NEMO2018/2019 (5th/6th)

The University of Vienna, Austria

Process Algebra to Model Smart Distributed Mobile Real-Time IoT

Implementation Perspective for Cyber-Physical Systems

20 Sept 2019

Prof. Moonkun Lee, Ph.D.

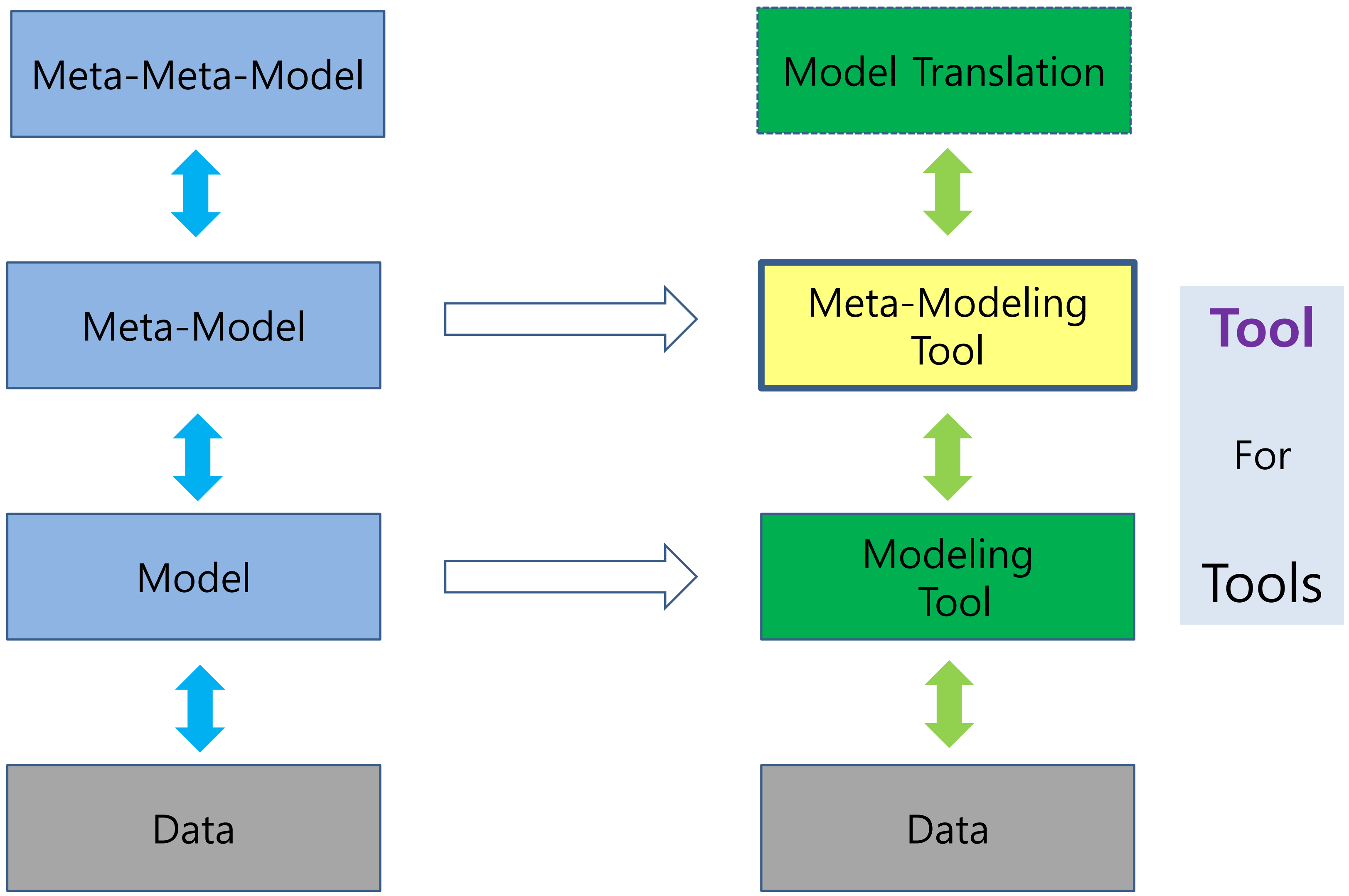
Division of Computer Science and Engineering
Chonbuk National University
Republic of Korea

OMiLAB KOREA

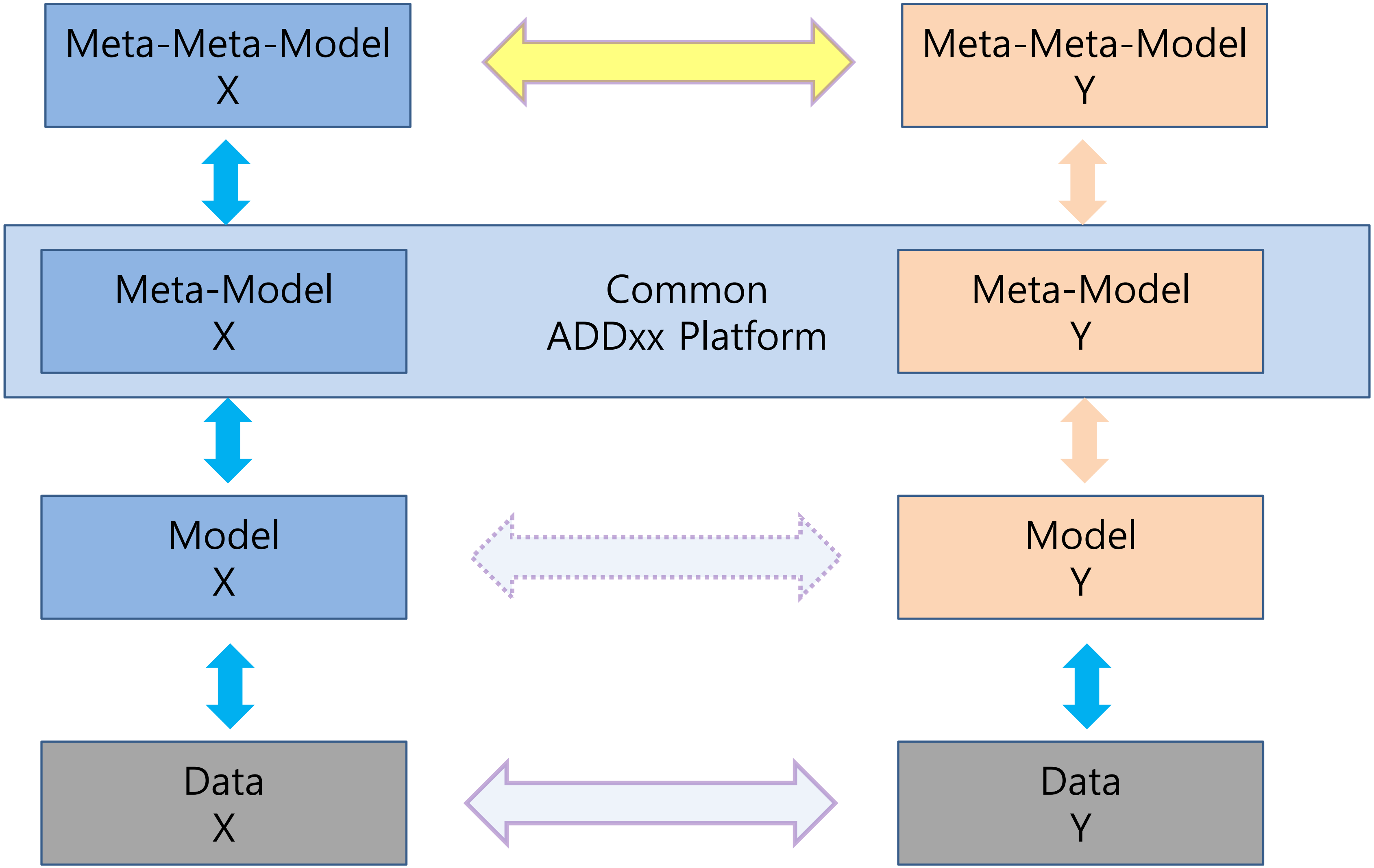
MEMO
SUMMER SCHOOL

ADOxx Meta-Modeling Platform

Modeling Hierarchy



Model Tranformation/Translation

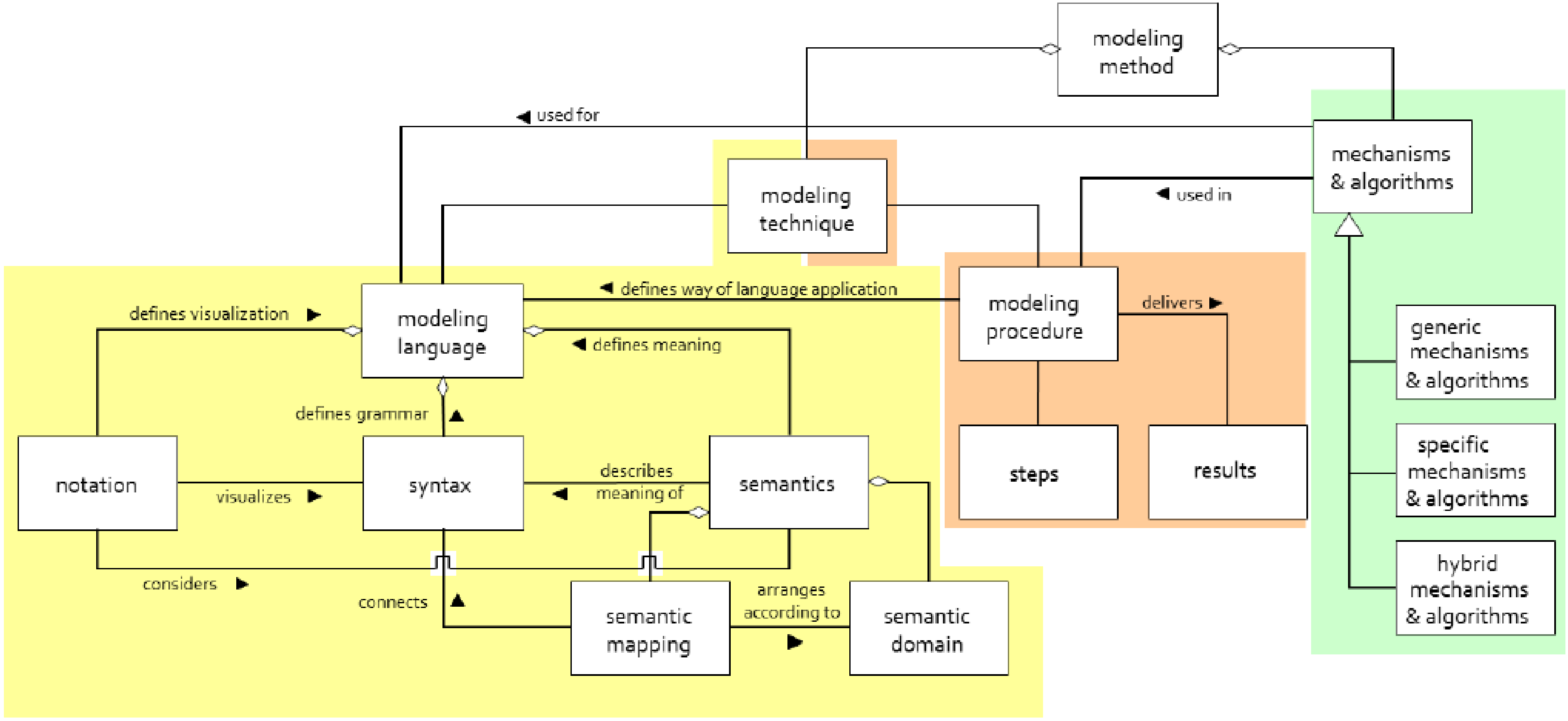


Meta-Modeling Tools

Aspects	AToM3	MetaEdit+	DOME	ADOxx
Platforms	Windows, Unix	Windows, Unix, Sun Solaris, HP	Windows, Linux, Sun Solaris	Windows
Meta-modeling language	ER	GOPRR	The DOME Tool Specification language	ADOxx Meta-modeling Language
Graphical specification?	Yes	No	Partly, the graphical appearance can't be edited in a graphical way	Yes
Hierarchy	Partly, not implement complete yet	Yes, decomposition	Yes, sub-diagram	Yes
Inheritance	No	Yes, (make dependant)	Yes	Yes
Constraint	Python function or OCL	No specific constraint language	Alter language	ADOxx Definition Language, AdoScript
Simulation	Yes	Yes	Yes	Yes
Simulation method and implementation workload	Graph Grammar, an intuitive way, less code by hand	Report definition language, all code by hand	Alter function, all code by hand	Supported by ADOxx or all code by hand
Code generation and workload	Python source code Little code by hand	Can be any language Most code by hand	Can be any language Most code by hand	No
Report generation	No	Yes	No	Yes

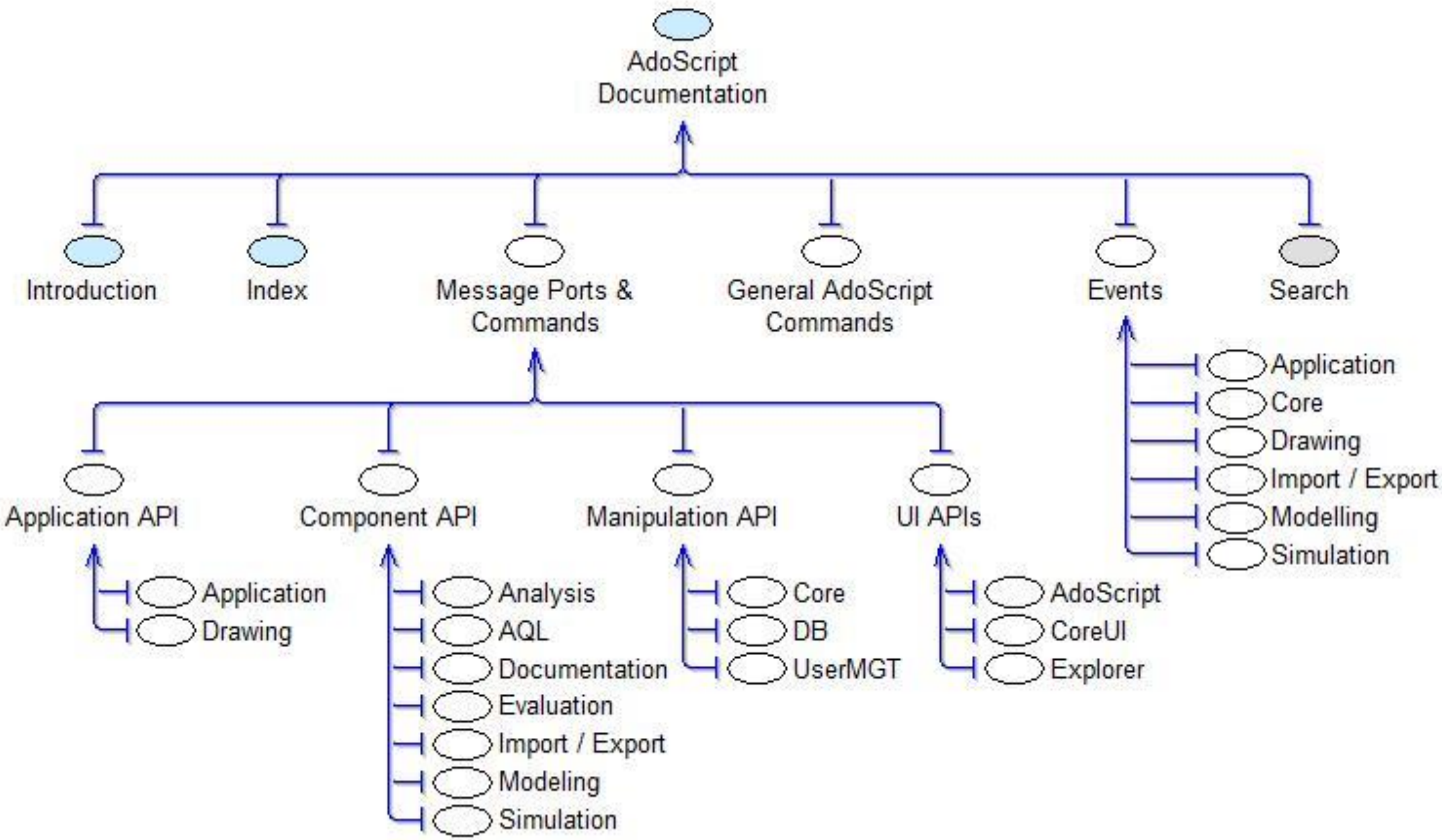
Generic Modelling Method Framework

Method = (T+MA)·(L+P)

