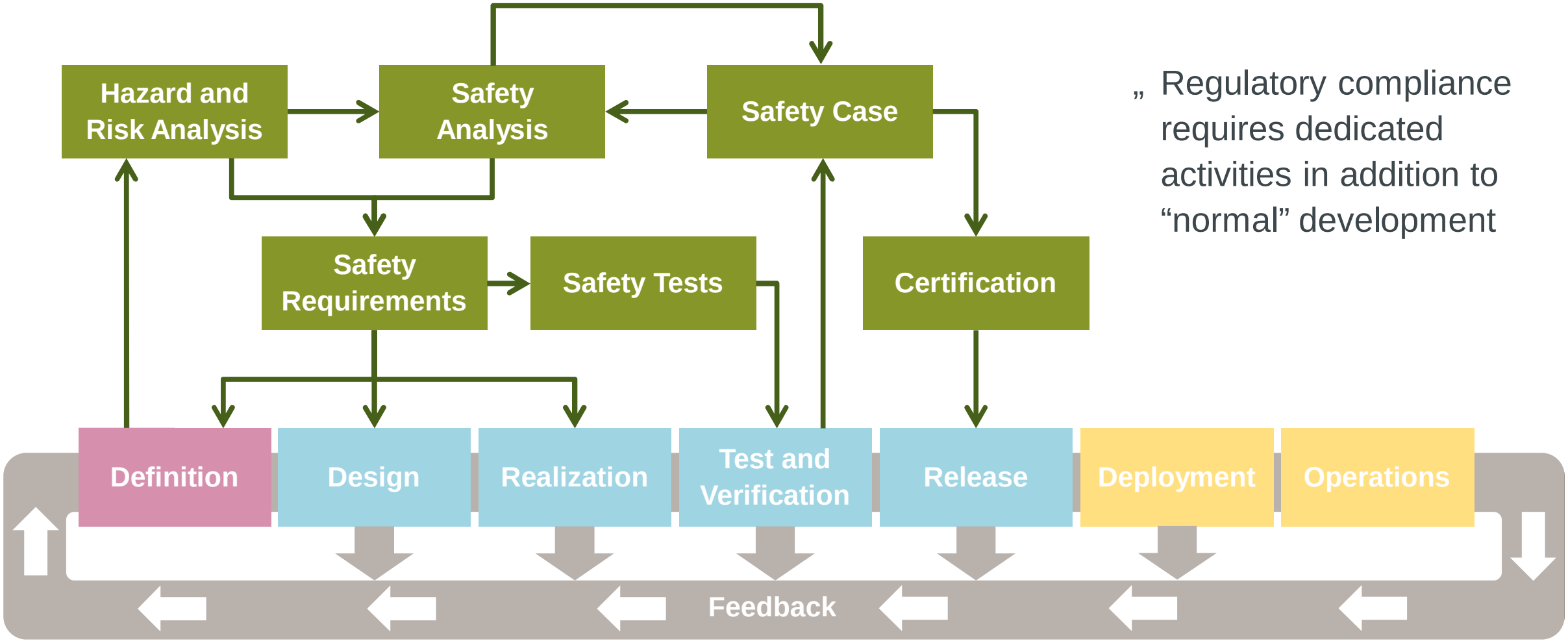
- „ Agility and continuous delivery create high volatility in ensuring regulatory compliance
- „ Current practice is time and effort intense
- „ Cross-cuts multiple engineering disciplines
- „ DevOps environments are subject of certification

- „ What enhancements to agile practices help address regulatory compliance in development fast enough?
- „ What methods and technologies support continuous delivery in the face of regulations and certification?

Safety assurance lifecycle in a nutshell

Strict compliance to (domain-specific) norms is mandatory

SIEMENS
Ingenuity for life



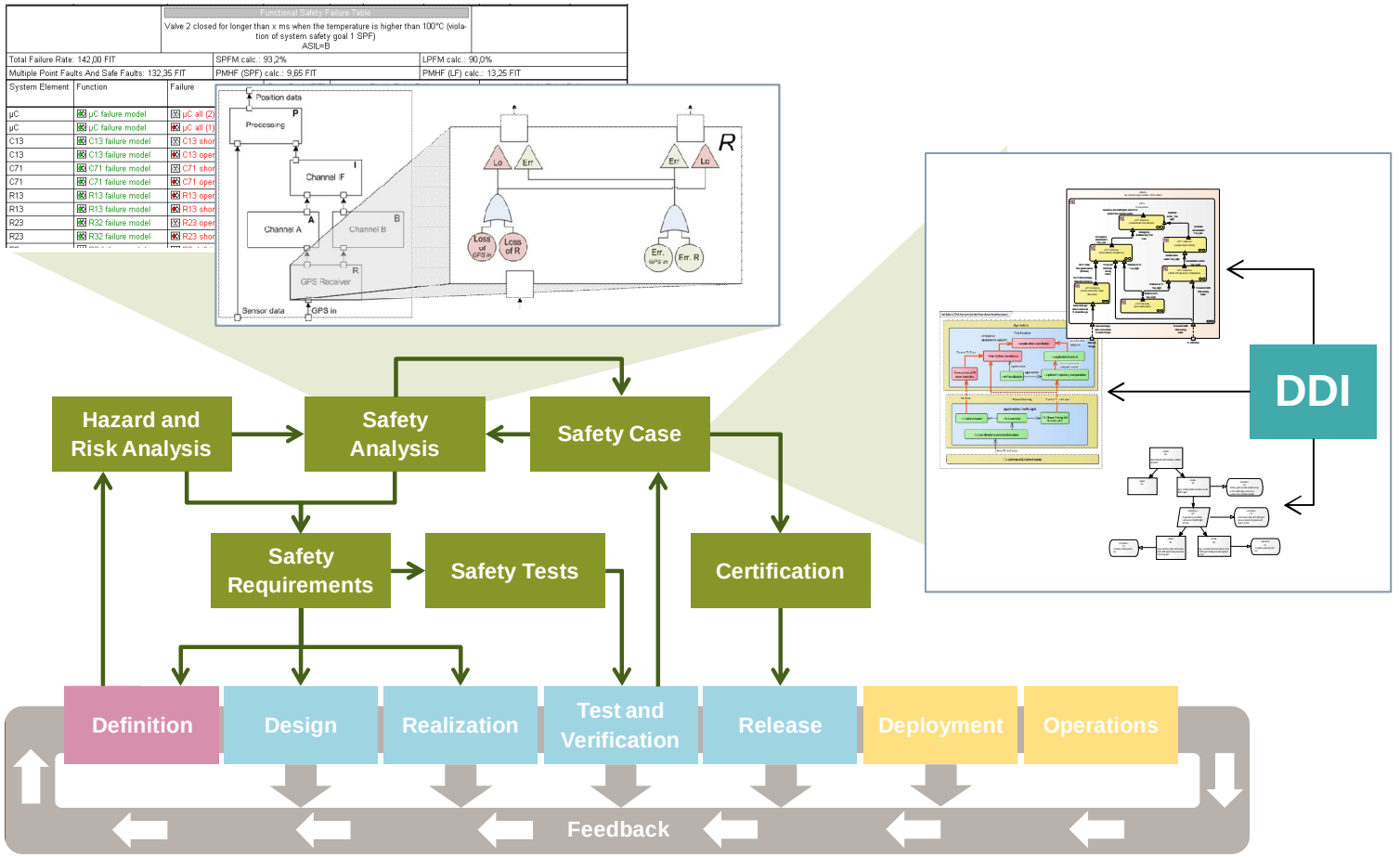
„ Regulatory compliance requires dedicated activities in addition to “normal” development

Methods and technologies for safety assurance are emerging

*Research driven by funded projects on EU and national level**

SIEMENS
Ingenuity for life

- Component Fault Trees (CFT)
- Safety Concept Trees (SCT)
- Conditional Safety Certificates (ConSerts)
- Component-based Failure Mode and Effect Analysis (FMEAexpress)
- Digital Dependability Identities (DDI)



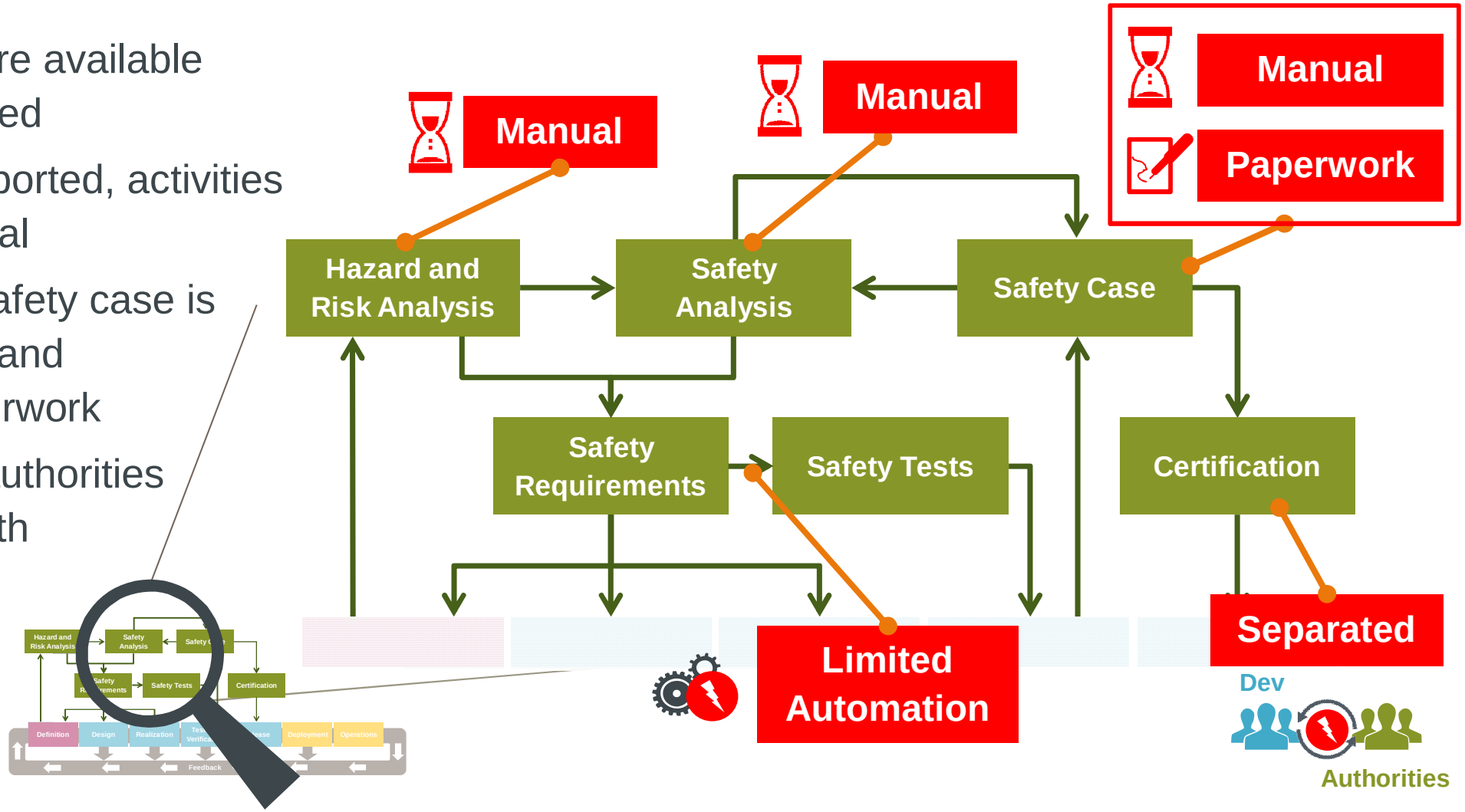
*) EU H2020 project DEIS (Dependability Engineering Innovation for Cyber Physical Systems), national BMBF project CrESt (Collaborative Embedded Systems)

Non-agile culture and limited automation are core challenges

Negative impact on agility and cycle time

SIEMENS
Ingenuity for life

- „ Agile practices are available but rarely practiced
- „ Though tool supported, activities are mostly manual
- „ Compilation of safety case is typically tedious and error-prone paperwork
- „ Certification by authorities not integrated with development