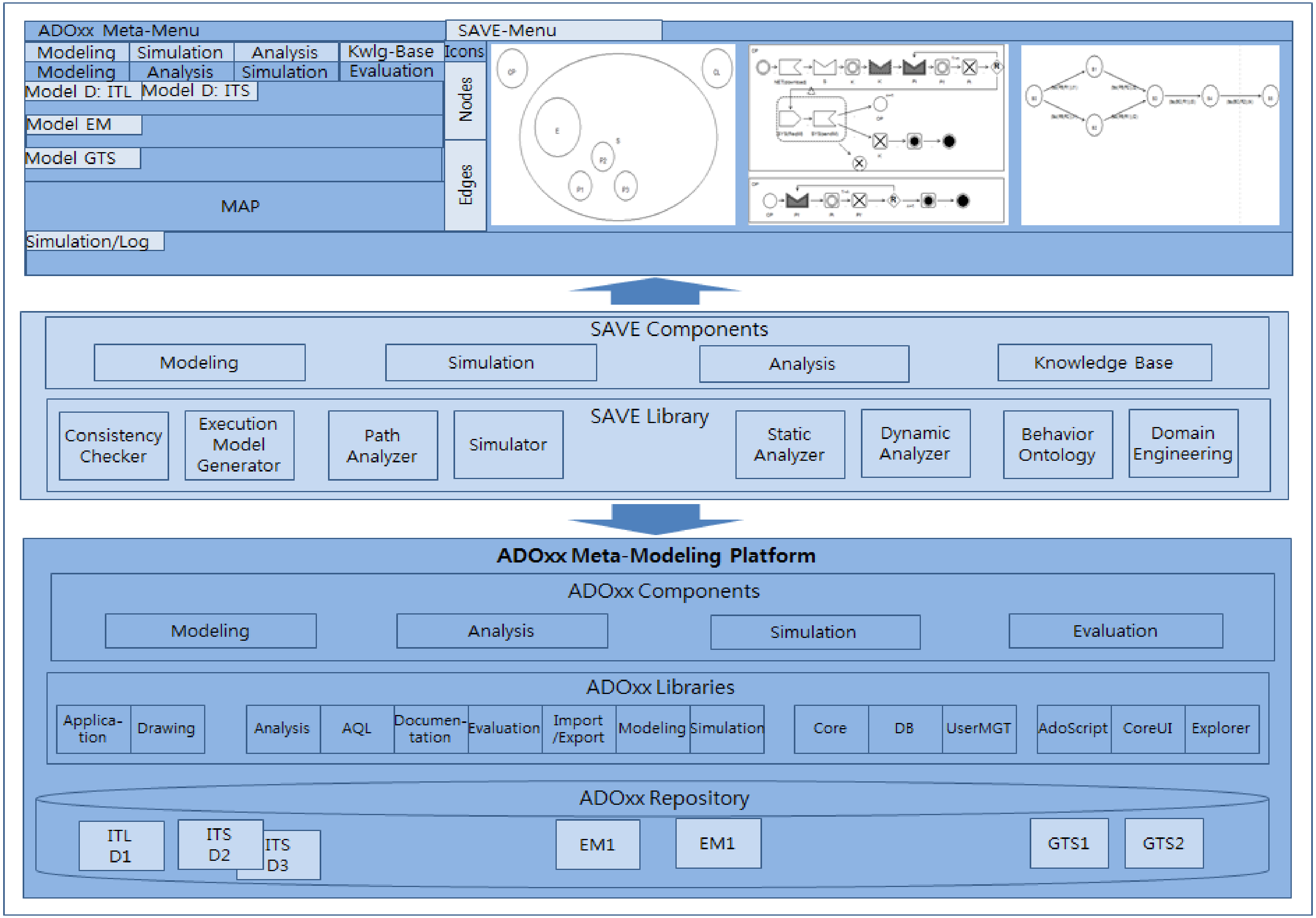


Karagiannis, D., Kühn, H.: „Metamodelling Platforms". In Bauknecht, K., Min Tjoa, A., Quirchmayer, G. (Eds.): Proceedings of the Third International Conference EC-Web 2002 – Dexa 2002, Aix-en-Provence, France, September 2002, LNCS 2455, Springer, Berlin/Heidelberg, p. 182.

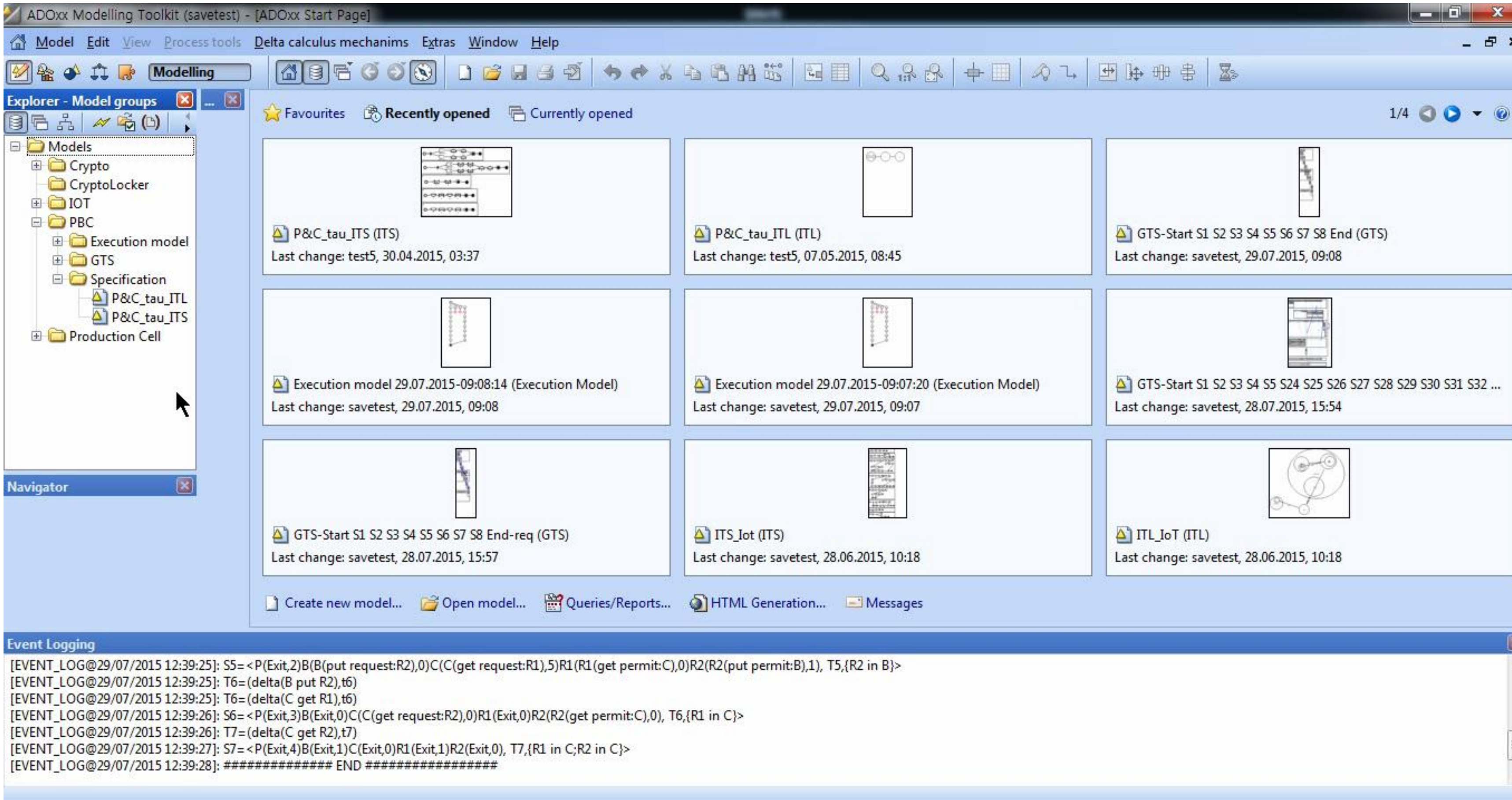
ADOxx Library



A Tool on the Platform

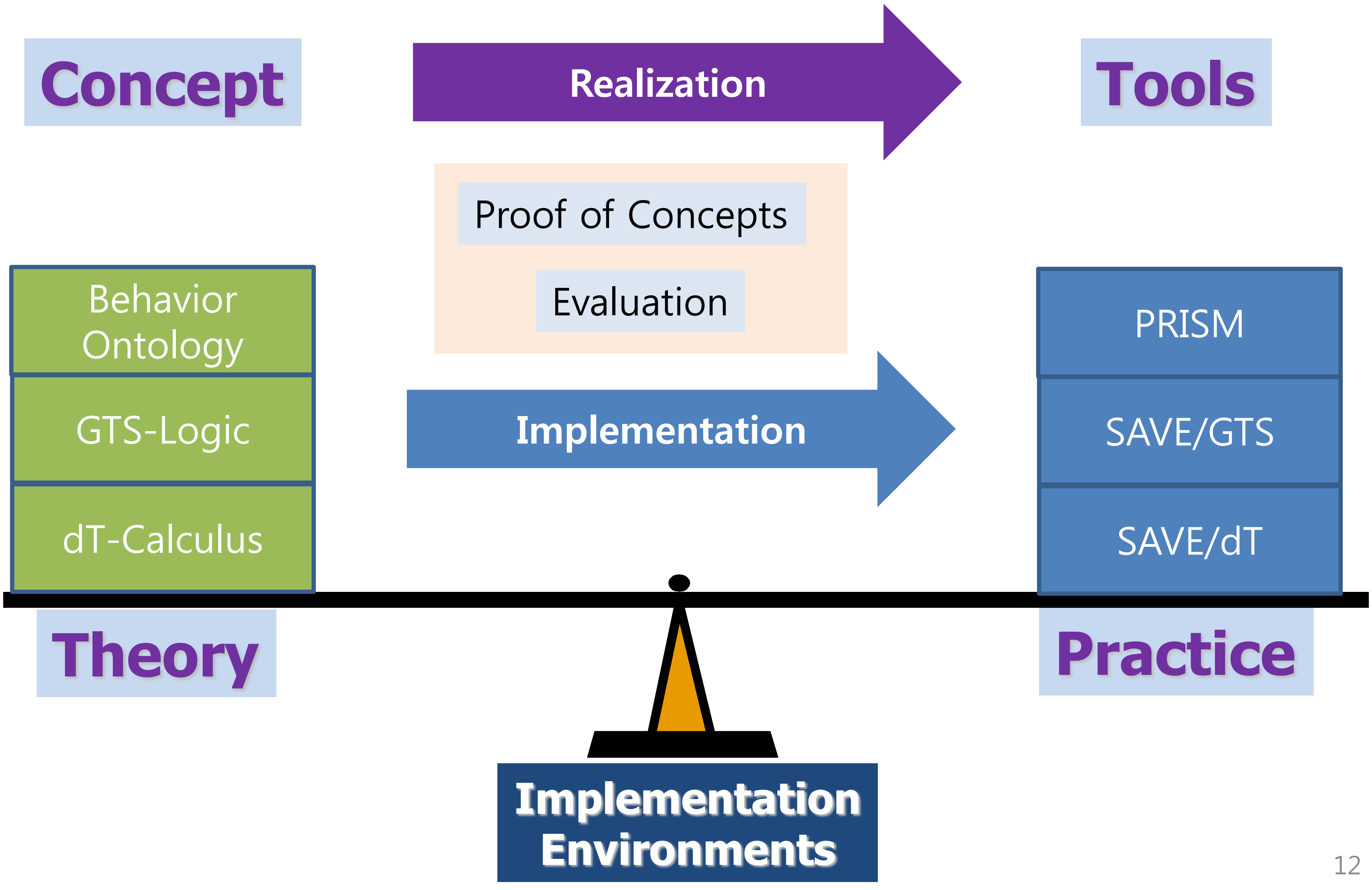


DEMO: PBC



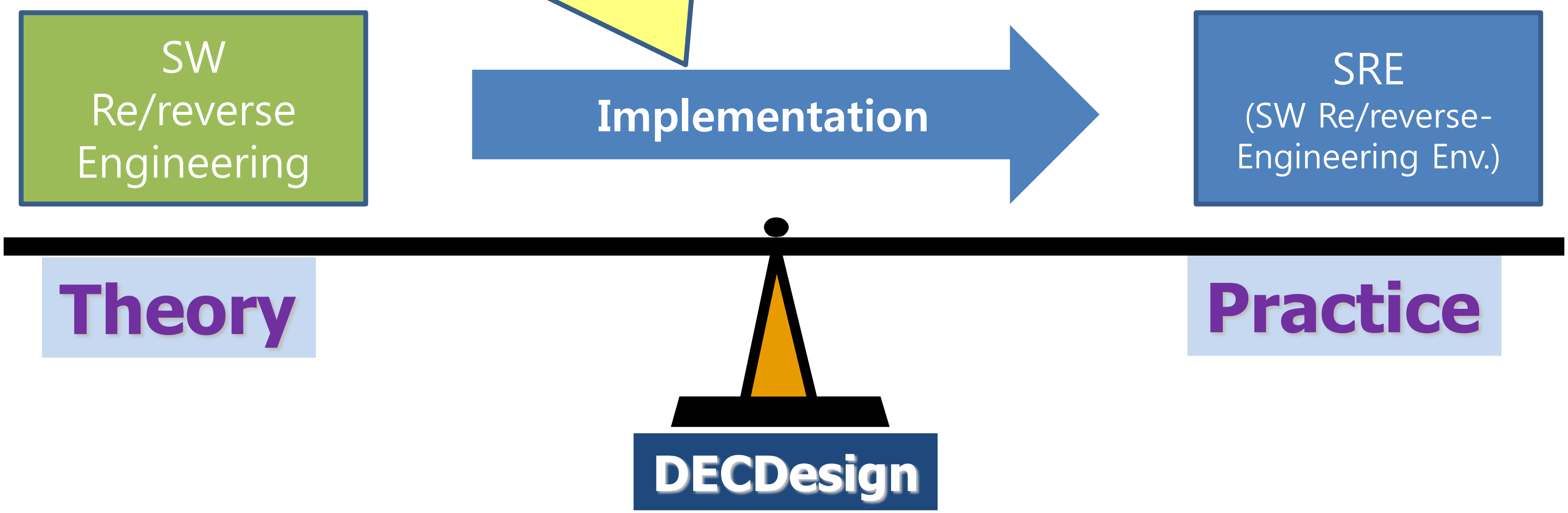
ADOxx Modelling Toolkit (savetest) - [ADOxx Start Page]
Model Edit View Process tools Delta calculus mechanims Extras Window Help
Modelling
Explorer - Model groups
Models
Crypto
CryptoLocker
IOT
PBC
Execution model
GTS
Specification
P&C_tau_ITL
P&C_tau_ITS
Production Cell
Navigator
Favourites
Recently opened
Currently opened
1/4
P&C_tau_ITS (ITS)
Last change: test5, 30.04.2015, 03:37
P&C_tau_ITL (ITL)
Last change: test5, 07.05.2015, 08:45
GTS-Start S1 S2 S3 S4 S5 S6 S7 S8 End (GTS)
Last change: savetest, 29.07.2015, 09:08
Execution model 29.07.2015-09:08:14 (Execution Model)
Last change: savetest, 29.07.2015, 09:08
Execution model 29.07.2015-09:07:20 (Execution Model)
Last change: savetest, 29.07.2015, 09:07
GTS-Start S1 S2 S3 S4 S5 S24 S25 S26 S27 S28 S29 S30 S31 S32 ...
Last change: savetest, 28.07.2015, 15:54
GTS-Start S1 S2 S3 S4 S5 S6 S7 S8 End-req (GTS)
Last change: savetest, 28.07.2015, 15:57
ITS_Iot (ITS)
Last change: savetest, 28.06.2015, 10:18
ITL_IoT (ITL)
Last change: savetest, 28.06.2015, 10:18
Create new model...
Open model...
Queries/Reports...
HTML Generation...
Messages
Event Logging
[EVENT_LOG@29/07/2015 12:39:25]: S5=<P(Exit,2)B(B(put request:R2),0)C(C(get request:R1),5)R1(R1(get permit:C),0)R2(R2(put permit:B),1), T5,{R2 in B}>
[EVENT_LOG@29/07/2015 12:39:25]: T6=(delta(B put R2),t6)
[EVENT_LOG@29/07/2015 12:39:25]: T6=(delta(C get R1),t6)
[EVENT_LOG@29/07/2015 12:39:26]: S6=<P(Exit,3)B(Exit,0)C(C(get request:R2),0)R1(Exit,0)R2(R2(get permit:C),0), T6,{R1 in C}>
[EVENT_LOG@29/07/2015 12:39:26]: T7=(delta(C get R2),t7)
[EVENT_LOG@29/07/2015 12:39:27]: S7=<P(Exit,4)B(Exit,1)C(Exit,0)R1(Exit,1)R2(Exit,0), T7,{R1 in C;R2 in C}>
[EVENT_LOG@29/07/2015 12:39:28]: ############## END #################