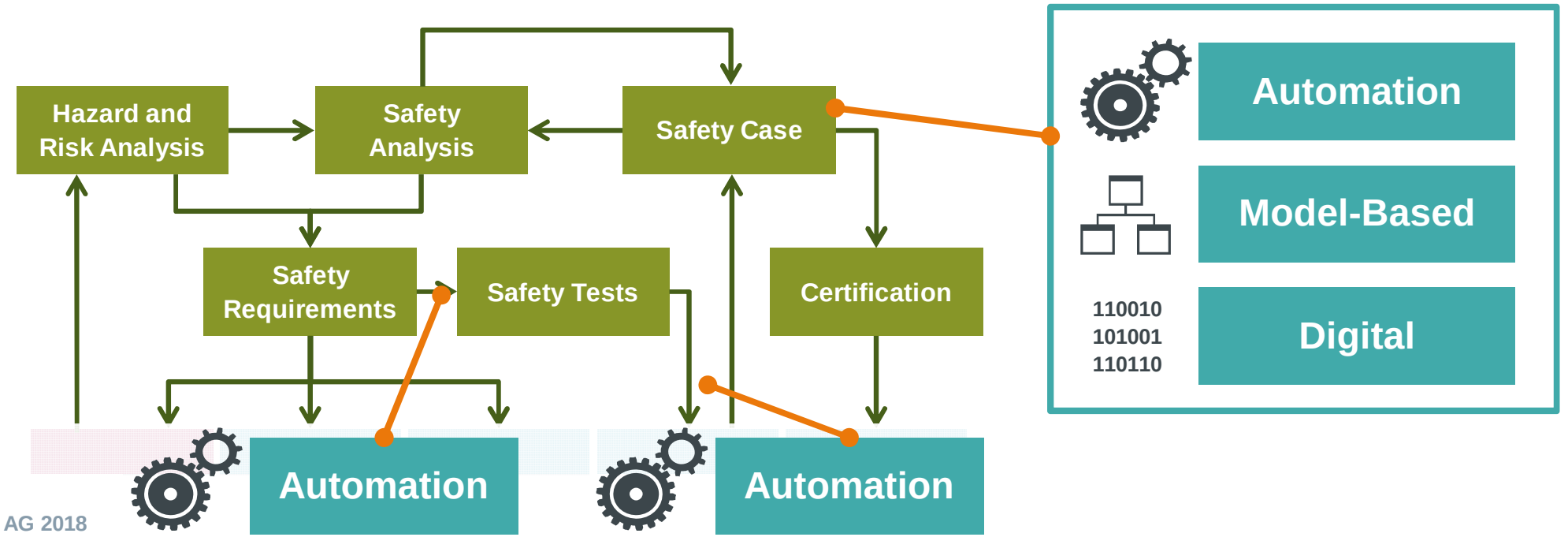


Automation of delivery process is a viable first step

Improves traceability and reduces pre-certification efforts

SIEMENS
Ingenuity for life

- Automatic generation of safety tests from component fault trees (CFTs)
- Integration of safety tests with test automation in delivery pipeline
- Adaptive test and simulation environments with hardware in the loop for test execution
- Automatic generation of safety cases using digital dependability identifiers (DDIs)



Component Fault Trees (CFTs)*

Extend classic fault trees with a component concept

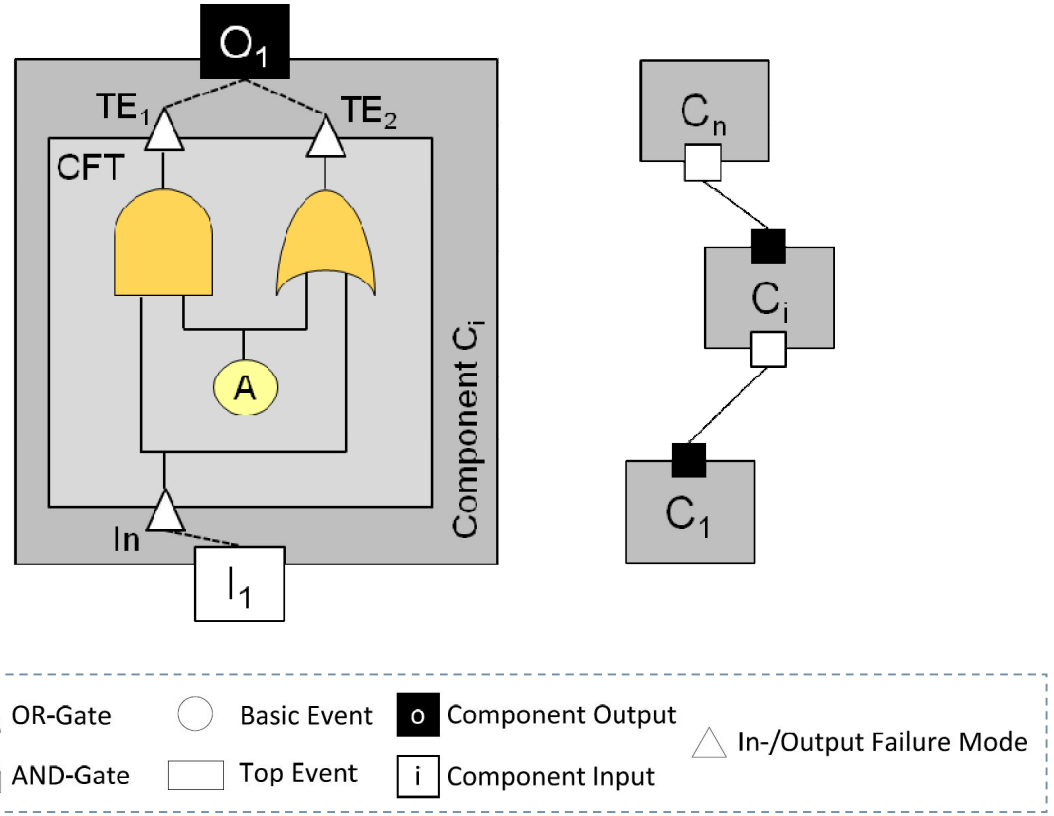
SIEMENS
Ingenuity for life

Extension of classic fault trees with a component concept

- „ Focus of are failure modes of an encapsulated system component
- „ Failures visible at the inport / outport of a component are modeled using Input / Output Failure Modes

Divide-and-conquer strategy for systems

- „ Modular, hierarchical decomposition of system fault trees
- „ Potential reuse of CFTs in other systems



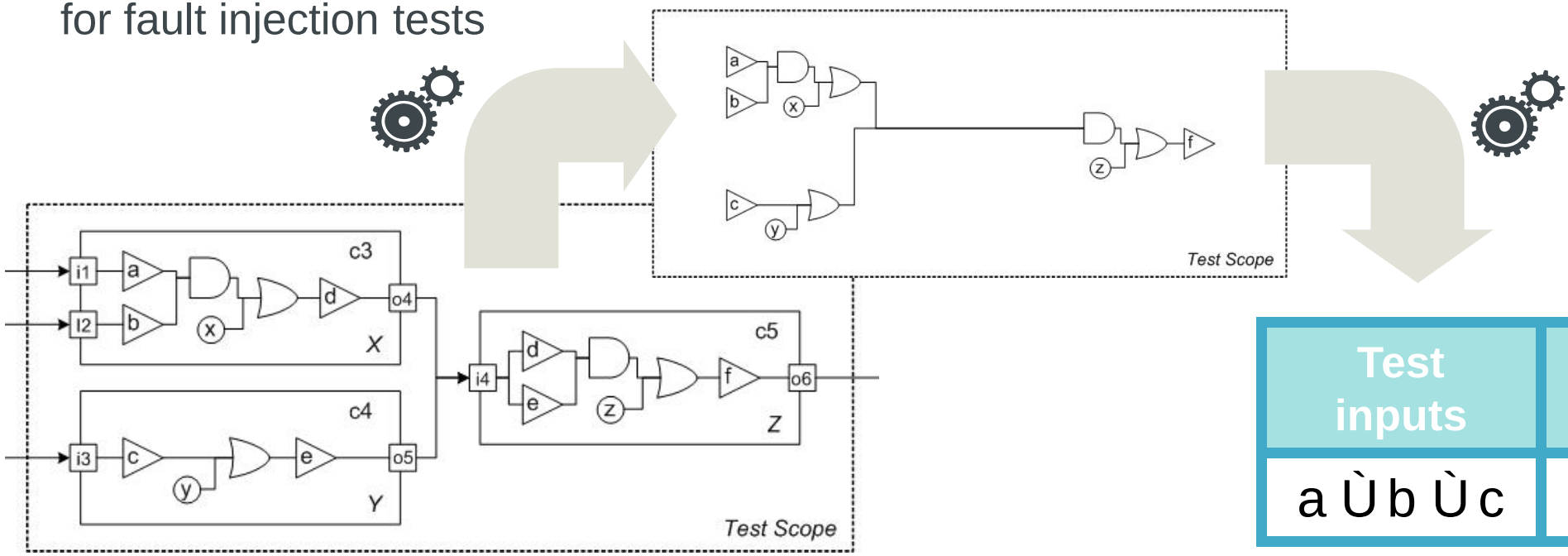
*) Höfig, K., Joanni, A., Zeller, M., Montrone, F., Rothfelder, M., Amarnath, R., Munk, P., Nordmann, A. (2018). Model-based Reliability and Safety: Reducing the complexity of safety analyses using component fault trees, Proceedings of the 2018 Annual Reliability and Maintainability Symposium (RAMS)

Automated Test Case Generation from CFTs

Derive test cases from the failure behavior specification (safety tests)

SIEMENS
Ingenuity for life

- „ Show that in case of failure the implemented behavior is compliant to the specified behavior
- „ Use of test results to verify if safety mechanisms are correctly implemented
- „ Provide inputs and expected outputs for fault injection tests



Test inputs	Expected test outputs
a Ù b Ù c	f

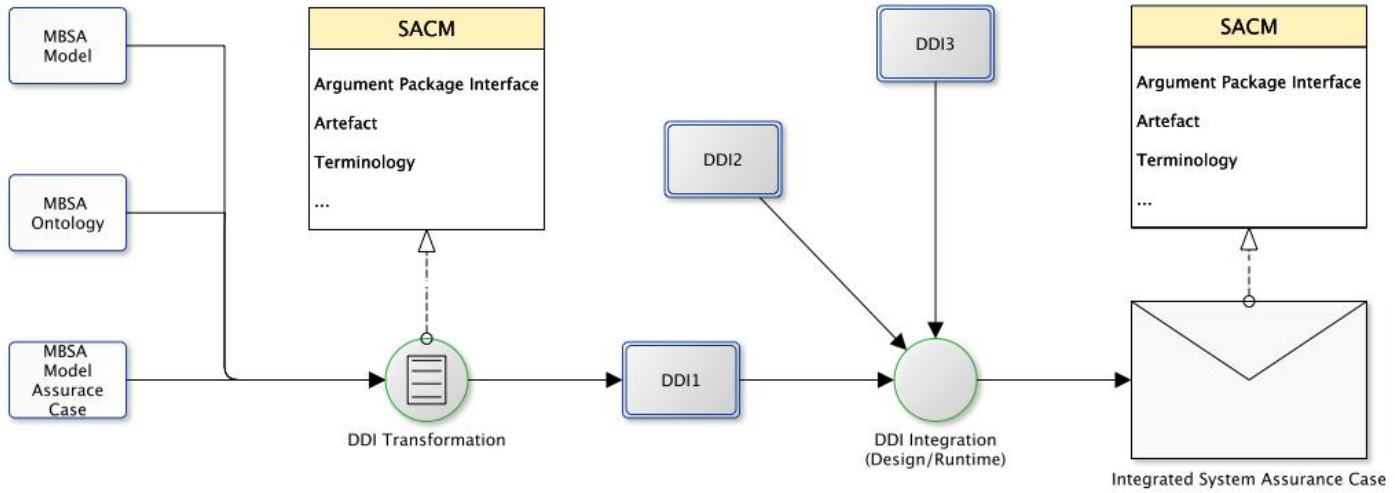
*) Zeller, M., Höfig, K. (2015). CONFeTTI – Component Fault Tree-Based Testing, Proceedings of the 25th European Safety and Reliability Conference (ESREL

Digital Dependability Identity (DDI)*

Ensures interoperability of safety information across organizations

SIEMENS
Ingenuity for life

- Contains all information that uniquely describes the safety characteristics of a system component and its interaction
- Supports encapsulation of model-based descriptions of a system component's safety artifacts
- Provides standardized, machine-readable interfaces to access the safety artifacts
- Component DDIs can be connected to describe safety characteristics of an entire system