SW Engineering

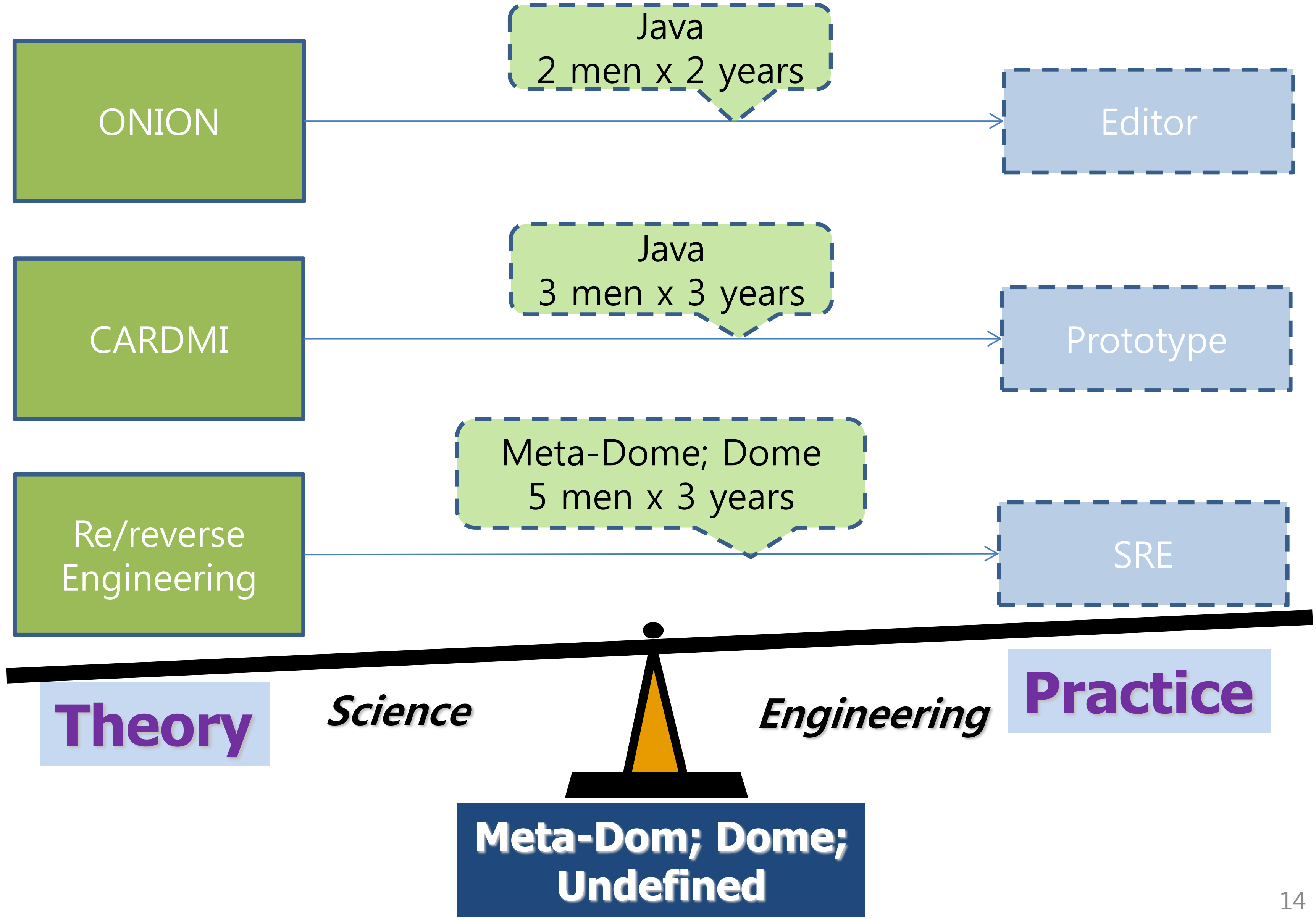


SW Engineering (1991~1996)

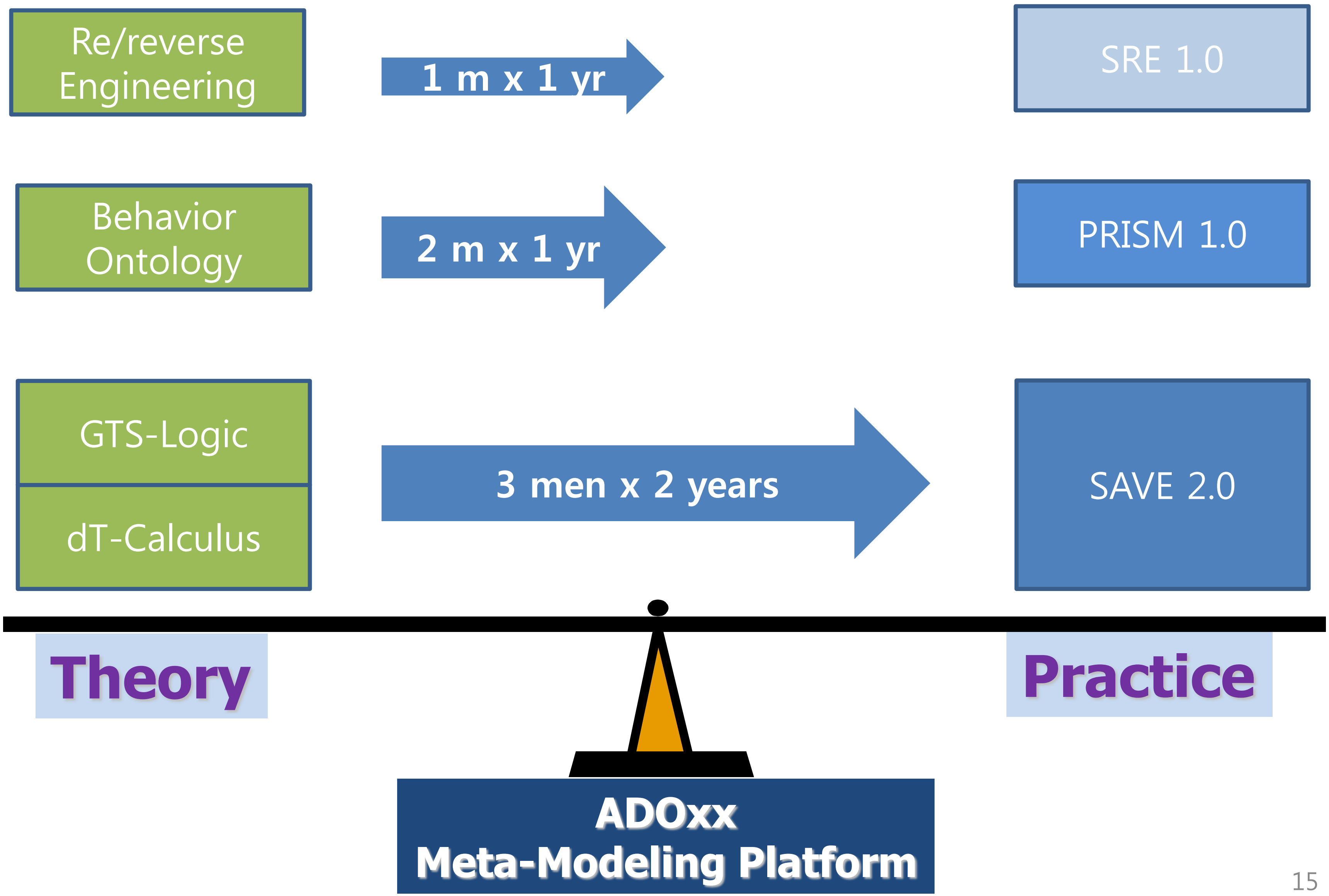
- R&D, CCCC, USA (~1996)
  - · SRE(SW Re/Reverse-engineering Environment) Tool
  - · DECDesign,
  - · 5 years (11 yrs x 5 men)
  - · USA, Navy, 100,000 ~ 1,000,000 LOC (Scalability)
  - · OS: ATES, SDEX-20 → Unix, VMS
  - · PL: Fortran, C, Ada83 → C, C++, Ada83, Ada95



SW Engineering



SW Engineering

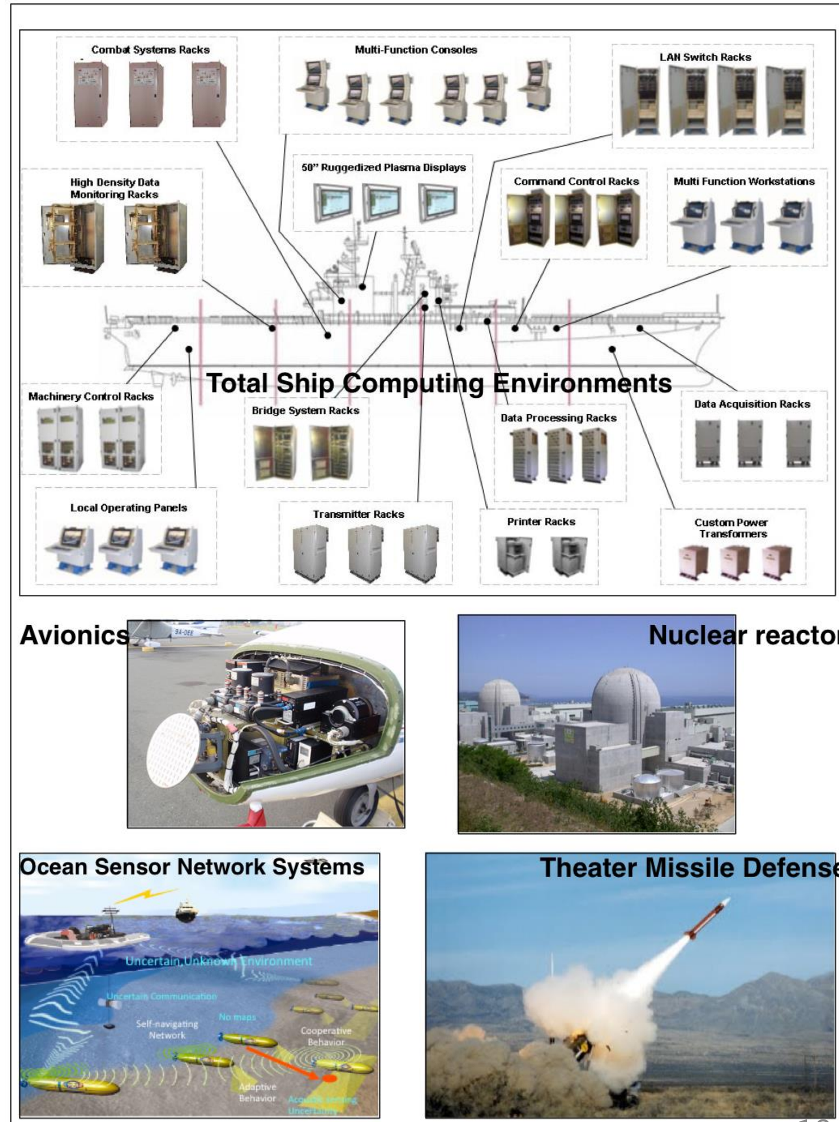


Contents

1. MOTIVATIONS

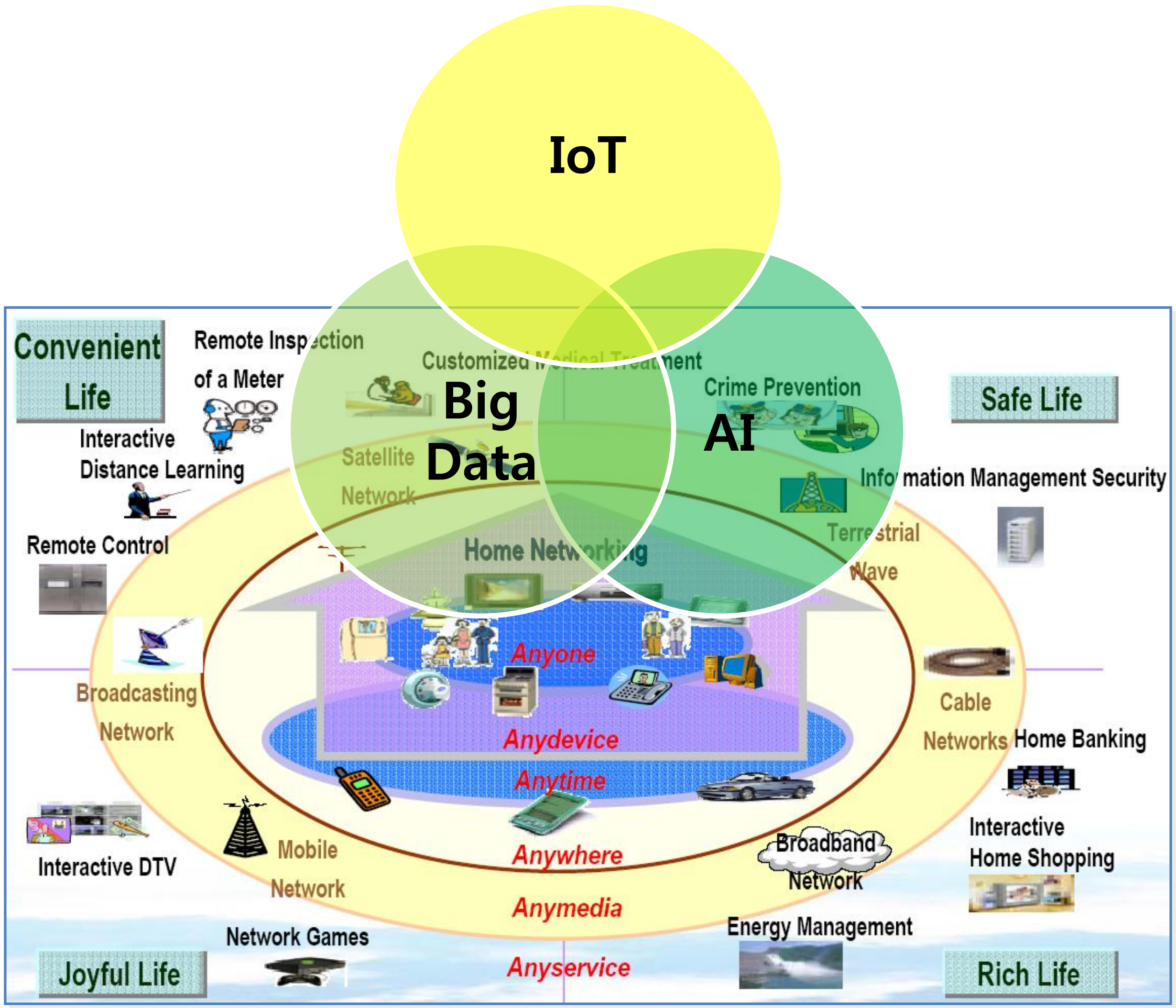
Mission –Critical Systems

- Properties
  - Distributedness
  - Mobility
  - Communication
  - Process Control
  - Temporality
- Characteristics
  - Complex
  - Large
  - Timeliness
- Examples
  - Telecommunication networks
  - Telemedicine
  - Process automation
  - Multimedia streaming
  - Avionics systems
  - Defense applications
- Requirements
  - Specification
  - Verification



Smart Systems

- Properties
  - Distributedness
  - Mobility
  - Communication
  - Process Control
  - Temporality
- Characteristics
  - IoT
  - Big Data
  - AI
- Examples
  - Smart Home
  - Smart Car
  - Smart Office
  - Smart Building
  - Smart City
  - Smart Factory
  - Smart Society
- Requirements
  - Safety
  - Security
  - Reliability



Accident Rates: USA

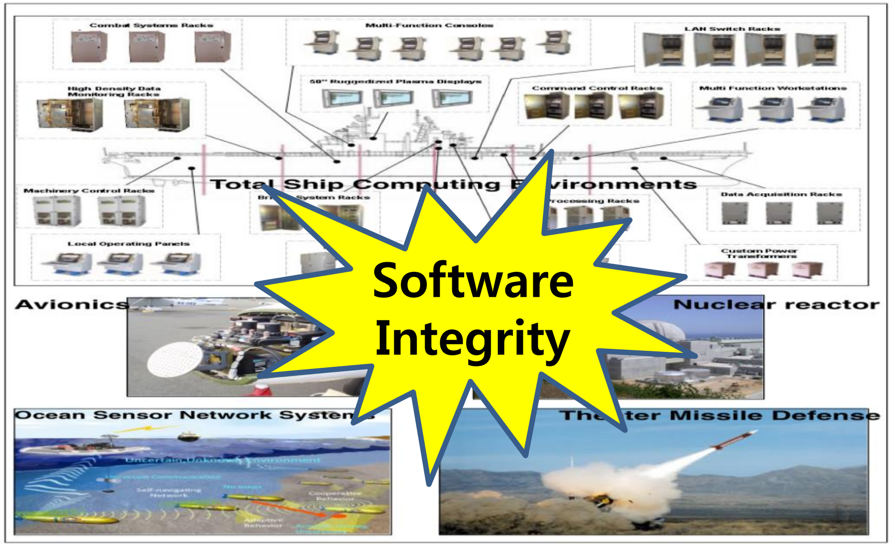
- Driving
  - The National Highway Traffic Safety Admin
  - Traffic Safety Facts Data
    - Year 2008
      - 1.27 fatalities per 100 million vehicle miles traveled
    - Year 1998
      - 1.58 fatalities per 100 million miles

- Flying
  - The National Transportation Safety Board
  - Preliminary statistics
    - Year 2008
      - 20 accidents for U.S. air carriers operating scheduled service
      - nearly zero accidents per million flying miles
      - No one died, and only 5 people were seriously injured.

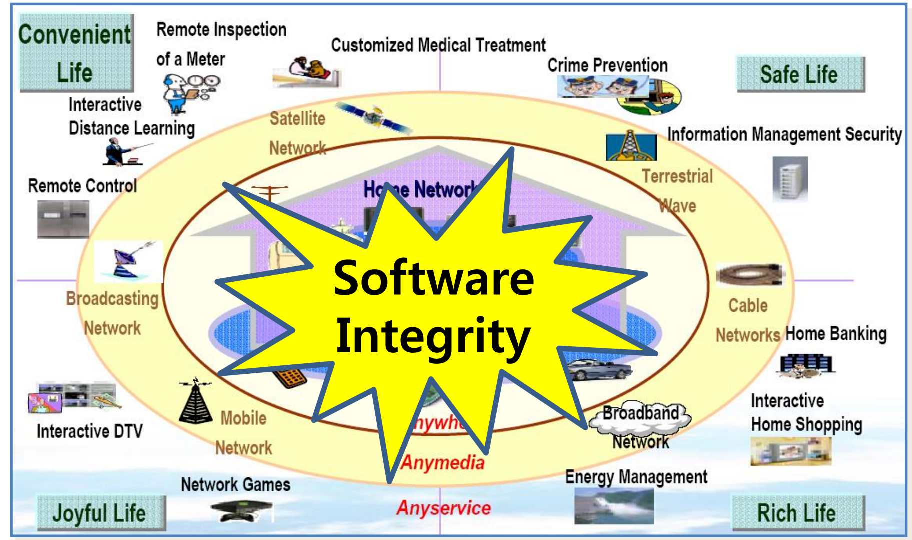
https://traveltips.usatoday.com/air-travel-safer-car-travel-1581.html

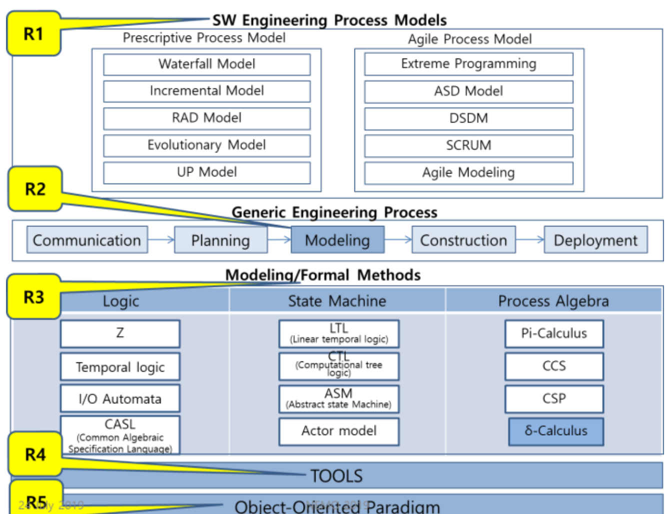
Safety/Security Requirements for SW

Mission-Critical Systems



Smart Systems

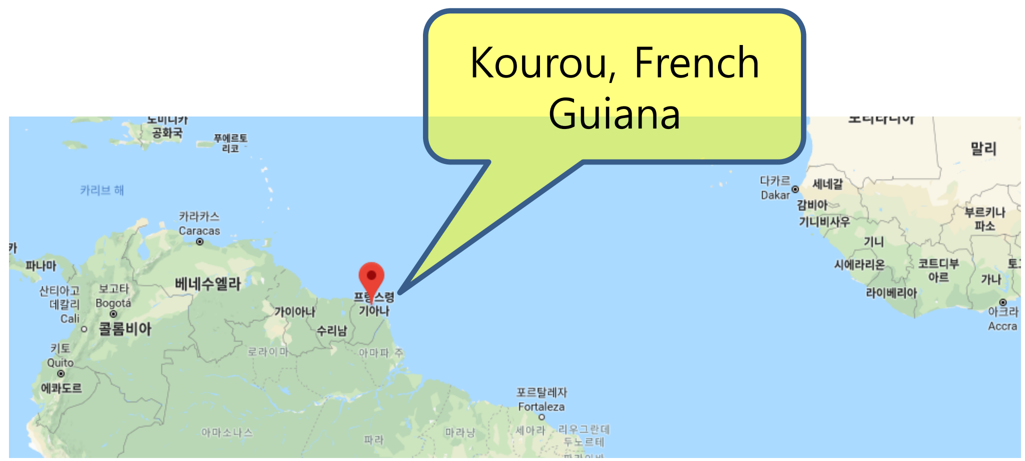




Motivation:
Secure Requirements

Year **1996**, ESA Ariane Flight 5 Failure

- Description:
  - 1996, ESA Ariane 5 Flight Exploded, at 40 seconds after launch.
- Cause of explosion:
  - A part of the flight SW, reused from Ariane 4.
  - One of the sensors in the flight 5 was designed to return a float point value.
  - But it used the code for the sensor from the Ariane 4 that was to return an integer value, which did not have an exception handler for overflow due to the inappropriate type of the return value.
  - As a result, the exception triggered a signal to the self-explosion of the flight.
- Total cost of the failure:
  - Hardware Cost: 0.37 Billion $
  - Development Cost: 7 Billion $.
  - Cluster II: 4 identical satellites to study the Earth's magnetosphere over the course of an entire solar cycle.



Cause: Reused Ada Source Code

Reused Ariane 4 Code for Ariane 5

```
procedure LIRE_DERIVE (...) is
...
begin
   ...
   L_MBV_32:=TBD.T_ENTIER_32S ((1.0/C_M_LSB_BV)*
                               G_M_INFO_DERIVE(T_ALG.E_BV));
   if L_M_BV_32 > 32767 then
      P_M_DERIVE(T_ALG.E_BV) := 16#7FFF#;
   elsif L_M_BV_32 < -32768 then
      P_M_DERIVE(T_ALG.E_BV) := 16#8000#;
   else
      P_M_DERIVE(T_ALG.E_BV):= UC_16S_EN_16NS(TBD.T_ENTER_16S(L_M_BV_32));
   end if;

   P_M_DERIVE_T_ALG.E_BH) := UC_16S_EN_16NS(TBD.T_ENTER_16S
                                  ((1.0/C_M_LSB_BH)*
                                   G_M_INFO_DERIVE(T_ALG.E_BV)));
end LIRE_DERIVE;
```

```
procedure LIRE_DERIVE (...) is
...
begin
   ...
   L_MBV_32:=TBD.T_ENTIER_32S ((1.0/C_M_LSB_BV)*
                               G_M_INFO_DERIVE(T_ALG.E_BV));
   if L_M_BV_32 > 32767 then
      P_M_DERIVE(T_ALG.E_BV) := 16#7FFF#;
   elsif L_M_BV_32 < -32768 then
      P_M_DERIVE(T_ALG.E_BV) := 16#8000#;
   else
      P_M_DERIVE(T_ALG.E_BV) := UC_16S_EN_16NS(TBD.T_ENTER_16S(L_M_BV_32));
   end if;

   L_M_BH_32 := TBD.T_ENTIER_32S ((1.0/C_M_LSB_BH)*
                                  G_M_INFO_DERIVE(T_ALG.E_BH));
   if L_M_BH_32 > 32767 then
      P_M_DERIVE(T_ALG.E_BH) := 16#7FFF#;
   elsif L_M_BH_32 < -32768 then
      P_M_DERIVE(T_ALG.E_BH) := 16#8000#;
   else
      P_M_DERIVE(T_ALG.E_BH):= UC_16S_EN_16NS(TBD.T_ENTER_16S(L_M_BH_32));
   end if;
end LIRE_DERIVE;
```

The internal SRI software exception was caused during execution of a data conversion from 64-bit floating point to 16-bit signed integer value. The floating point number which was converted had a value greater than what could be represented by a 16-bit signed integer.*

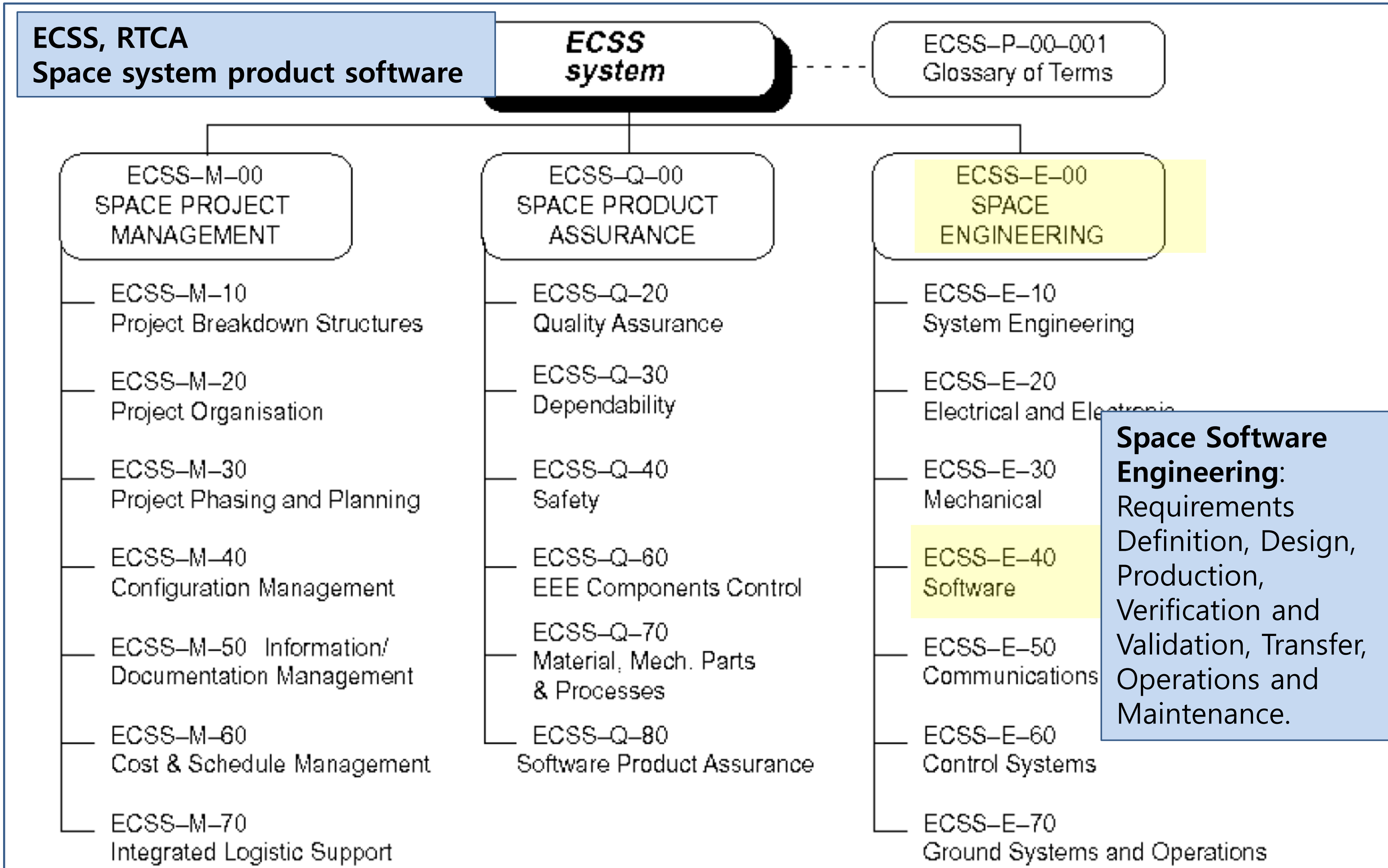
http://moscova.inria.fr/~levy/talks/10enslongo/enslongo.pdf
http://www-users.math.umn.edu/~arnold/disasters/ariane.html

Standards

- ESA:
  - 1975
  - Paris, France
  - 22 member states
  - Budget: 5.250 Billion Euro in 2016.
- ECSS
  - Organization: 1993
- Standardization
    - Management: ECSS-M-00
    - Assurance: ECSS-Q-00
    - Engineering: ECSS-E-00
  - SW:
    - **ECSS-E-40: SW Engineering (Version A: 1999)**
      - **Derived from ISO** 12207
    - **ECSS-Q-80: SW Product Assurance (Version A: 1996)**
- **ECSS-E-40**
  - SW Engineering
    - SW Engineering Process
    - Model-Based SW Engineering
    - Formal Methods
    - Tool-Based SW Engineering
    - SW life Cycle Process
- Results:
  - ~ 2013년
  - Total 67 launches; 4 failures.