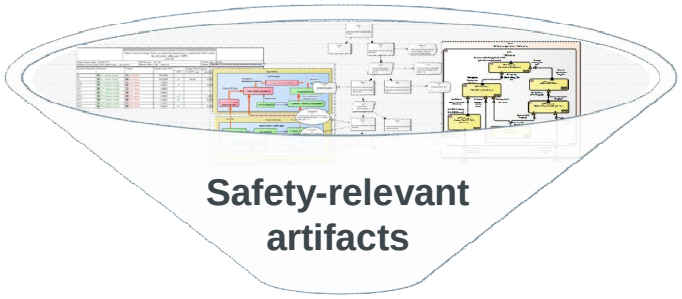


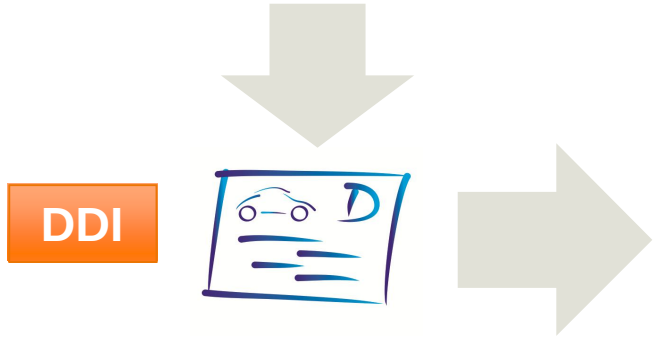
*) Schneider, D.; Trapp, M.; Papadopoulos, Y.; Armengaud, E.; Zeller, M. Höfig, K. WAP: Digital Dependability Identities 2015 IEEE International Symposium on Software Reliability Engineering (ISSRE), 2015, 324-329

Composition of safety cases from DDIs

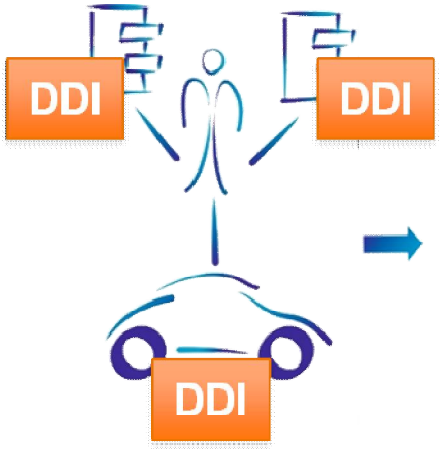
Definition and execution of modular, hierarchical safety cases

SIEMENS
Ingenuity for life

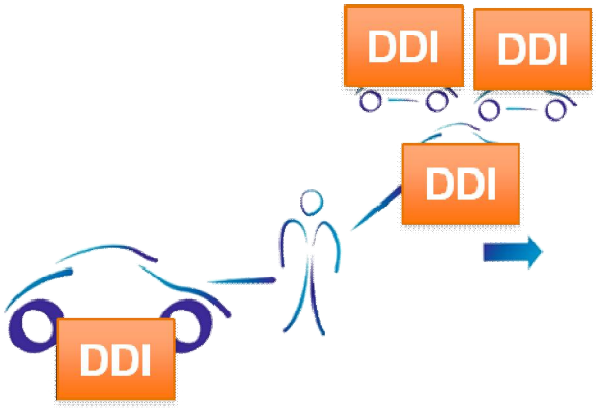




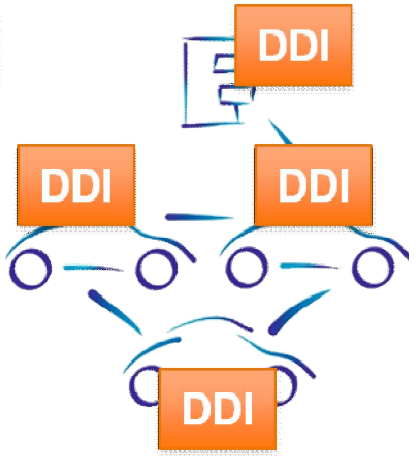
- Continuous and defined extension along the system's lifecycle
- Basis for automatic execution of formal safety tests
- Support for reliable and traceable certification by authorities



Integration at
design time



Integration at
configuration time



Integration at
runtime

Regulated domains challenge agility and cycle time

First steps towards DevOps possible, a long and windy road is still ahead

SIEMENS
Ingenuity for life

- Component Fault Trees (CFT), Conditional Safety Certificates (ConSerts) and Digital Dependability Identities (DDI) are promising technologies to automate the delivery process
  - Design and implementation of adaptive test and simulation environments is a challenge
- Automated delivery process is important, but not sufficient to practice DevOps in regulated domains
- Additional methods and technologies required, e.g., for rapid design, change / impact analysis

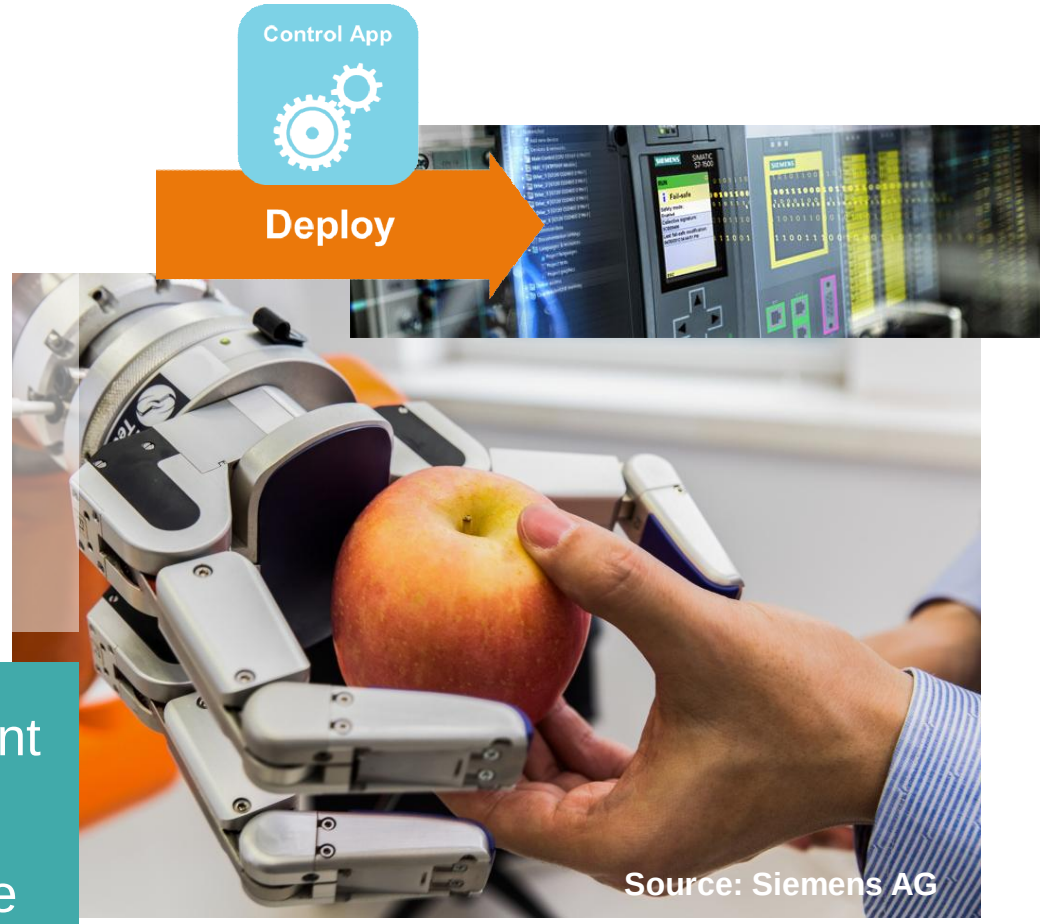
- Agile practices available, but practices do not automatically create culture!
- Certification of tools is a challenge by itself, especially if DevOps environments evolve

Operational quality demands side-effect-free deployment

Correct system behavior, availability and performance must not degrade

SIEMENS
Ingenuity for life

- „ Many systems run 24/7, some with 99.999% availability – especially in Operations and Control
- „ System correctness and (real-time) performance must be guaranteed when needed
- „ Actual configuration may differ from test configuration, e.g., hardware change, exact position of machine



- „ What product designs enable continuous deployment in run and test-in-production without side effects?
- „ What runtime architectures ensure a side-effect-free deployment of features in run?

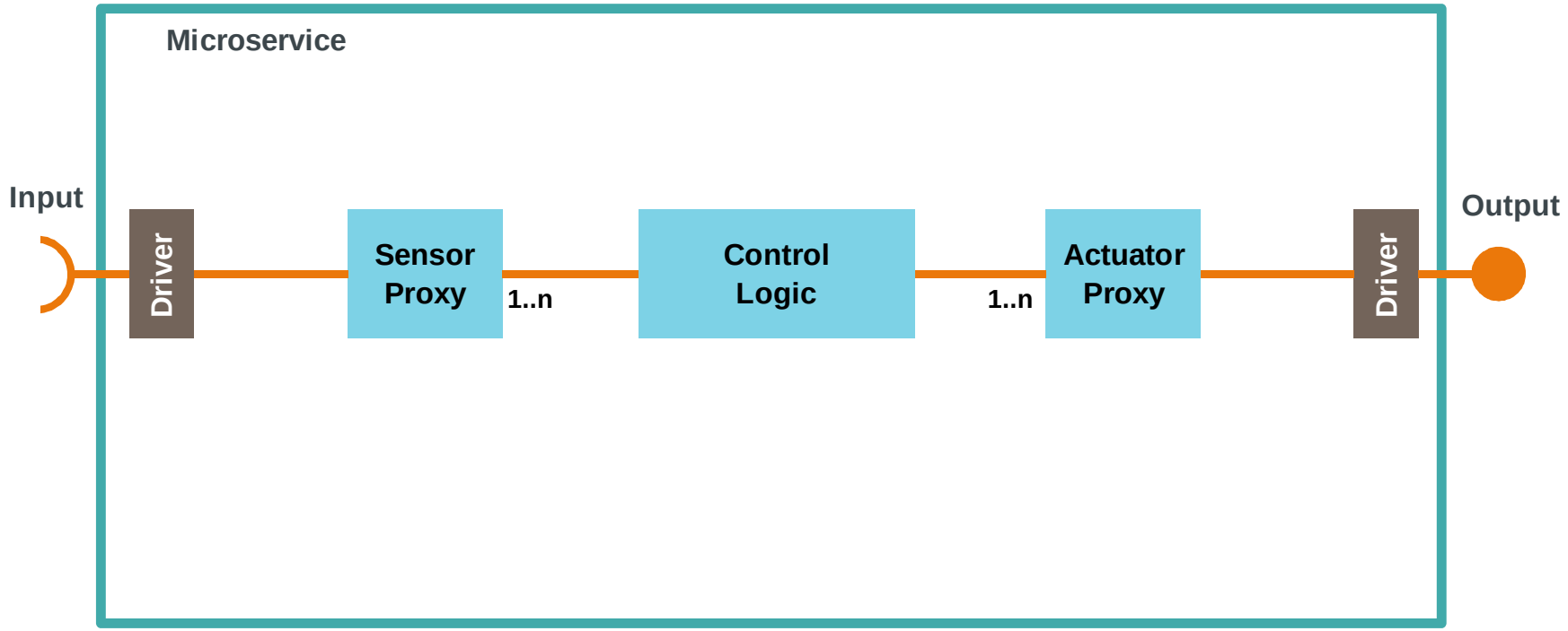
Product features must be prepared for continuous deployment