ECSS-E-40C (~2009)

ECSS, RTCA
Space system product software

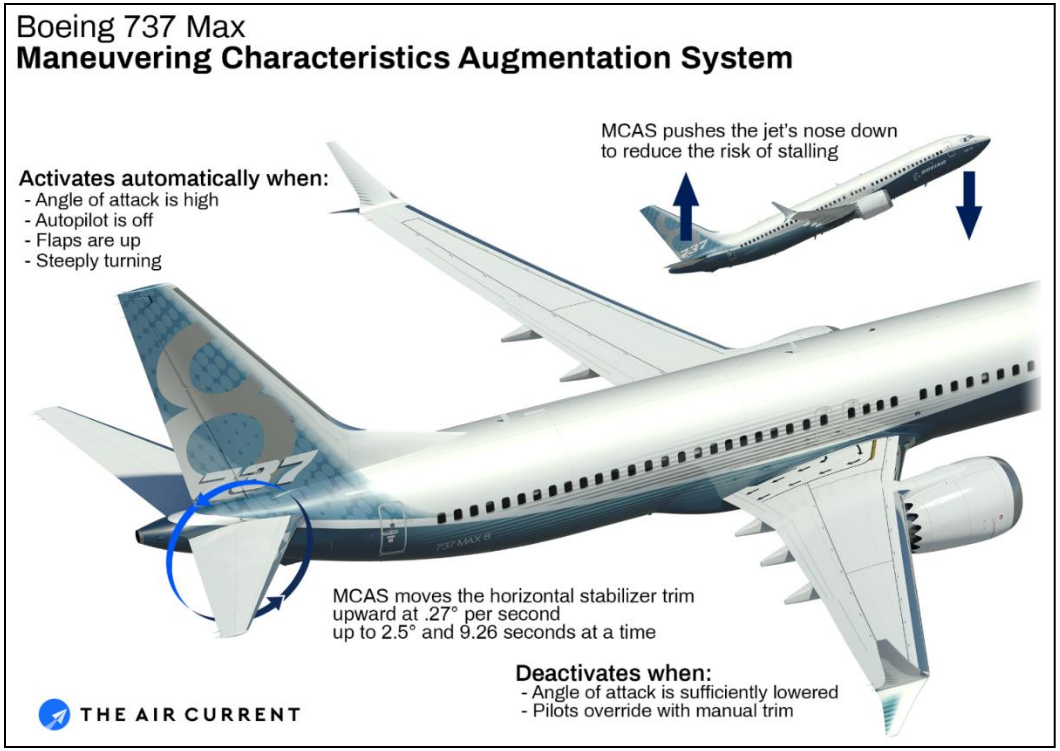


Space Software Engineering: Requirements Definition, Design, Production, Verification and Validation, Transfer, Operations and Maintenance.

Year 2018/19 Boeing 737 Max MCAS

- Boeing 737 Max, MCAS SW
  - Boeing's newest family of single-aisle airplanes
  - The fastest-selling airplane in Boeing history
    - About 5,000 orders
    - from more than 100 customers worldwide.
- MCAS
  - The Maneuvering Characteristics Augmentation System
  - It activates when the sensed Angle of Attack (AOA) exceeds a threshold based on airspeed and altitude.
  - That tilts the 737 Max's horizontal stabilizer upward at a rate of .27 degrees per second for a total travel of 2.5 degrees in just under 10 seconds.
  - How much the stabilizer moves depends on Mach number.
  - At higher Mach the stablizer moves less, at slower speeds it moves more.
  - The trim system under MCAS is no stopped by simply moving the control yoke.
- Accidents
  - Indonesia Lion Jet 610 [Oct 2018]: All 189 passengers dead.
  - Ethiopian Airline 302 [March 2019]: All 157 passengers dead.
- Possible cause
  - Malfunction at sensors for angle between the wings and the air current.
  - MCSA engaged to handle the situation, and it causes the nose to down.
  - The pilots tried to hold back the flight control, but failed.
  - The planes crashed

Close Investigation



https://theaircurrent.com/aviation-safety/what-is-the-boeing-737-max-maneuvering-characteristics-augmentation-system-mcas-jt610/

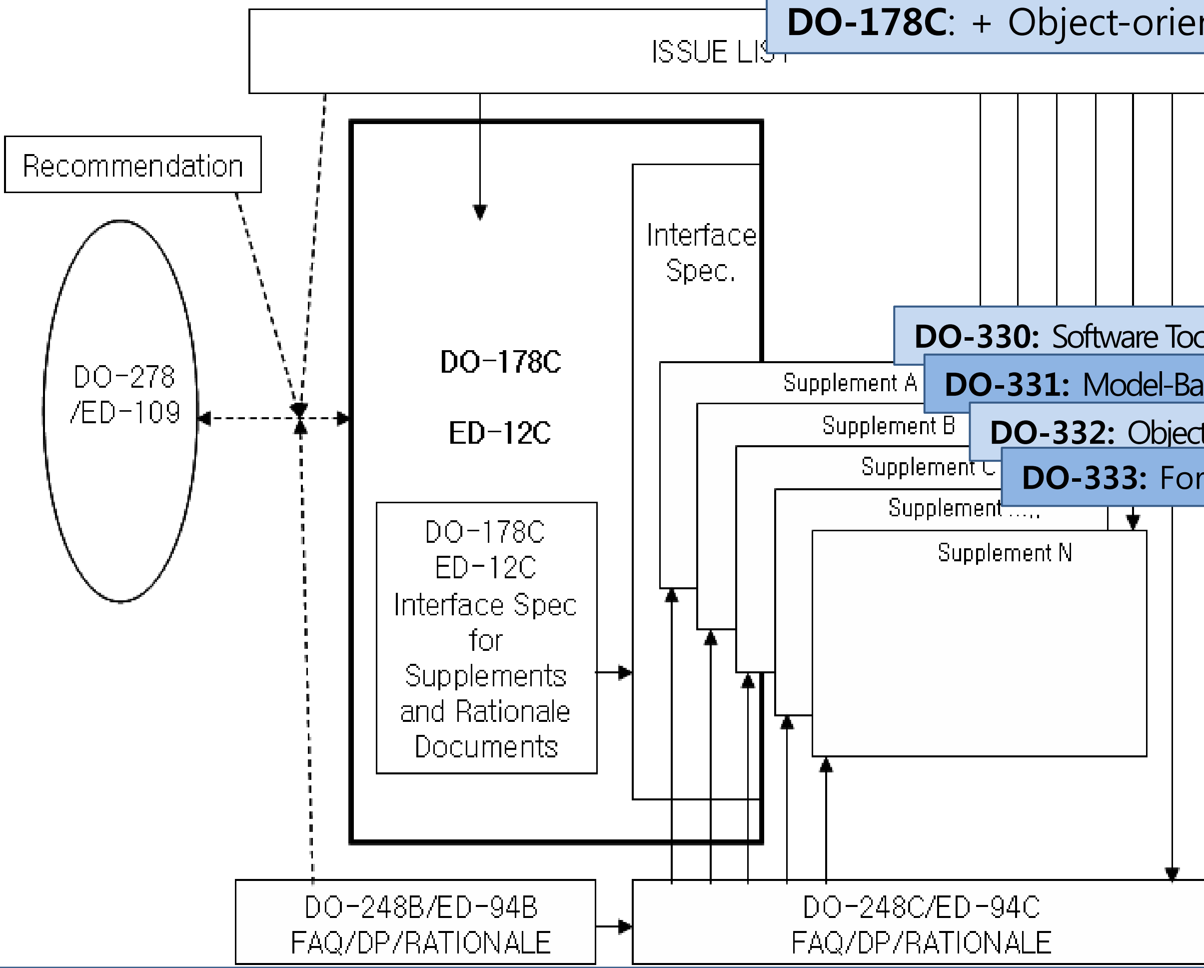
DO-178C (USA)

(~2013)

RTCA, EUROCAE
Software Considerations in Airborne Systems and Equipment Certification

DO-178B: Software Requirements and Software Design

DO-178C: + Object-oriented Programming



DO-330: Software Tool Qualification Considerations

DO-331: Model-Based Development and Verification

DO-332: Object-Oriented Technology and Related Techniques

DO-333: Formal Methods

International Standard Organizations and Their Standards

- ANSI: American National Standards Institute
- AIAA: American Institute of Aeronautics and Astronautics
- EIA: Electronic Industries Association
- IEC: International Electrotechnical Commission
- IEEE: Institute of Electrical and Electronics Engineers, Computer Society, SW Engineering Standards Committee
- ISO: International Organization for Standardization
- RTCA: Radio Technical Commission for Aeronautics
- EUROCAE: European Organization for Civil Aviation Equipment
- ECSS: European Cooperation for Space Standardization

Aerospace/ Avionics Systems	Railway Systems	Nuclear Power Plants	Automobile Systems	Embedded Systems	Defense Systems	Quality Business Mgmt
ECSS-E-40 DO-178C IEEE 12207 AIAA G-010-1993 CMMI	EN-50128	IEC-60880	ISO-26262 IEC 61508	IEC-61508	MIL-STD-882E	ISO9001

SMART SYSTEMS

Industry 4.0 & Smart Systems

- Smart
  - Home/Office/Car
  - City/Factory/Building
- Characteristics
  - Big Data
  - Intelligence
  - Automation
- Requirements
  - Safety
  - Security
  - Reliability

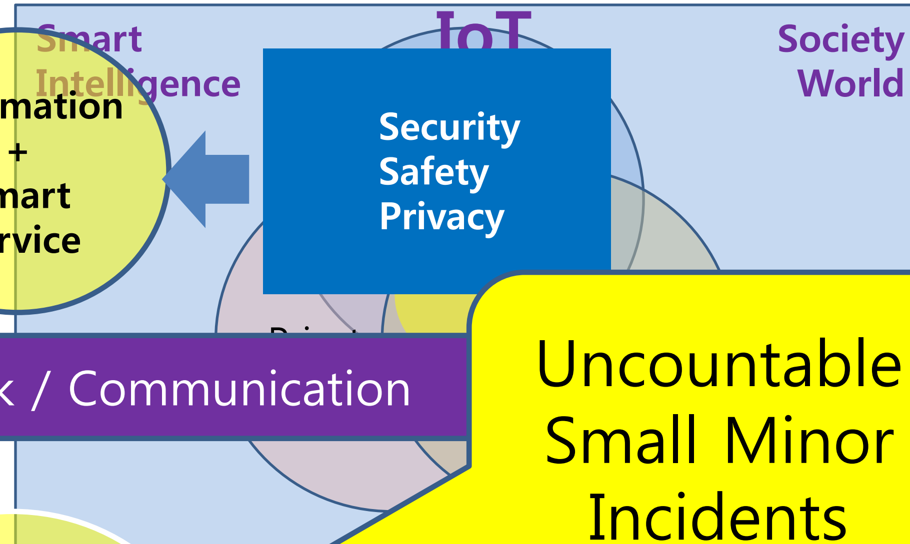
IoT: Internet of Things

- Trend
  - Automation
  - Ubiqu
  - Smar
- Characte
  - Identi
  - Sensi
  - Netwo…ing
  - Processing
- Technolo
  - RFID,
  - Middleware
  - Searching/browsing
- Goal: Convergence
  - Private sectors
    - Industries
    - Business
    - Financial/banking
    - Health care
    - Traffic systems
  - Public sectors
    - Admin sector
- Requirements
  - Specification
  - Verification
- Main issues
  - Security
  - Privacy