Design for independence

SIEMENS
Ingenuity for life

„ Realize product features as independent, self-contained Microservices

„ Define and block dedicated time and resource budgets for testing in production

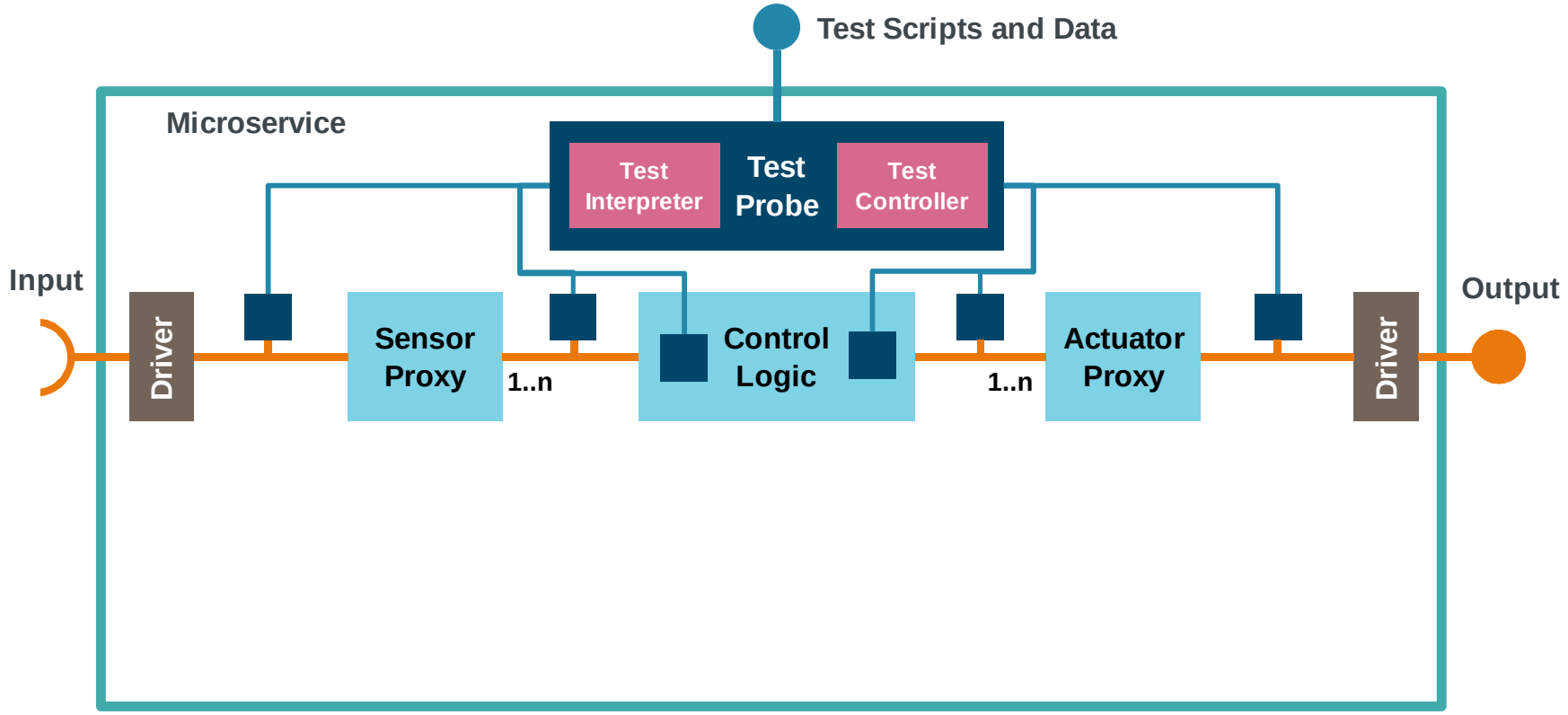


Product features must be prepared for continuous deployment

Design for testability

SIEMENS
Ingenuity for life

„ Integrate a permanent TEST PROBE* to dynamically configure and execute tests in production



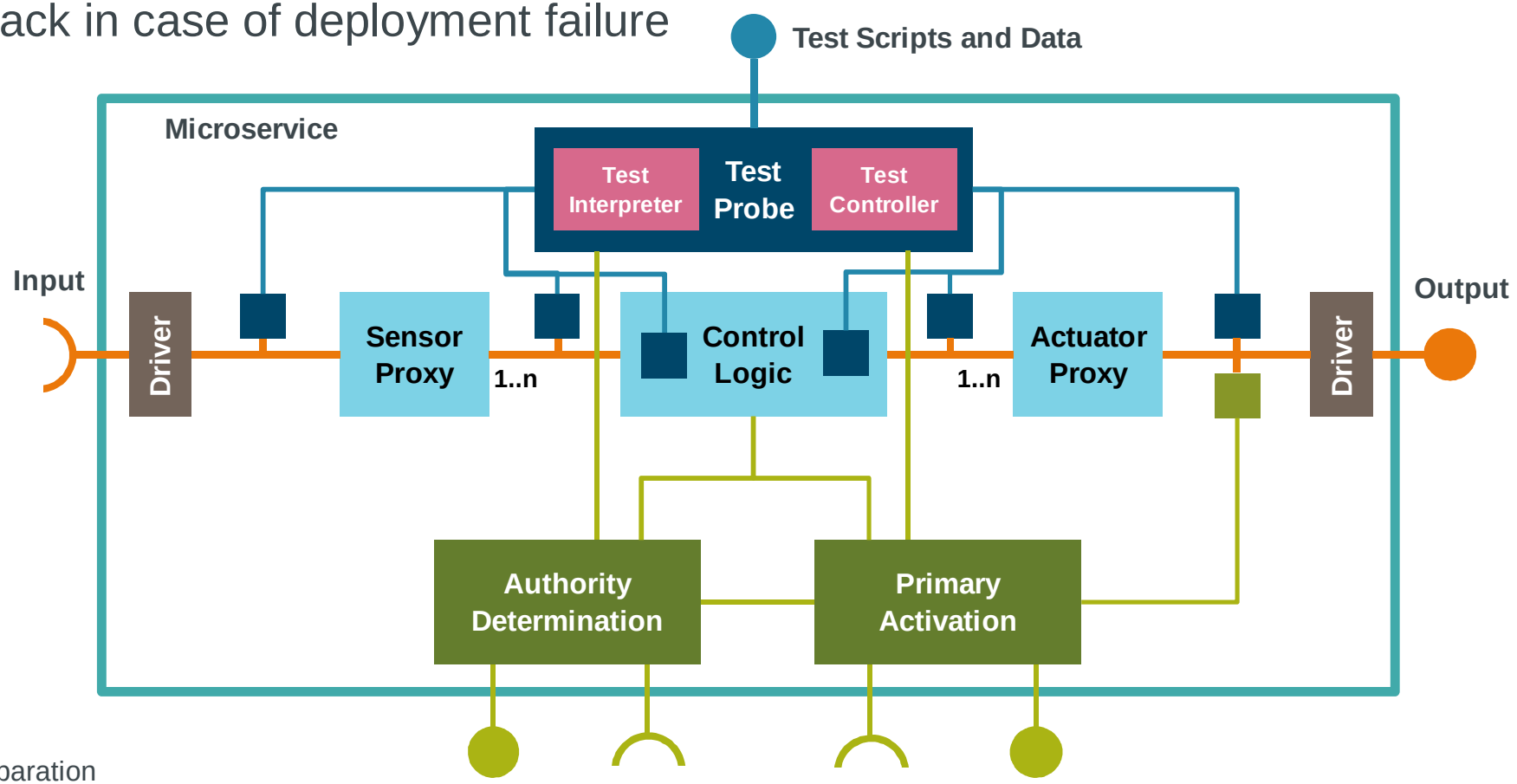
*) F. Li, J. Fröhlich, D. Schall, M. Lachenmayr, C. Stückjürgen, S. Meixner, F. Buschmann: Microservice Patterns for Industrial Edge Applications, EuroPLoP 2018

Product features must be prepared for continuous deployment

Design for availability

SIEMENS
Ingenuity for life

„ Use AUTHORITY DETERMINATION* paired with PRIMARY ACTIVATION* for seamless version switch and fall back in case of deployment failure



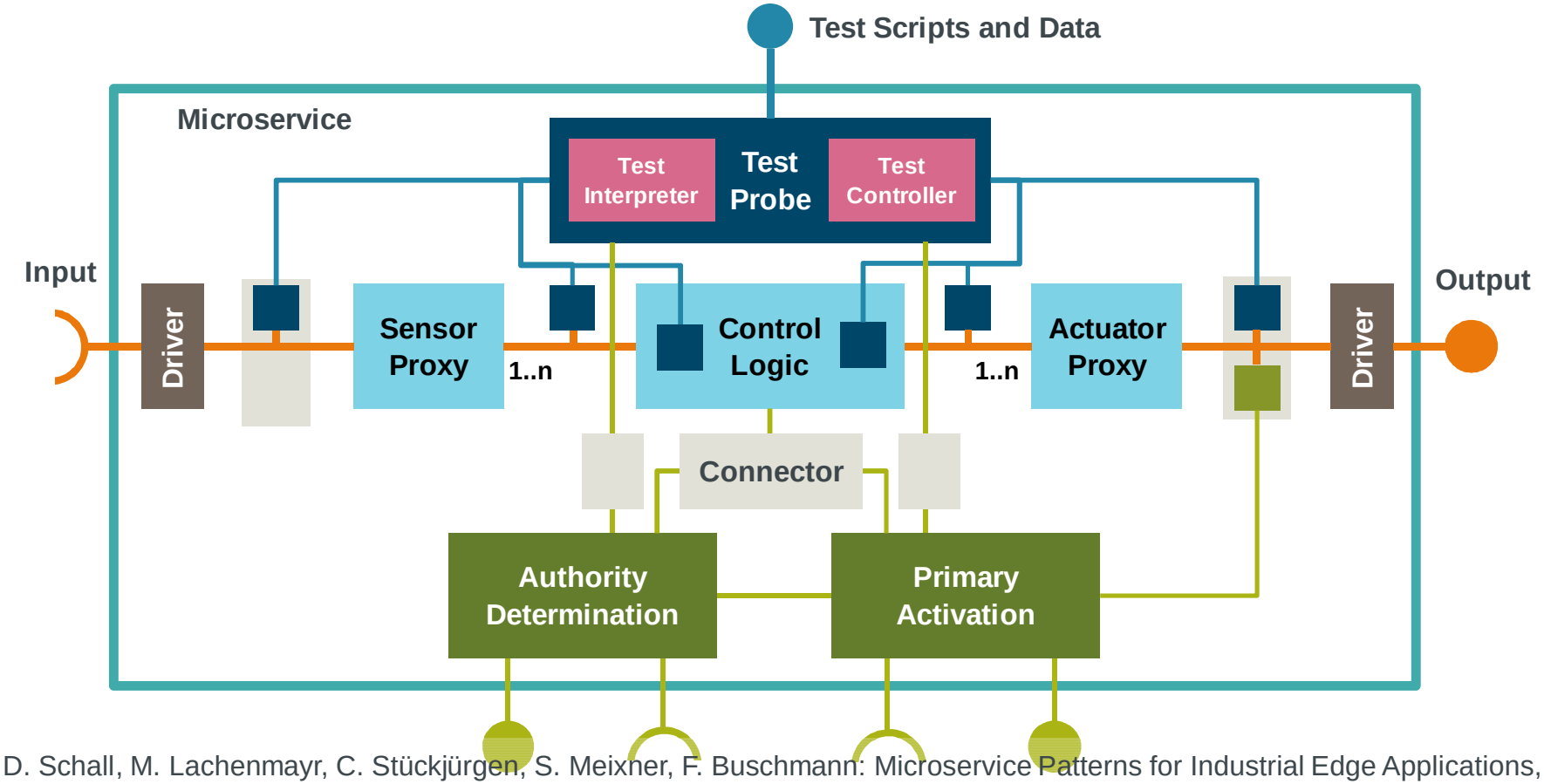
*) Publication in preparation

Product features must be prepared for continuous deployment

Design for availability

SIEMENS
Ingenuity for life

„ Integrate CONNECTORS* to separate domain logic and infrastructure domains from one another



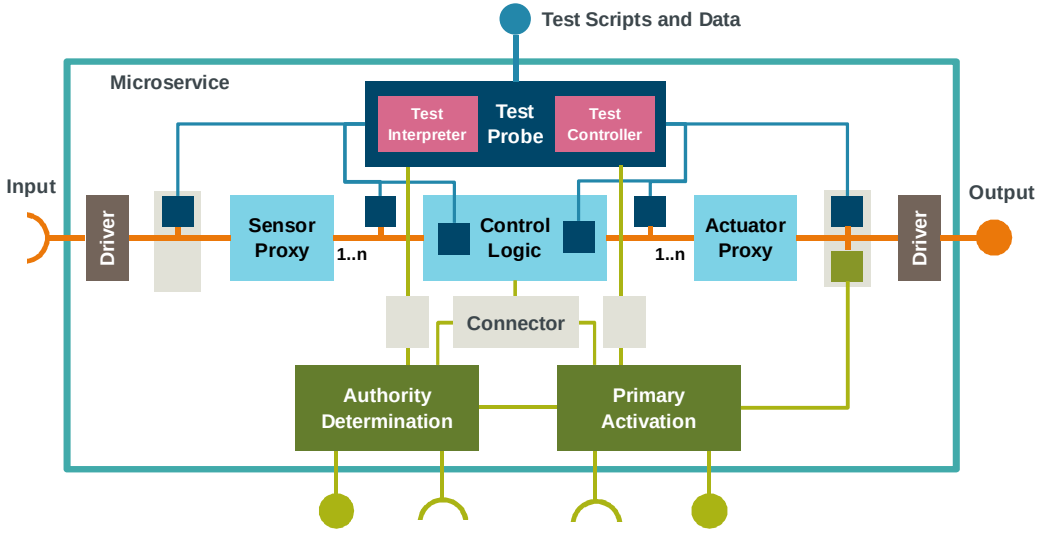
*) F. Li, J. Fröhlich, D. Schall, M. Lachenmayr, C. Stückjürgen, S. Meixner, F. Buschmann: Microservice Patterns for Industrial Edge Applications, EuroPLoP 2018