Distribution
Mobility
Communication
Process Control
Temporality

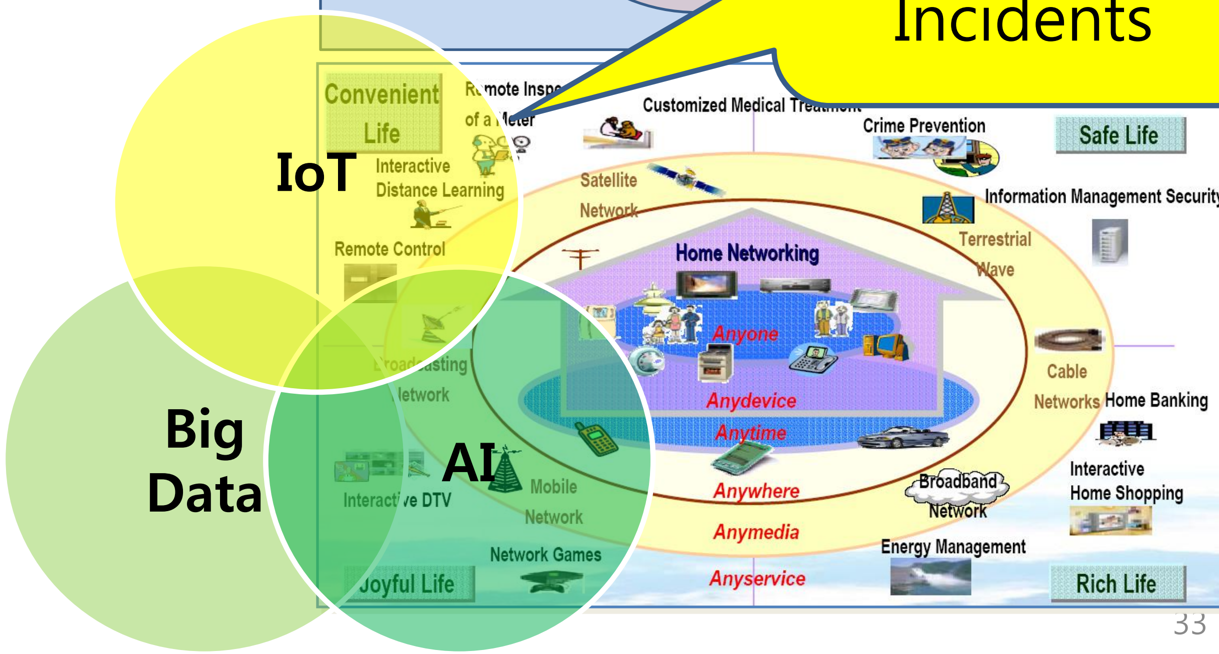
Automation + Smart Service

Security
Safety
Privacy



Internet / Network / Communication

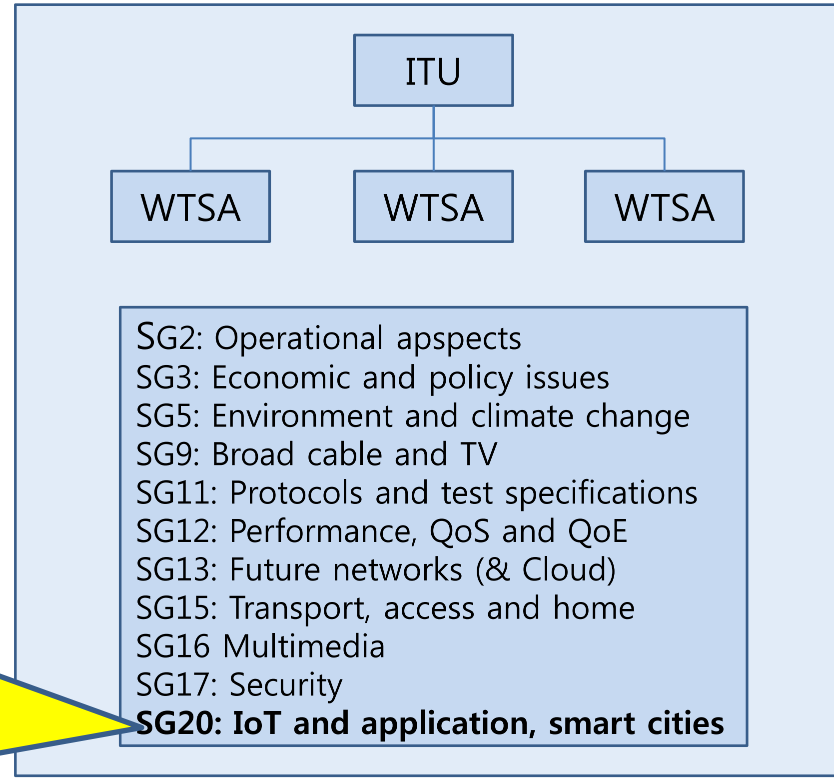
Uncountable Small Minor Incidents

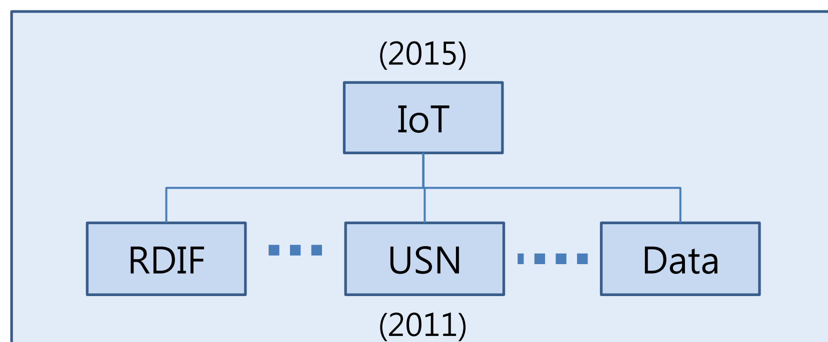


IoT Standard

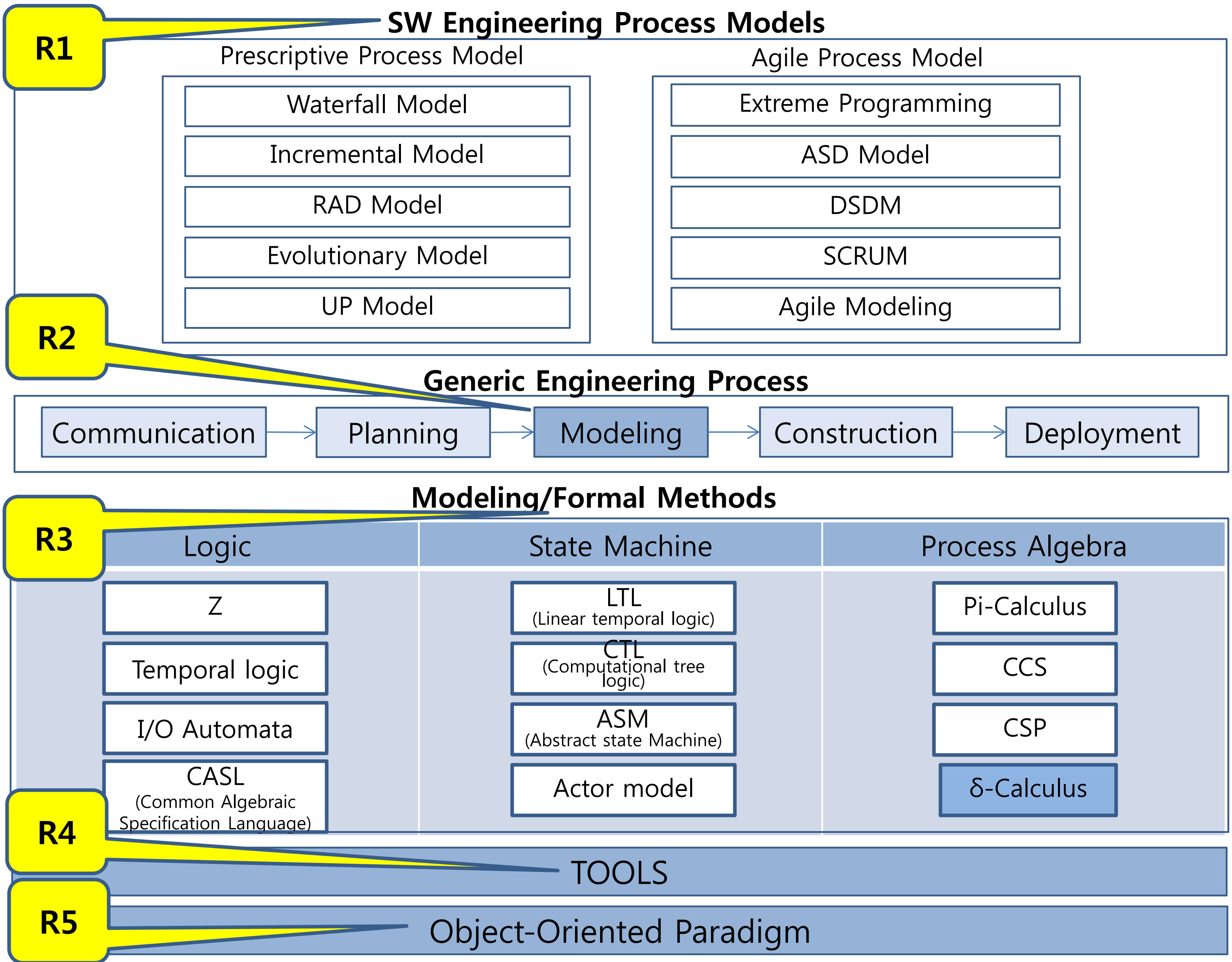
- Smart City, Smart Life, and Smart World
- International standard for IoT applications
- ITU (Internation Telecommunication Union)
  - 15 June '15, Geneva
  - ITU-T SG20: IoT Standardization
- Plan for standardization
  - M2M(machine-to-machine) communication
  - Ubiquitous sensor network
  - Mechanism for IoT app. interoperability
  - E2E(end-to-end) architecture
- Goal: IoT standard p
- Application area: Int
  1) Industrial sector
     - Health care
     - Electronic device
     - Traffic systems
  2) Business sector
     - Financial systems
     - Banking systems
  3) Administration systems
     - Local government
     - Central government
- Target
  - 2020: To connect 50 Billion things

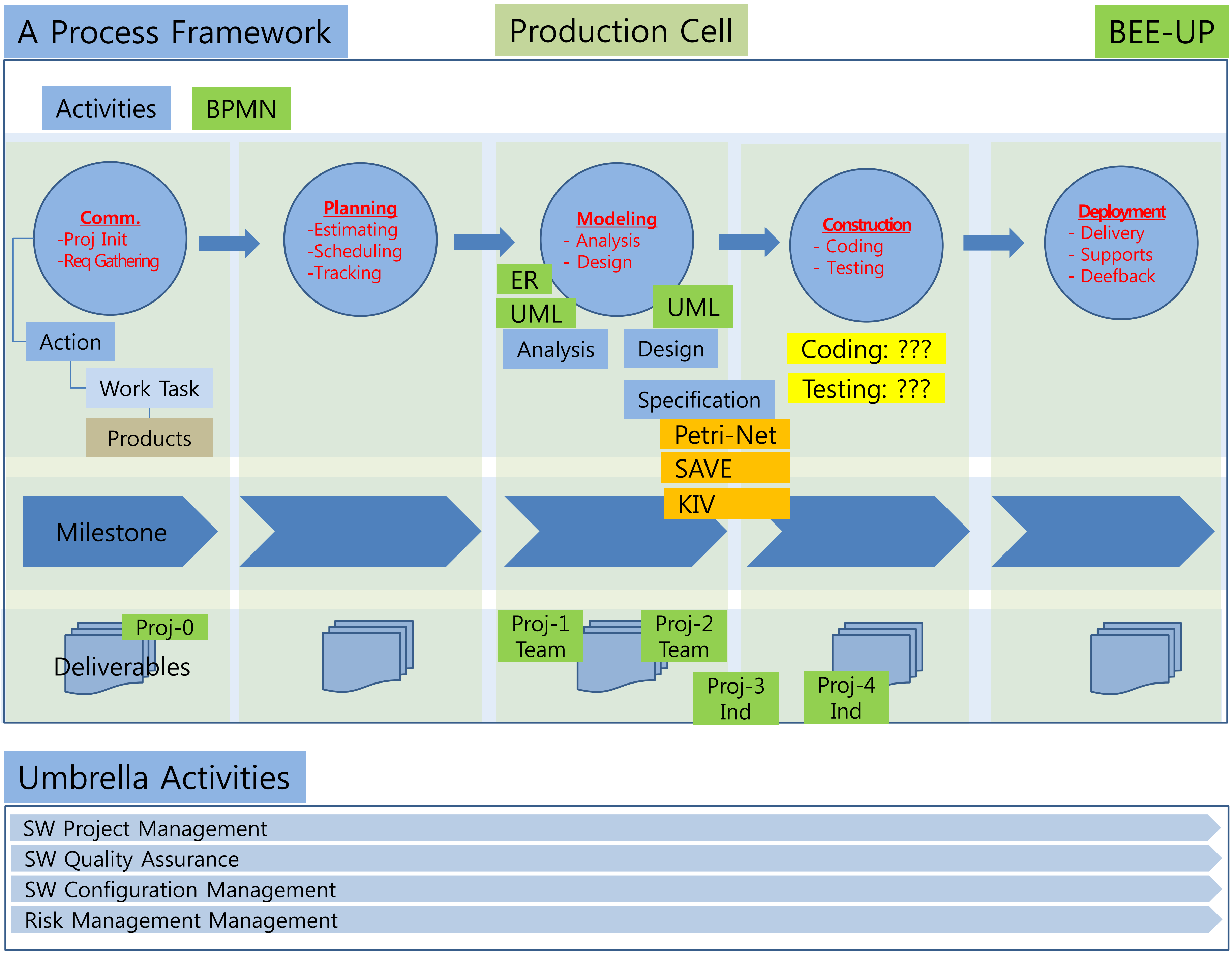
What kind of Requirements?





Motivation: SW Engieering Requirements from ECSS Standard

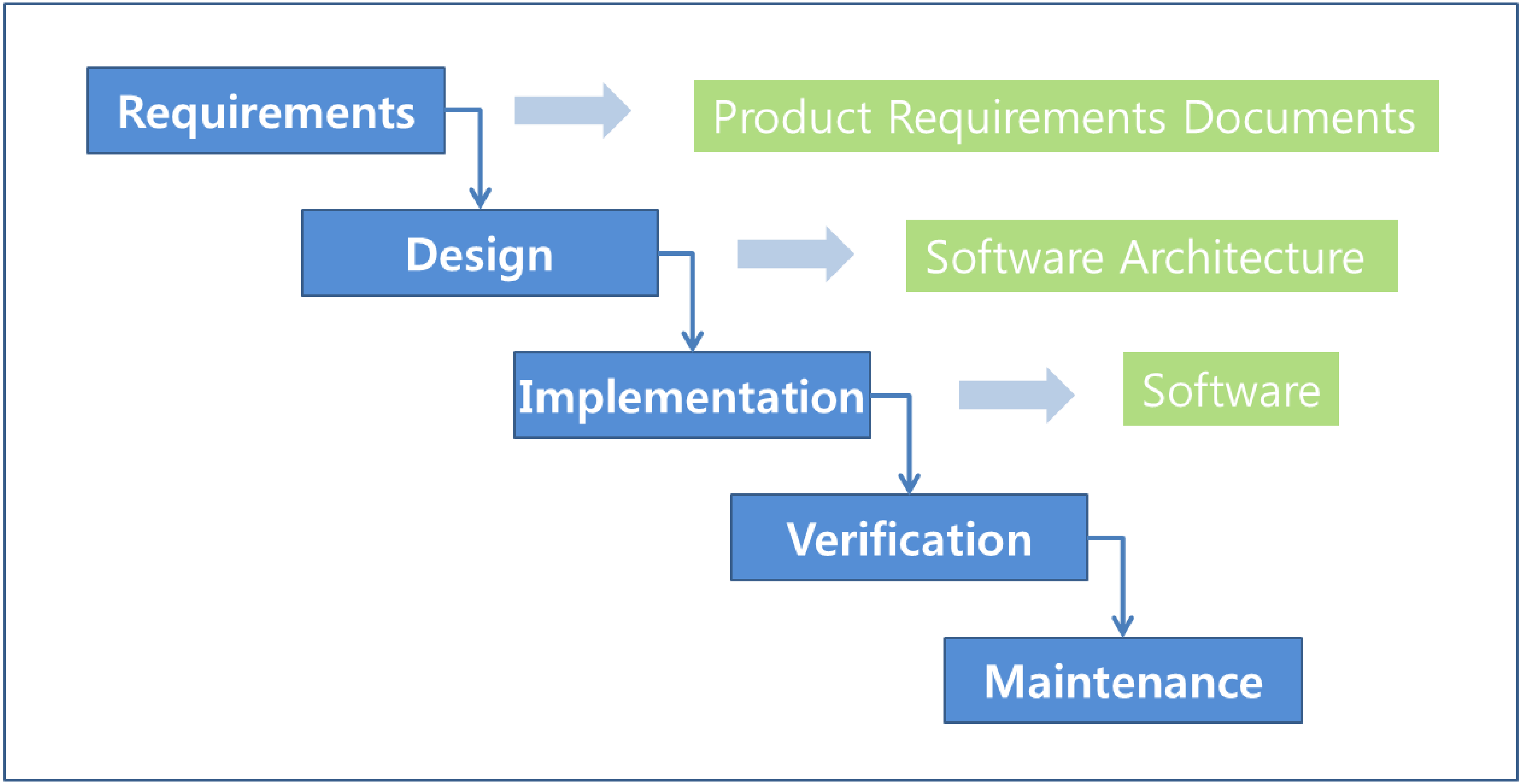

R1
SW Engineering Process Models
Prescriptive Process Model
Waterfall Model
Incremental Model
RAD Model
Evolutionary Model
UP Model
Agile Process Model
Extreme Programming
ASD Model
DSDM
SCRUM
Agile Modeling
R2
Generic Engineering Process
Communication
Planning
Modeling
Construction
Deployment
R3
Modeling/Formal Methods
Logic
Z
Temporal logic
I/O Automata
CASL (Common Algebraic Specification Language)
State Machine
LTL (Linear temporal logic)
CTL (Computational tree logic)
ASM (Abstract state Machine)
Actor model
Process Algebra
Pi-Calculus
CCS
CSP
δ-Calculus
R4
TOOLS
R5
Object-Oriented Paradigm