Product features must be prepared for continuous deployment

Design for independence, testability and availability

SIEMENS
Ingenuity for life

- „ Realize product features as independent, self-contained Microservices
- „ Define and block dedicated time and resource budgets for testing
- „ Integrate a permanent TEST PROBE to dynamically configure and execute tests in production
- „ Use AUTHORITY DETERMINATION paired with PRIMARY ACTIVATION for seamless version switch and fall back in case of deployment failure
- „ Integrate CONNECTORS to separate domain logic and infrastructure domains from one another



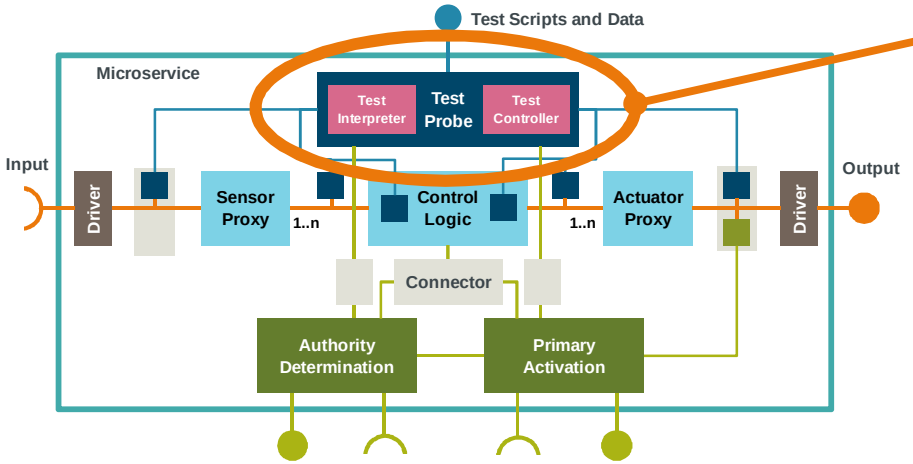
Ensure all timing and resource requirements are met!

Product features must be prepared for continuous deployment

Design for independence, testability and availability

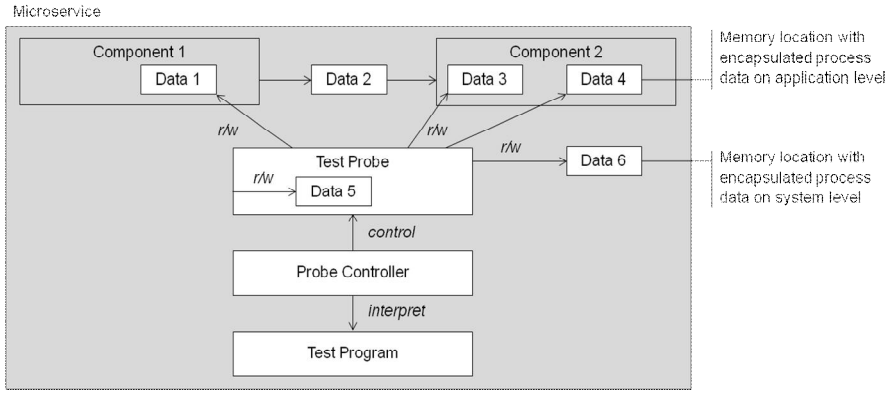
SIEMENS
Ingenuity for life

- „ Design based on “Microservice Patterns for Industrial Edge Applications”
- „ Paper accepted for EuroPLoP 2018*
- „ Patterns integrate well with existing Microservice pattern space, e.g. Microservice.io



How can we enable field tests of an industrial microservice to access internal process data, possibly distributed across several, internal components, without impairing the real-time behavior of the microservice under test?

Build a TEST PROBE permanently into each microservice. Encapsulate testable process data. Make the TEST PROBE programmable, so that test programs can exactly control read and write accesses to testable process data. Let microservices treat TEST PROBES as ordinary components with reserved and limited system resources, so that test programs cannot accidentally change the microservice behavior



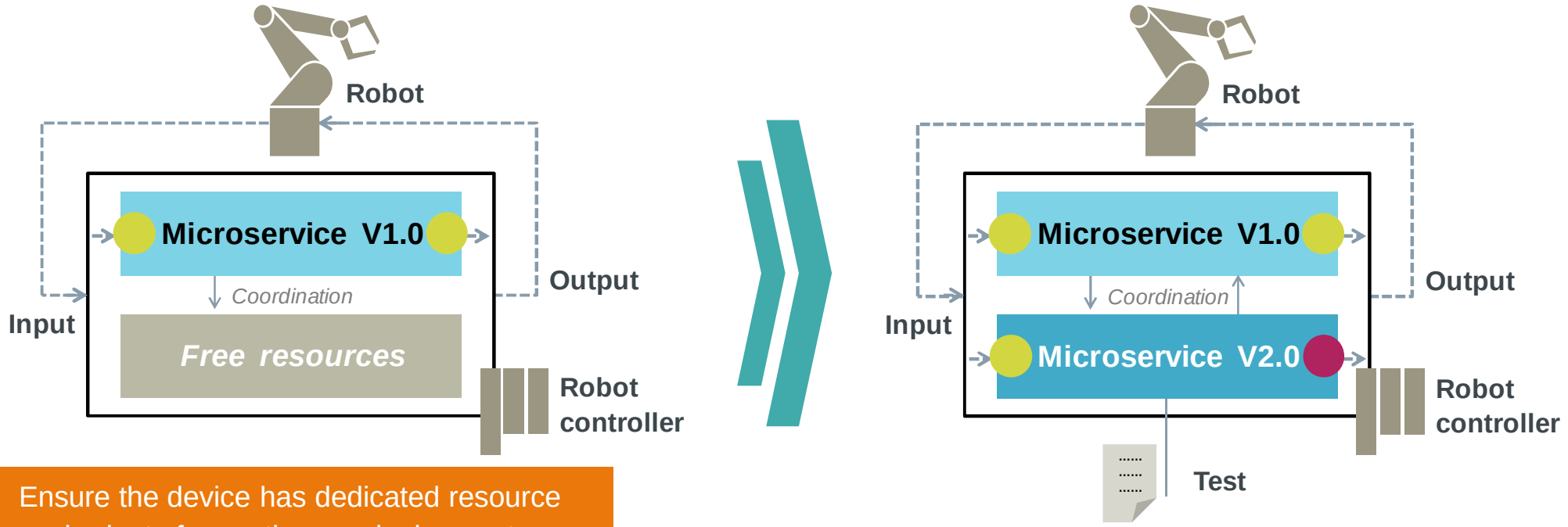
*) F. Li, J. Fröhlich, D. Schall, M. Lachenmayr, C. Stückjürgen, S. Meixner, F. Buschmann: Microservice Patterns for Industrial Edge Applications, EuroPLoP 2018

Deployment architecture must support zero downtime

Design for test in production

SIEMENS
Ingenuity for life

- Deploy new microservice version, connect it with the availability infrastructure of the current version, let it receive input but “mute” is output
- Execute pre-activation tests on the new microservice version via its TEST PROBE



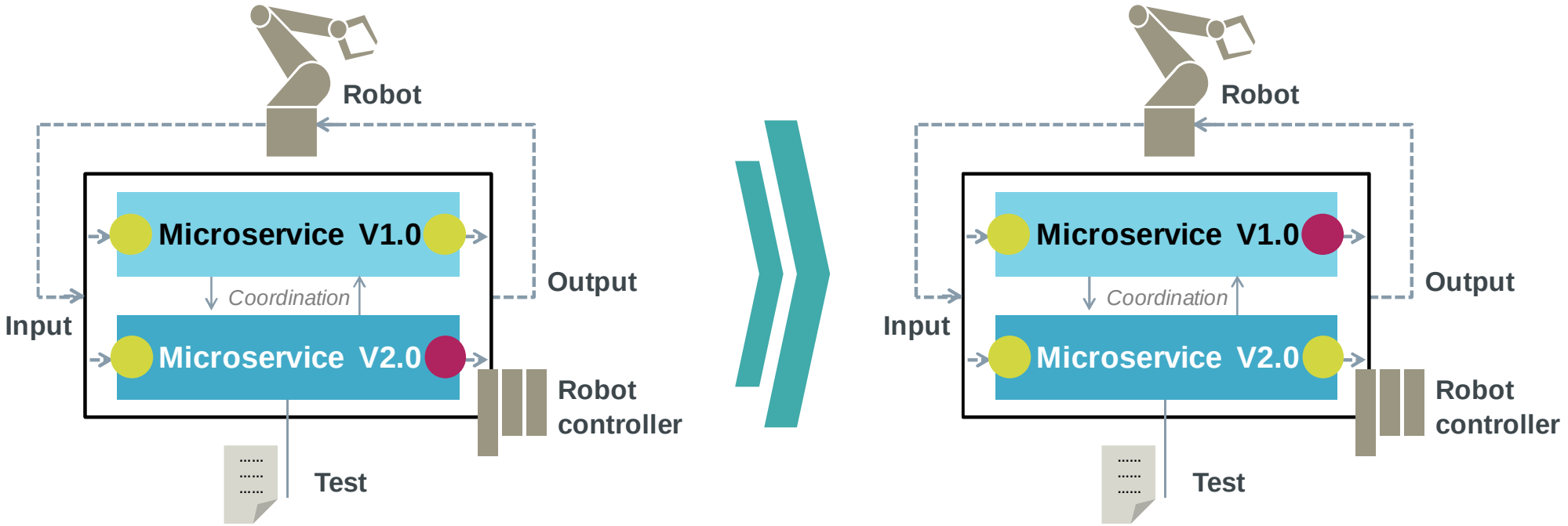
Ensure the device has dedicated resource budgets for continuous deployment

Deployment architecture must support zero downtime

Design for seamless activation

SIEMENS
Ingenuity for life

- „ Notify the AUTHORITY DETERMINATION infrastructure to determine the new primary
- „ Let the PRIMARY ACTIVATION infrastructure activate the new microservice version when seamless switch-over is possible



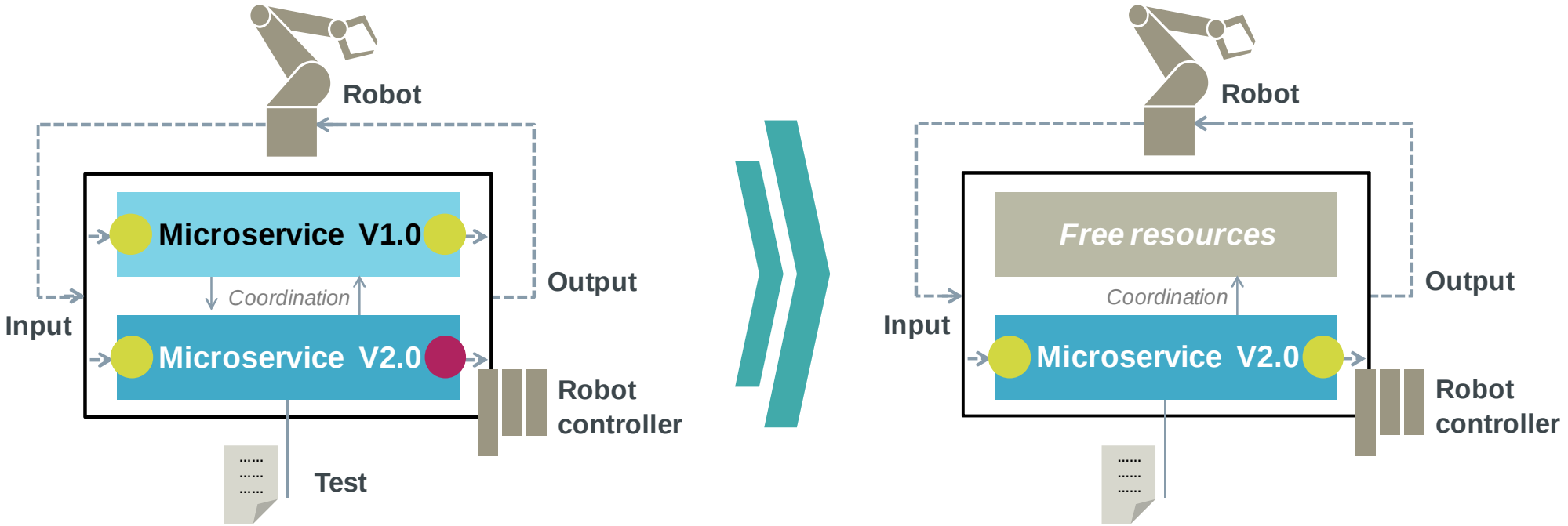
Deployment architecture must support zero downtime