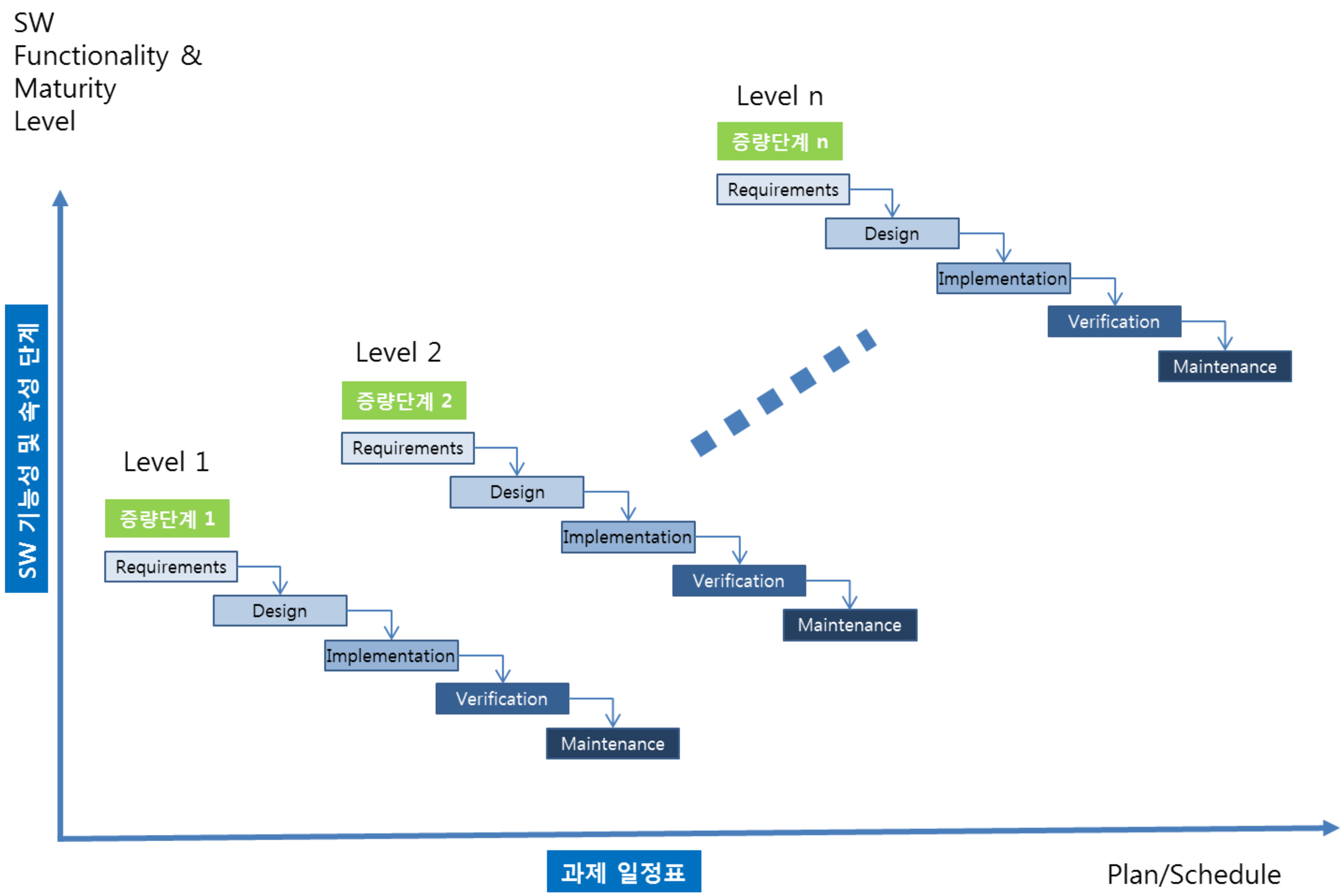
A Process Framework
Production Cell
BEE-UP
Activities
BPMN
Comm.
-Proj Init
-Req Gathering
Planning
-Estimating
-Scheduling
-Tracking
Modeling
- Analysis
- Design
Construction
- Coding
- Testing
Deployment
- Delivery
- Supports
- Deefback
Action
Work Task
Products
ER
UML
UML
Analysis
Design
Specification
Petri-Net
SAVE
KIV
Coding: ???
Testing: ???
Milestone
Proj-0
Deliverables
Proj-1 Team
Proj-2 Team
Proj-3 Ind
Proj-4 Ind
Umbrella Activities
SW Project Management
SW Quality Assurance
SW Configuration Management
Risk Management Management

Prescriptive
SE Process Model

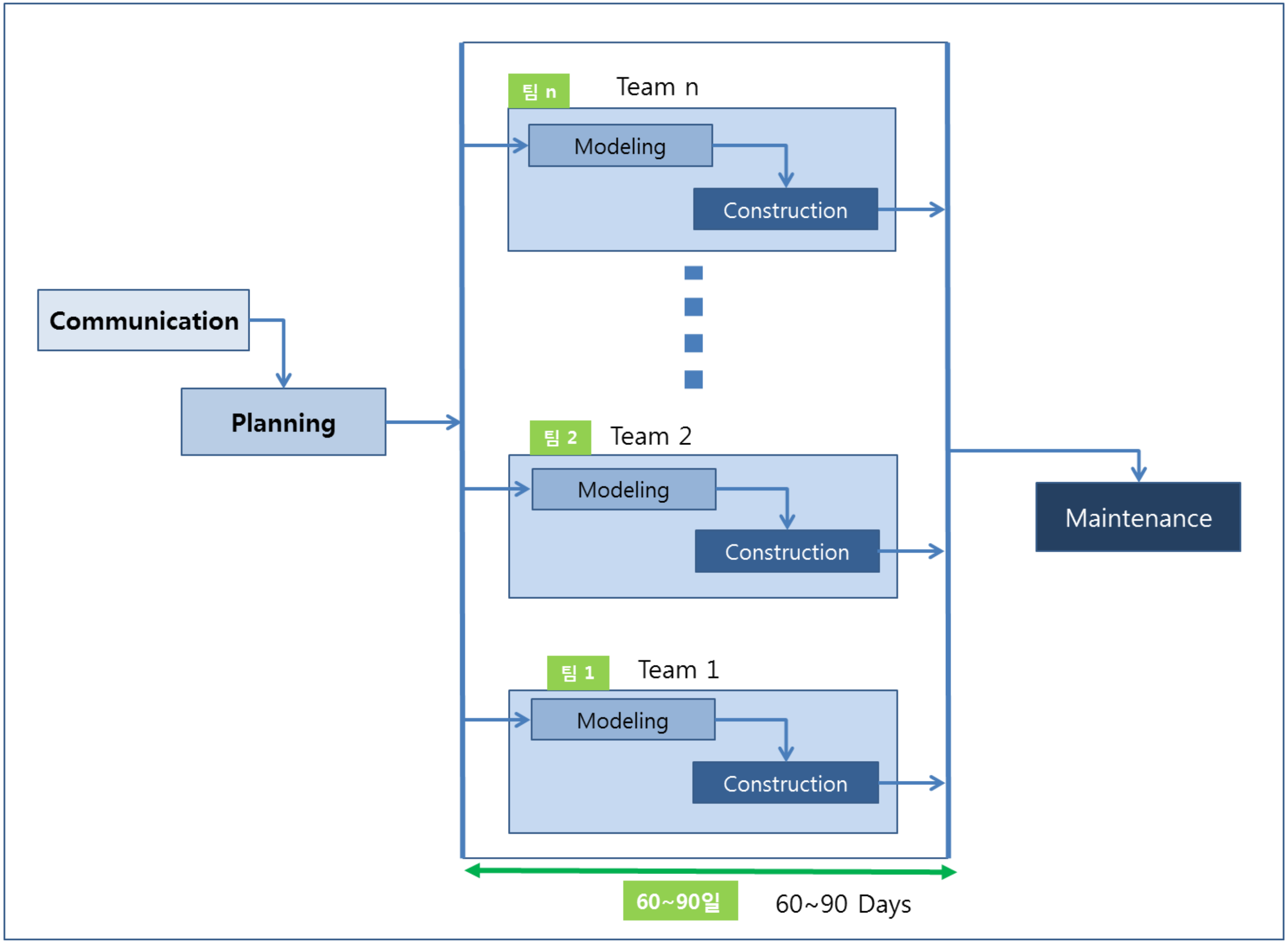
Waterfall Model



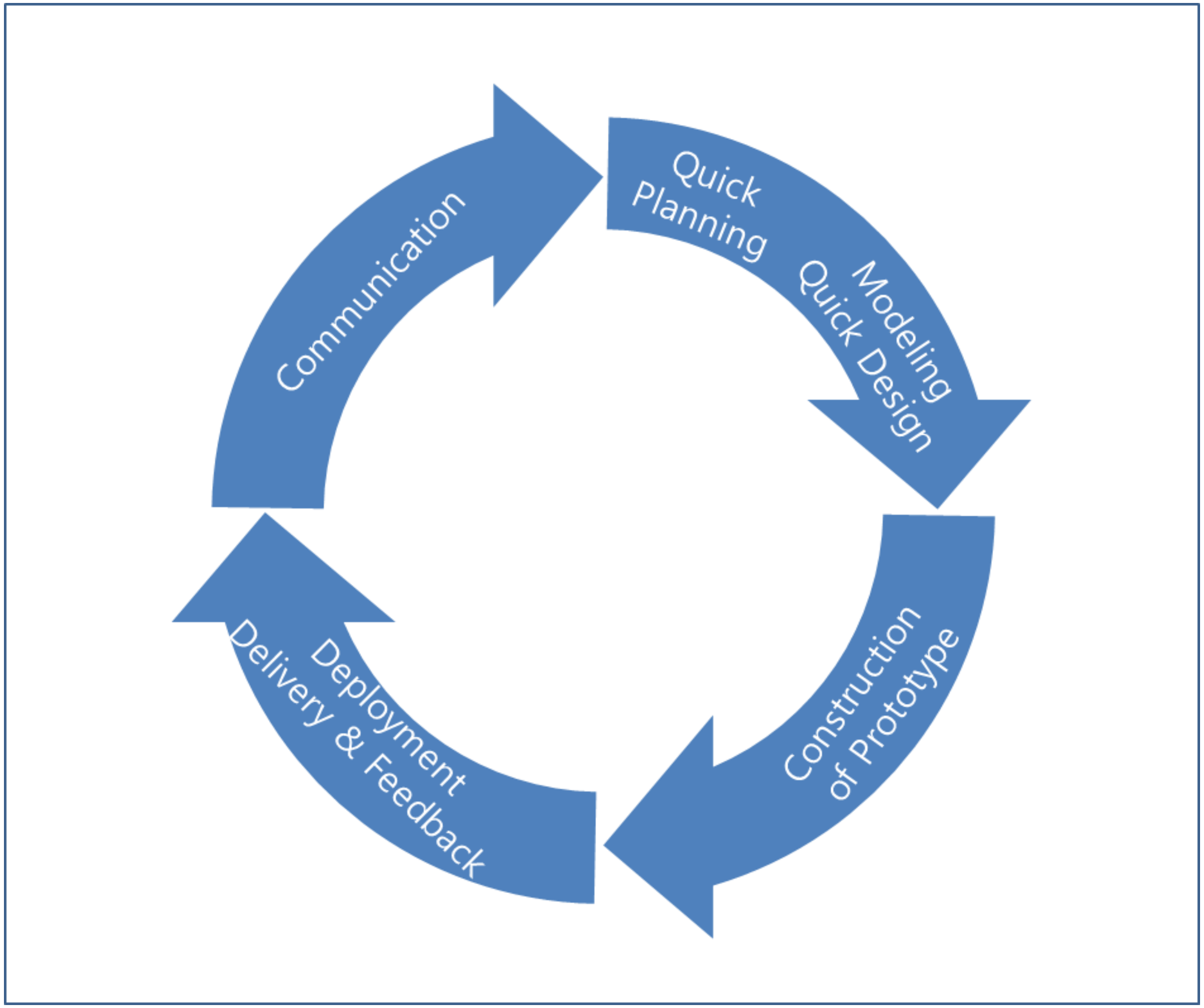
Incremental Model



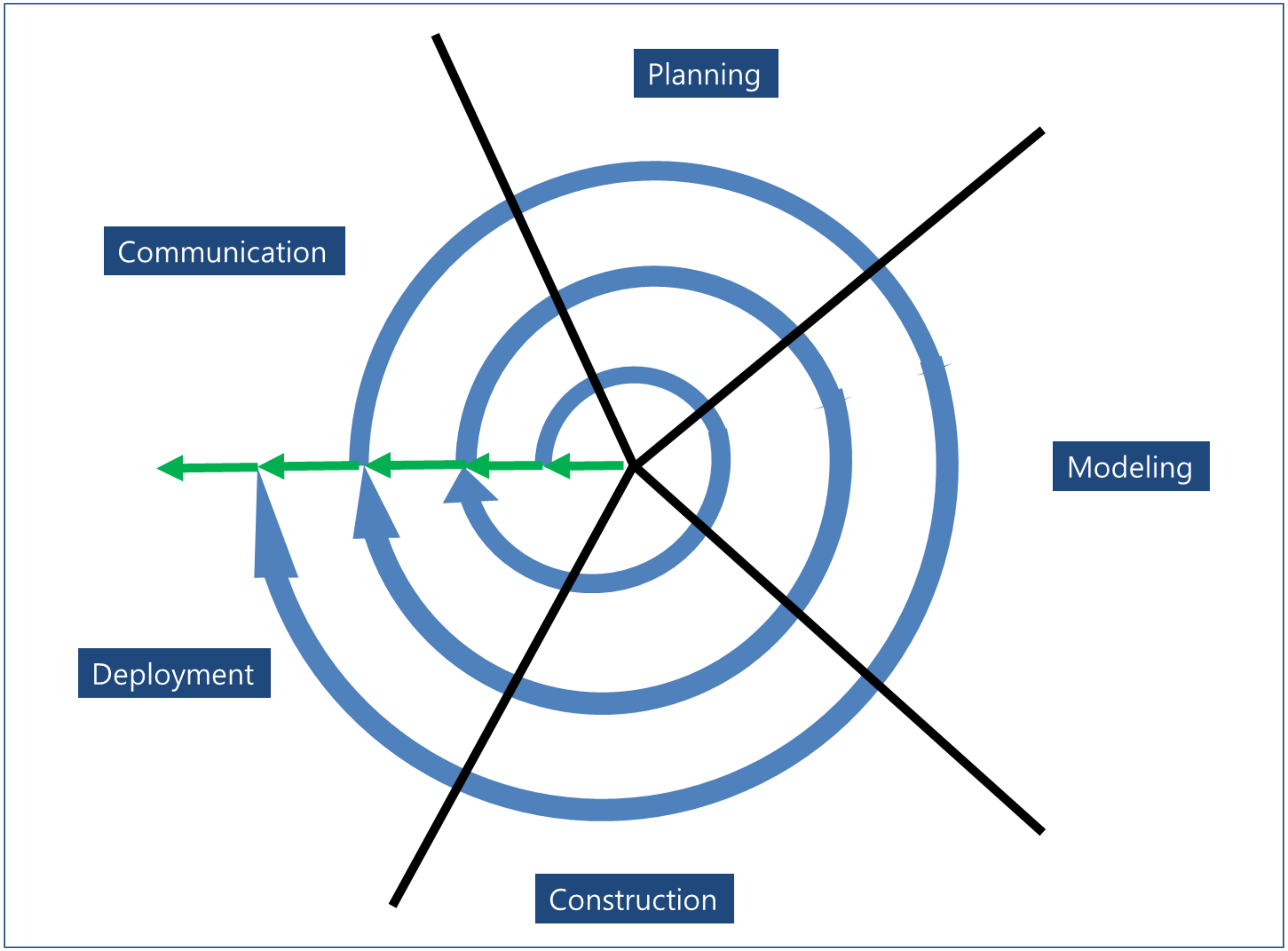
Rapid Application Development (RAD) Model