Design for fail-over

SIEMENS
Ingenuity for life

„ Continuously test the new microservice version in production via its TEST PROBE

„ Fall back to old microservice version in case of problems, otherwise uninstall it

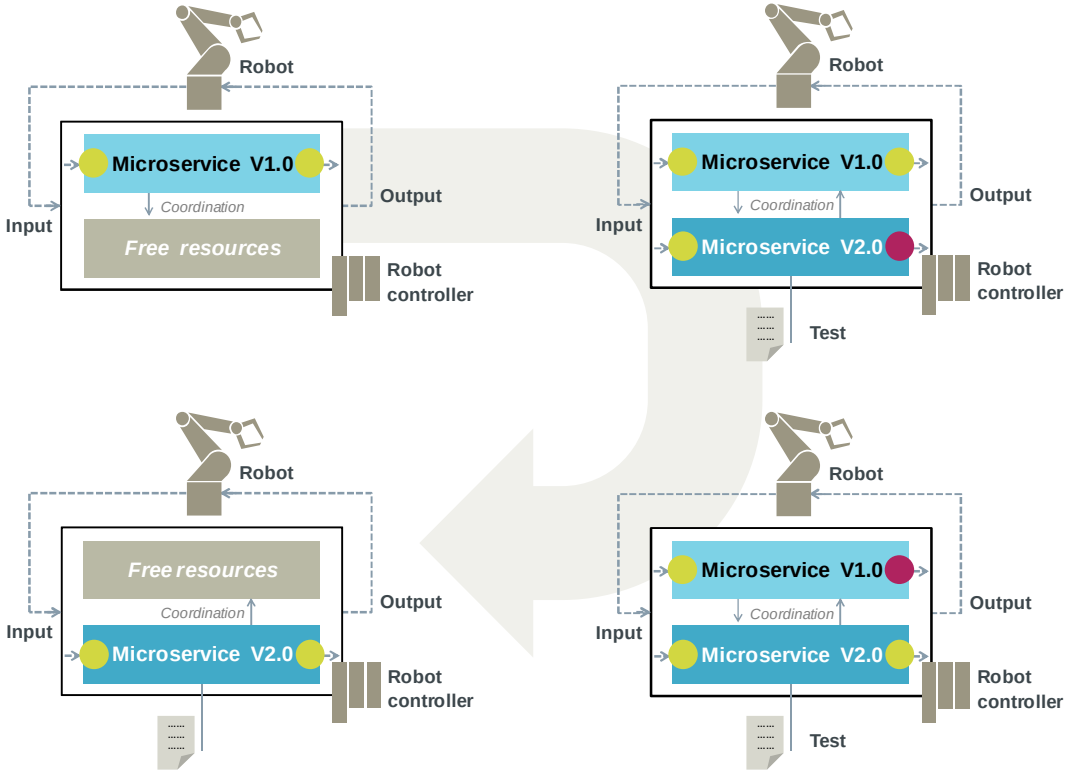


Deployment architecture must support zero downtime

Design for test in production, seamless activation and fail-over

SIEMENS
Ingenuity for life

- „ Deploy new microservice version to device, let it receive input but “mute” is output
- „ Execute pre-activation tests on the new microservice version via its TEST PROBE
- „ Notify the AUTHORITY DETERMINATION infrastructure to determine the new primary
- „ Let the PRIMARY ACTIVATION infrastructure activate the new microservice version when seamless switch-over is possible
- „ Continuously test the new microservice version in production via its TEST PROBE
- „ Fall back to old microservice version in case of problems, otherwise uninstall it



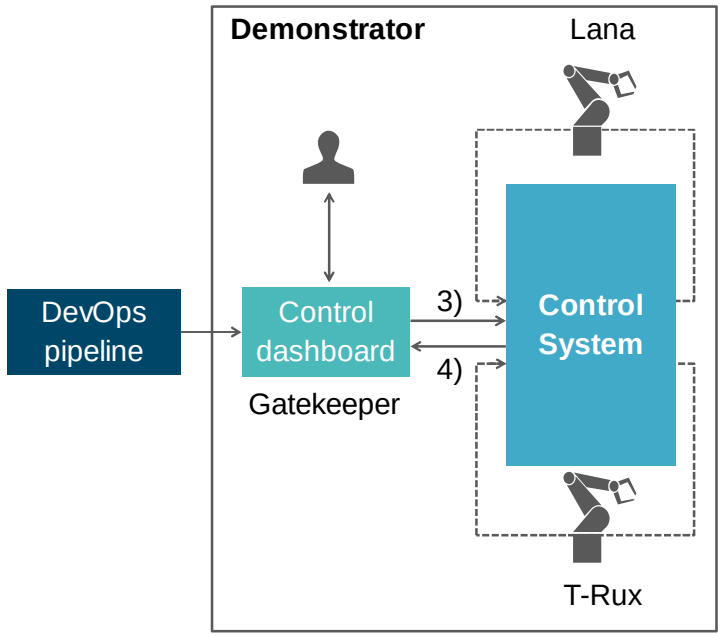
Ensure the device has dedicated resource budgets for continuous deployment

Operational quality demands side-effect-free deployment

Proof-of-Concept up and running

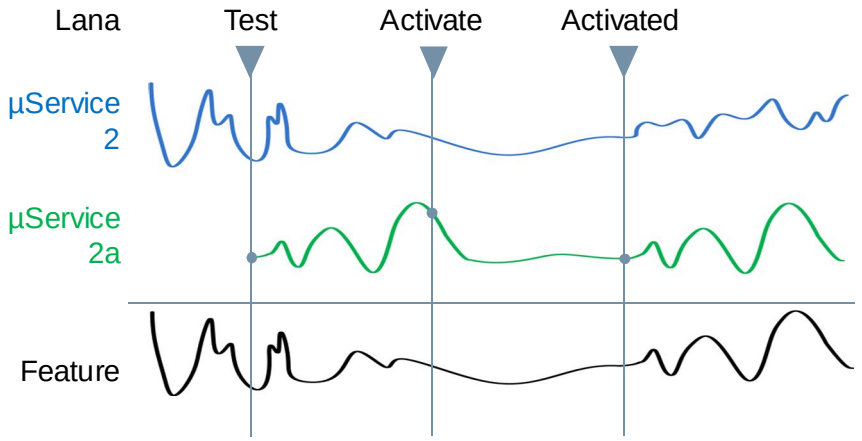
SIEMENS
Ingenuity for life

Demonstrator set-up

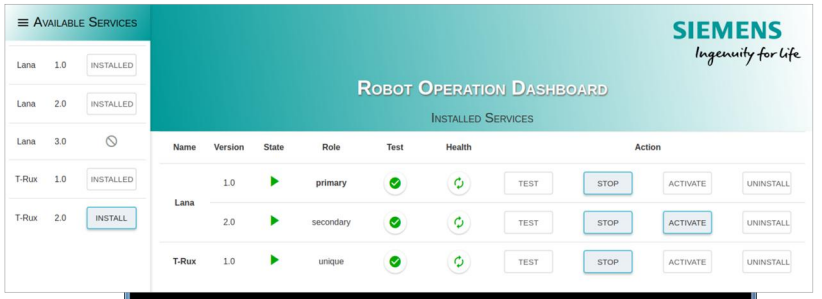


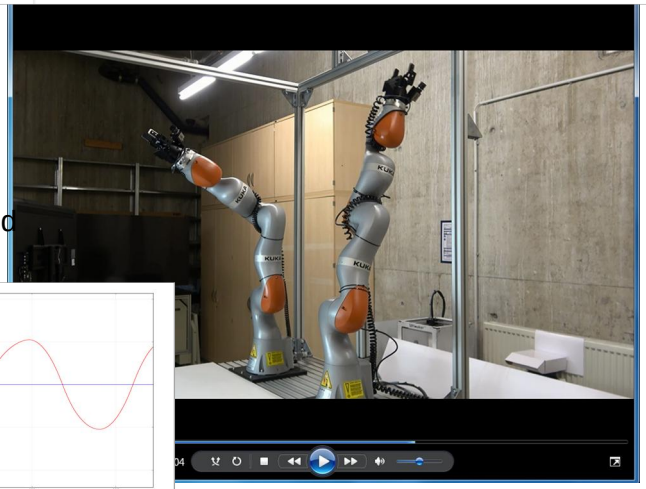
3) Deploy in operation
4) Monitor
5) Testing in operation

Expected behavior

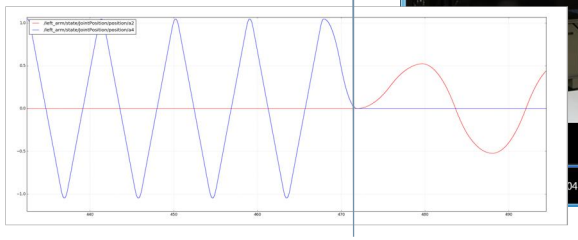


Lab set-up





Activated

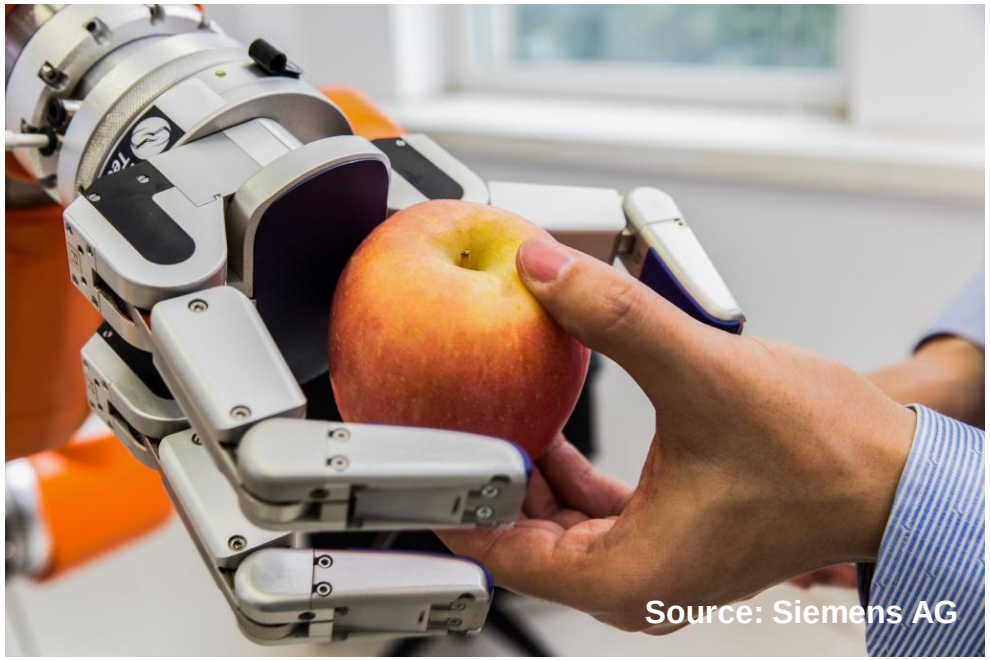


Operational quality demands side-effect-free deployment

Key aspects addressed, several research questions remain

SIEMENS
Ingenuity for life

- Design for continuous deployment adopts and enhances patterns for fault-tolerant systems
- Design concepts are feasible for independent microservices that implement a self-contained control program
  - PRIMARY ACTIVATION is a sensitivity point regarding correctness and availability
- Additional design concepts necessary for
  - Control programs that are federated across multiple (distributed) microservices
  - Assurance that deployment is side-effect-free to other microservices
- Applicability of common test-in-production practices like chaos monkey uncertain


Source: Siemens AG

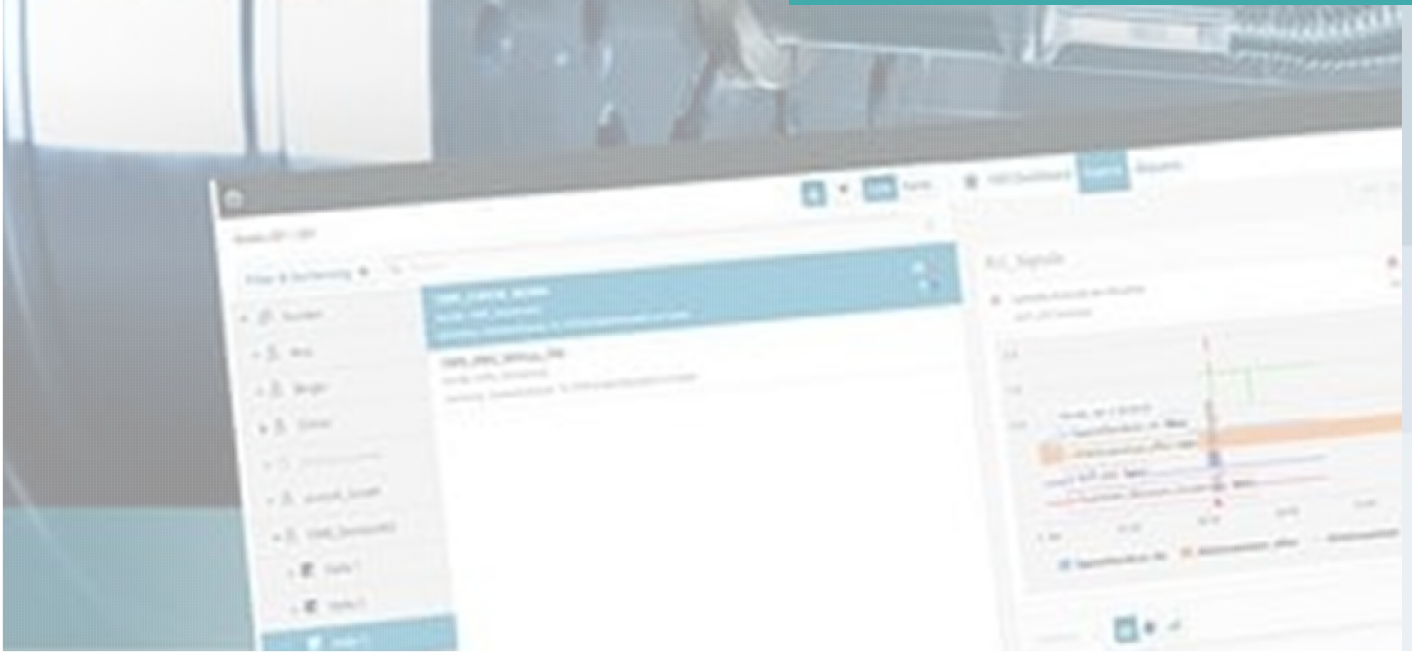
First adoptions of DevOps in industry target at the industrial IoT

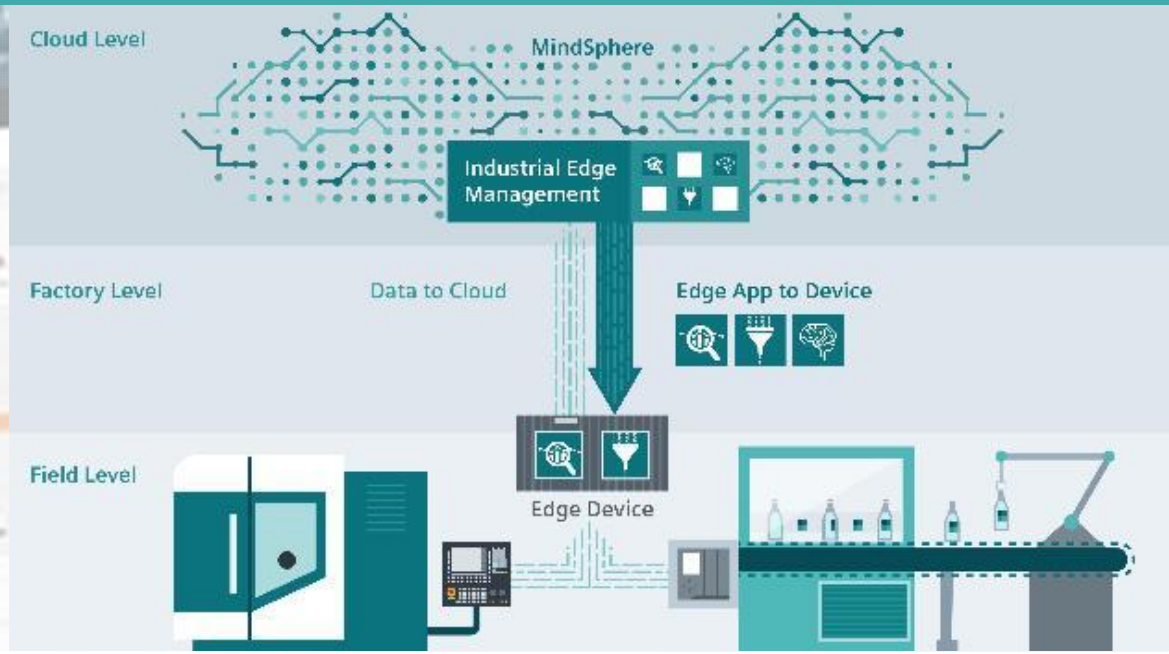
Cloud to edge analytics applications are in focus

SIEMENS
Ingenuity for life

Source: Siemens AG

Siemens Industrial Edge offers users the possibility of executing a range of descriptive, diagnostic, predictive and prescriptive analytical applications. This allows cloud connectivity (data to cloud) to be used in combination with Edge Apps from Siemens, third party providers or end users themselves in an integrated hardware and software ecosystem (Edge App to Device) for automation components.



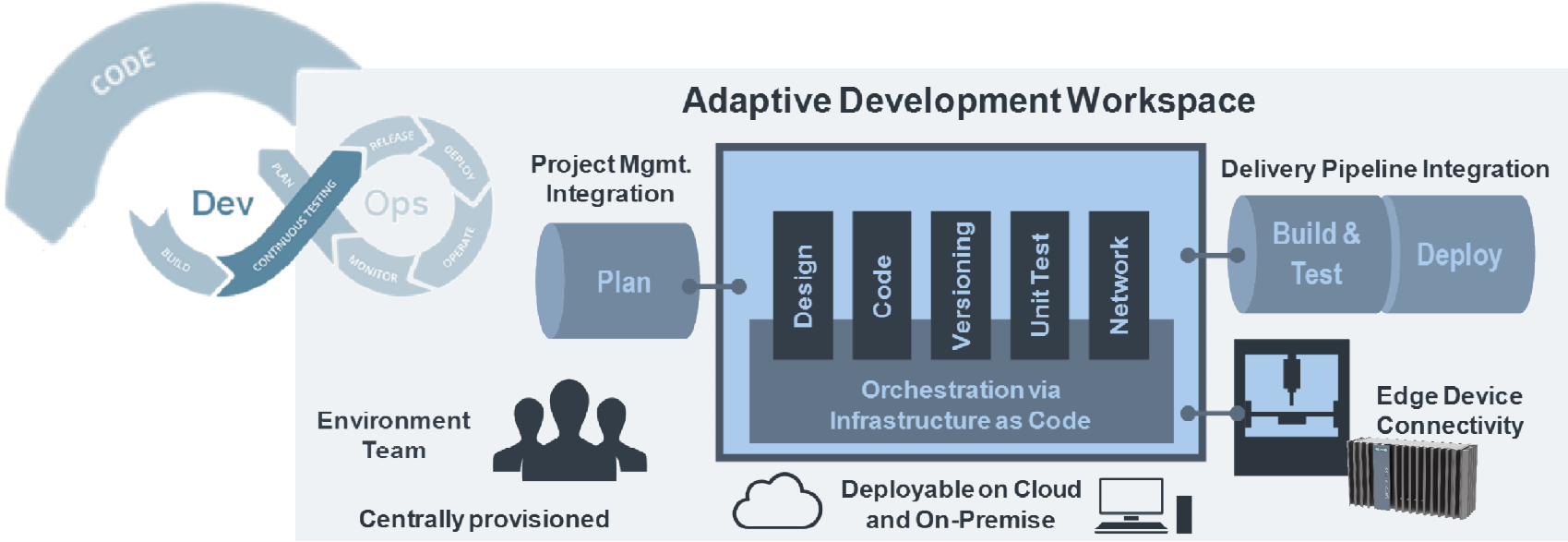


First adoptions of DevOps in industry target at the industrial IoT

Key aspects are development efficiency and delivery automation

SIEMENS
Ingenuity for life

- Adaptive Development Workspace
  - Centrally managed, locally adaptable by partners
  - Set-up and configuration < 30 min
  - Project templates to get developers productive < 1 day
  - Connectivity to delivery pipeline and edge devices
- Delivery Pipeline and App Management
  - Multi-staged pipeline with defined quality gates
  - Orchestration of apps federated across cloud and edge
  - Provisioning of runtimes for all target ops environments
  - App management infrastructure



DevOps proof of concepts for industrial operations systems in work

MOM and SCADA are the target

SIEMENS
Ingenuity for life

Manufacturing Operations Management

Supervisory Control and Data Acquisition

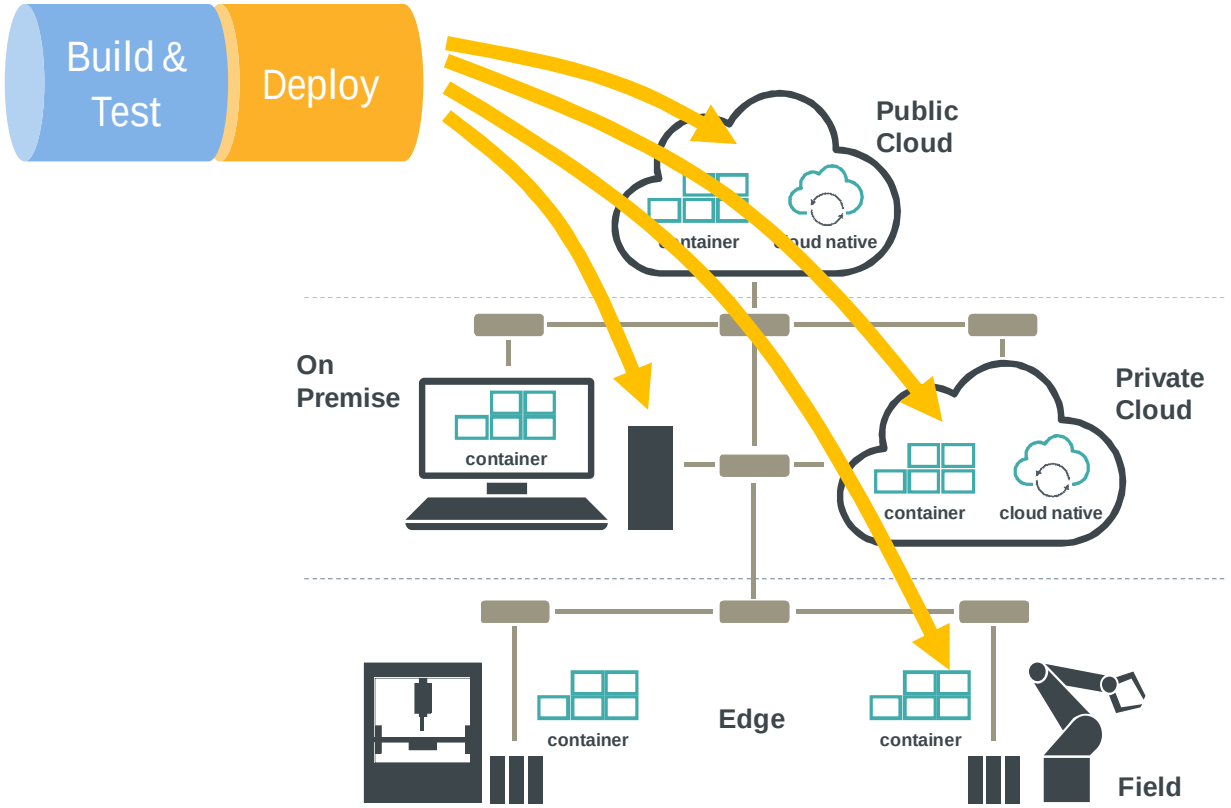
Source: Siemens AG

DevOps proof of concepts for industrial operations systems in work

Deployment flexibility and operational quality in focus

SIEMENS
Ingenuity for life

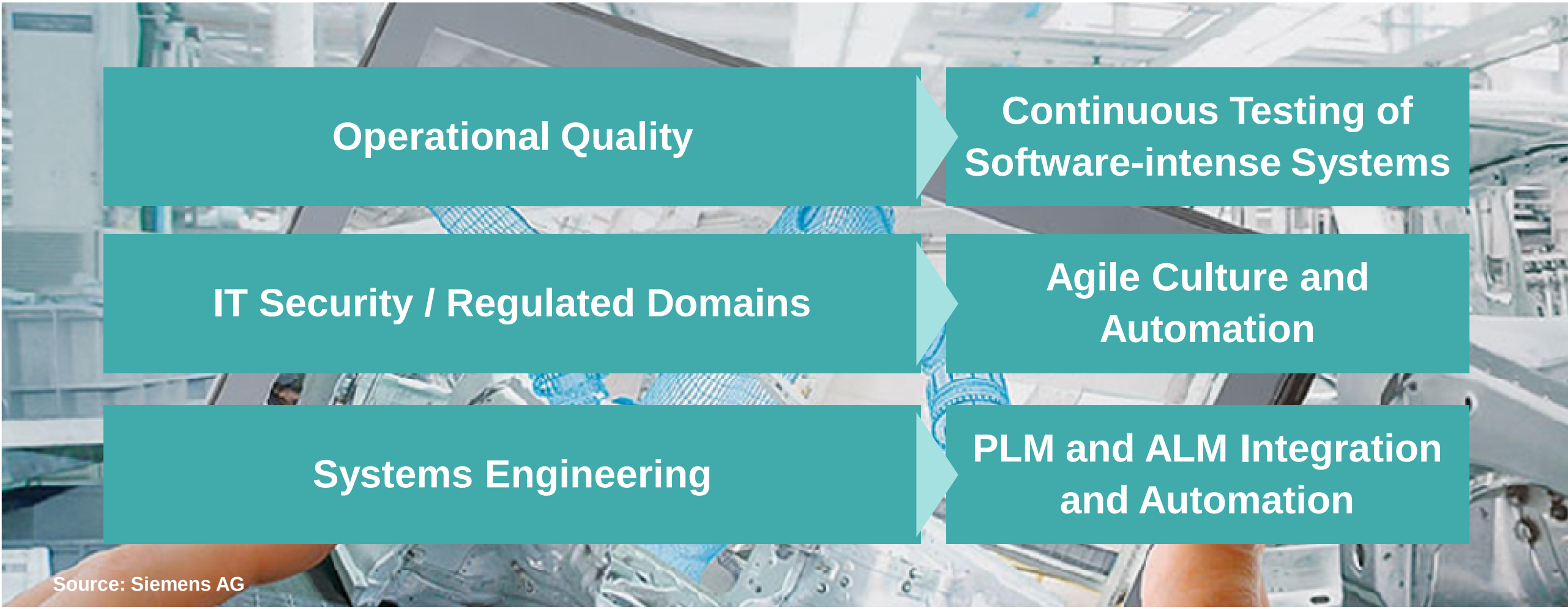
- Delivery pipeline for flexible deployment
  - Automatic orchestration of federated, distributed applications: cloud, on-premise, cloud to edge
  - Automatic provisioning of runtime images for all target ops environments
  - Firmware updates
  - App and firmware management
- Operational quality during deployment
  - Reliability
  - IT Security
  - Availability (on-premise and edge)



Research on industrial-grade DevOps ongoing

Tough industry challenges in focus

SIEMENS
Ingenuity for life



Source: Siemens AG

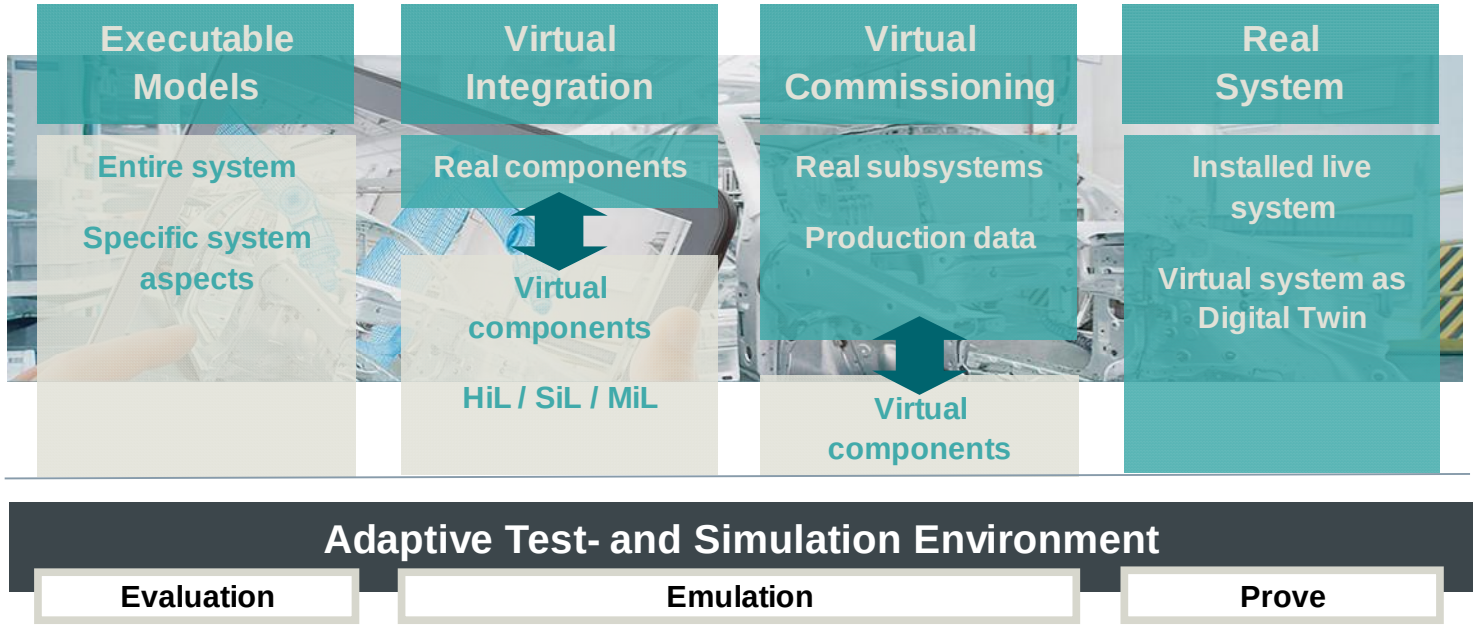
Continuous testing of software-intense industrial systems

Adaptive test and simulation environment to balance speed and quality

SIEMENS
Ingenuity for life

Enabler for shift-left and shift-right in software intense-systems, e.g., industry automation

- „ Model-based Digital Twin of the software to get immediate and early feedback on its quality in industrial environments
- „ Virtual integration and deployment as digital sandbox
- „ X-in-the-loop to step-wise frontload physical reality into software development



*) concept plus prototype

Research in industrial-grade DevOps is well founded

Core technologies developed over a longer time period

SIEMENS
Ingenuity for life

Höfig, K., Joanni, A., Zeller, M., Montrone, F., Rothfelder, M., Amarnath, R., Munk, P., Nordmann, A. (2018). Model-based Reliability and Safety: Reducing the complexity of safety analyses using component fault trees, Proceedings of the 2018 Annual Reliability and Maintainability Symposium (RAMS)

Möhrle, F., Zeller, M., Höfig, K., Rothfelder, M., Liggesmeyer., P. (2016). Automating Compositional Safety Analysis Using a Failure Type Taxonomy for Component Fault Trees, Proceedings of the 26th European Safety and Reliability Conference (ESREL), pp. 1380-1387

Zeller, M., Höfig, K. (2015). CONFeTTI – Component Fault Tree-Based Testing, Proceedings of the 25th European Safety and Reliability Conference (ESREL), pp 4011-4017

Armengaud, E.; Macher, G.; Massoner, A.; Frager, S.; Adler, R.; Schneider, D.; Longo, S.; Melis, M.; Groppo, R.; Villa, F.; O'Leary, P.; Bambury, K.; Finnegan, A.; Zeller, M.; Höfig, K.; Papadopoulos, Y.; Hawkins, R. & Kelly, T. DEIS: Dependability engineering innovation for automotive CPS 21st International Forum on Advanced Microsystems for Automotive Applications, 2017

Schneider, D.; Trapp, M.; Papadopoulos, Y.; Armengaud, E.; Zeller, M. & Höfig, K. WAP: Digital Dependability Identities 2015 IEEE International Symposium on Software Reliability Engineering (ISSRE), 2015, 324-329

Höfig, K.; Zeller, M. & Grunske, L. metaFMEA-A Framework for Reusable FMEAs Model-Based Safety and Assessment, Springer International Publishing, 2014, 8822, 110-122

Fröhlich, J., Stückjürgen, C. 2017: Reliable Inspection of an Autonomous System At System Runtime with Built-in Data Probes. ISSRE Workshops, Industry Track, Toulouse, IEEE Computer Society 2017, ISBN

Fröhlich, J., Frtunikj, J., Rothbauer, S., Stückjürgen, C. 2016: Testing Safety Properties of Cyber-Physical Systems with Non-Intrusive Fault Injection – An Industrial Case Study. SafeCOMP 2016, Trondheim, Springer, LNCS 9923.

Fröhlich, J., and Schwarzinger, M. 2006: Improve Component-Based Programs with Connectors. Joint Modular Language Conference, Oxford, Springer, LNCS 4228

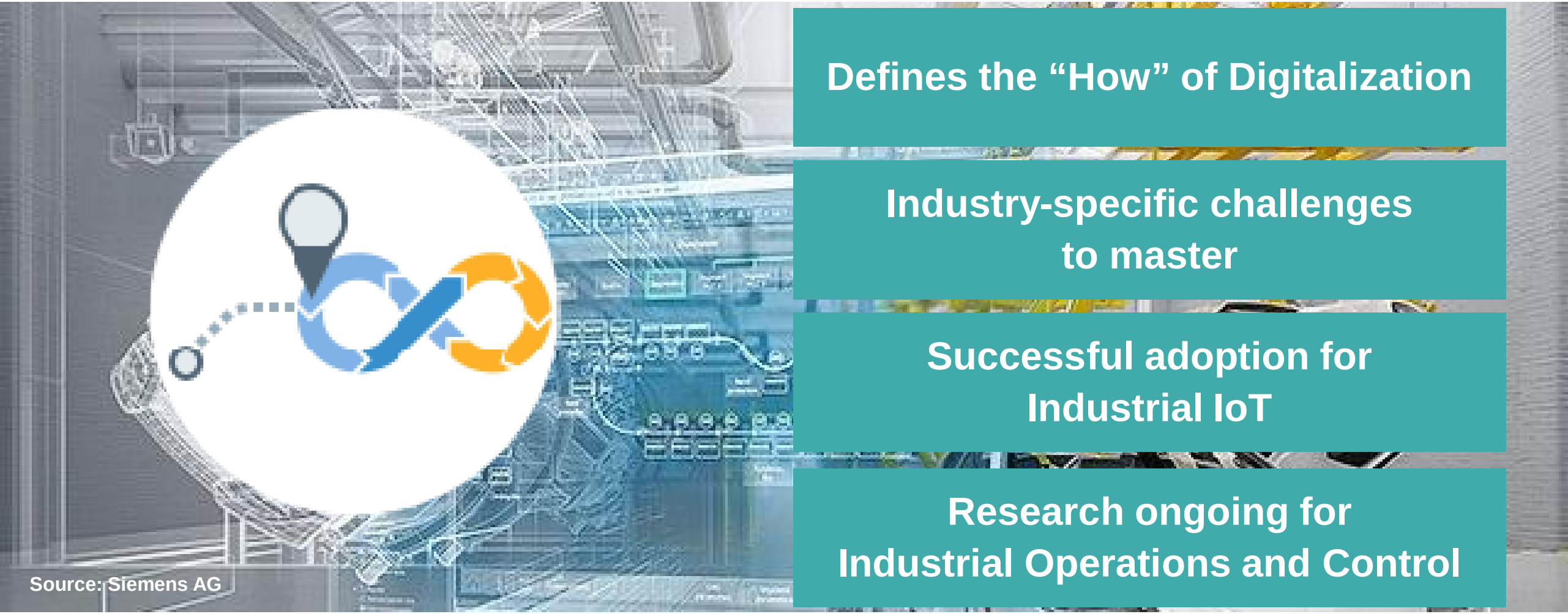
F. Li, J. Fröhlich, D. Schall, M. Lachenmayr, C. Stückjürgen, S. Meixner, F. Buschmann: Microservice Patterns for Industrial Edge Applications, EuroPLoP 2018

SELECTED PUBLICATIONS

Industrial-grade DevOps is key for the Digitalization of Industry

Helps mastering the digital transformation at speed and scale

SIEMENS
Ingenuity for life



Source: Siemens AG

Defines the “How” of Digitalization

Industry-specific challenges to master

Successful adoption for Industrial IoT

Research ongoing for Industrial Operations and Control

SIEMENS
Ingenuity for life

Industrial-Grade DevOps

Balancing Speed with Extreme Quality

Frank Buschmann w/ Joachim Fröhlich, Lars Gelbke, Fei Li, Marc Zeller, Peter Zimmerer
Siemens AG, Corporate Technology