Prototyping Model

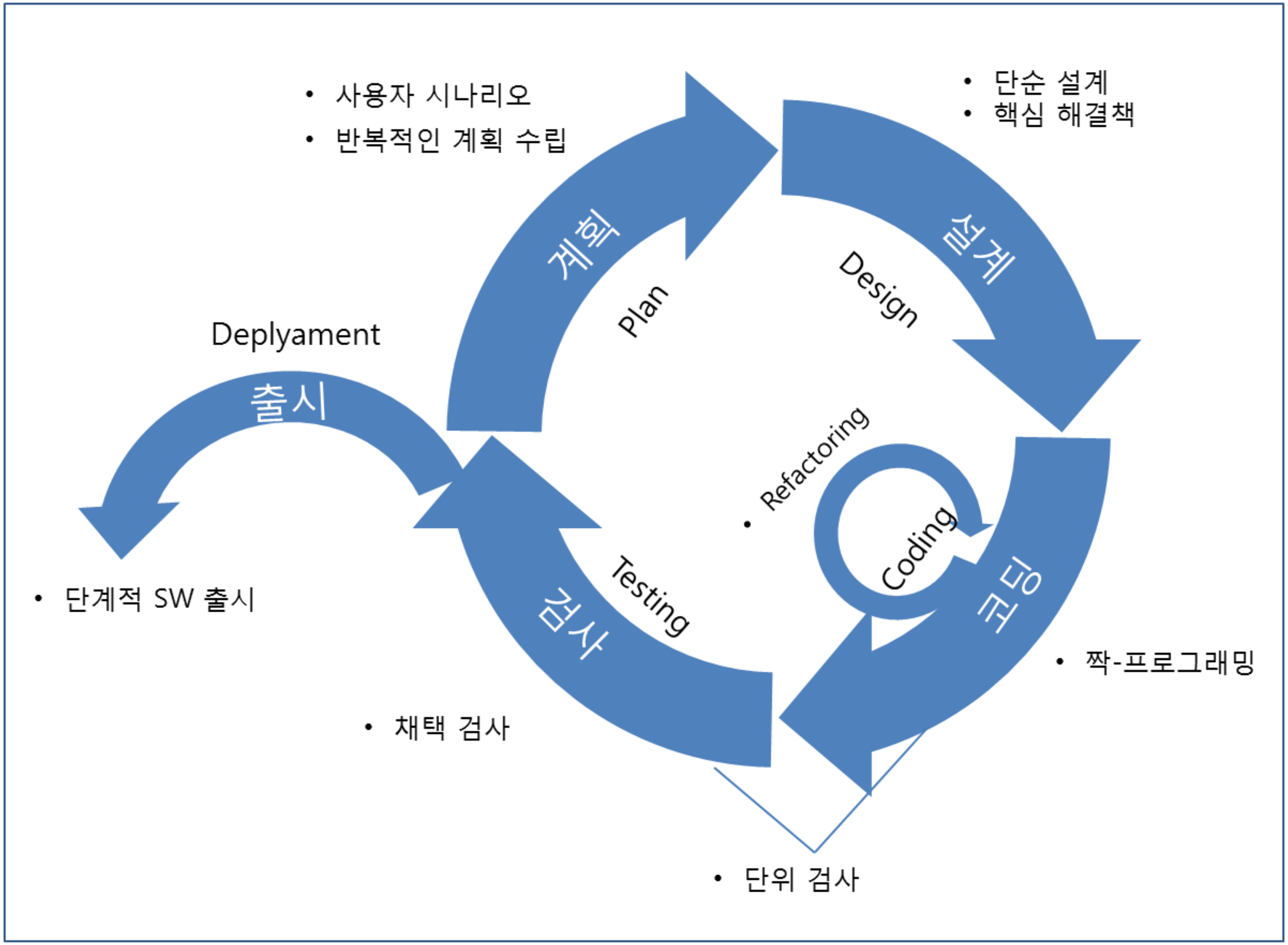


Spiral Model

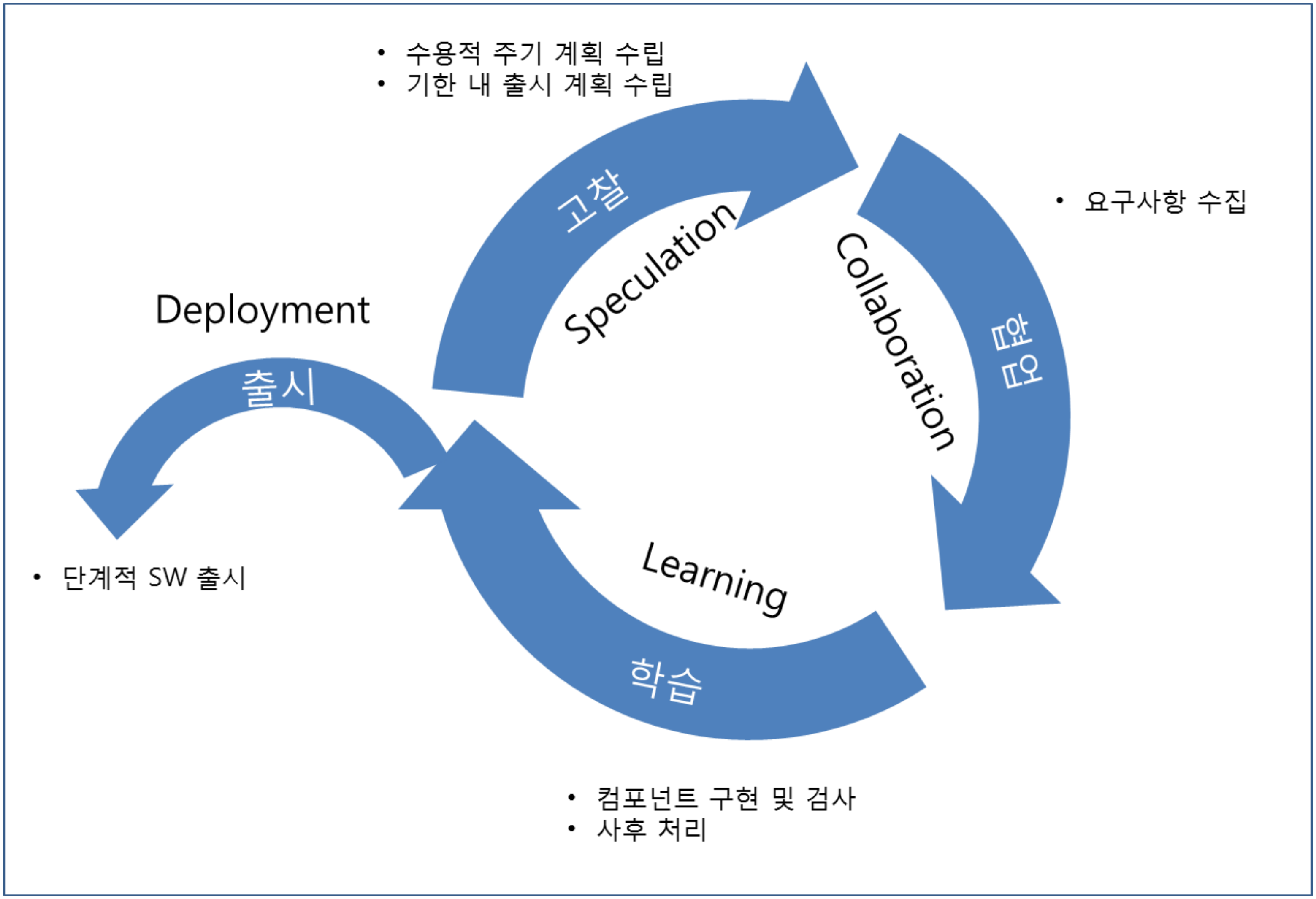


Agile
SE Process Model

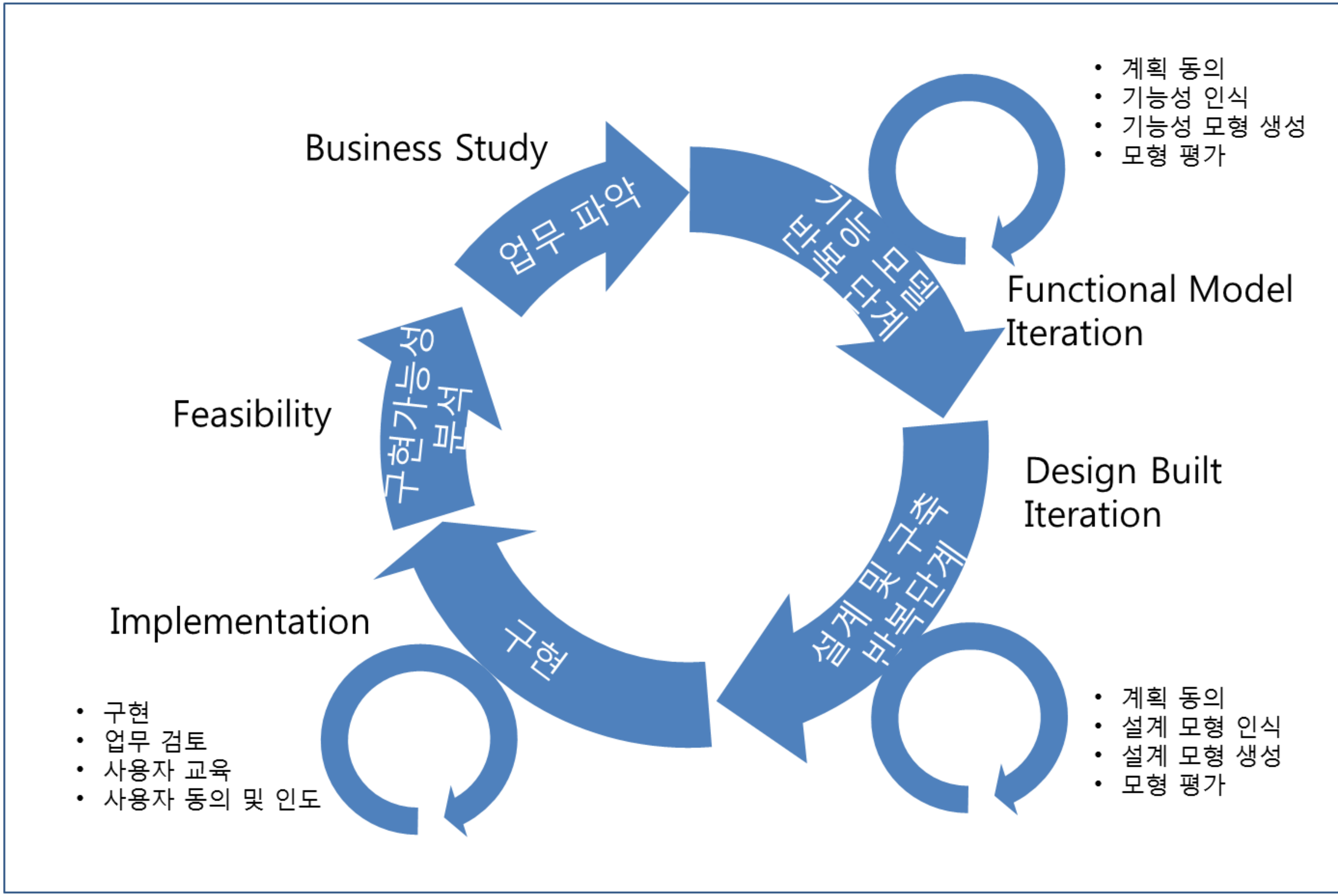
Extreme Programming (XP) Model



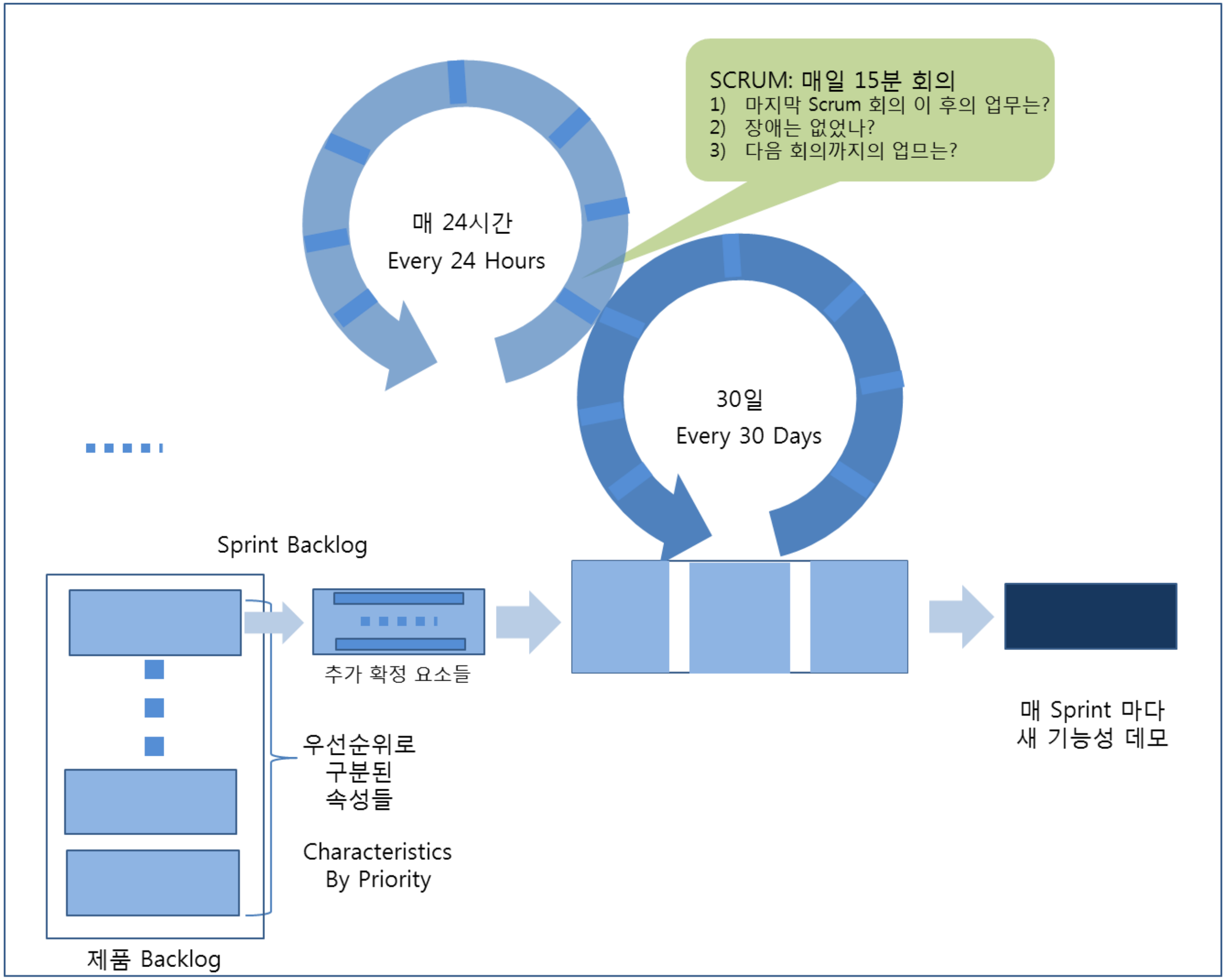
Adaptive Software Development (ASD) Model



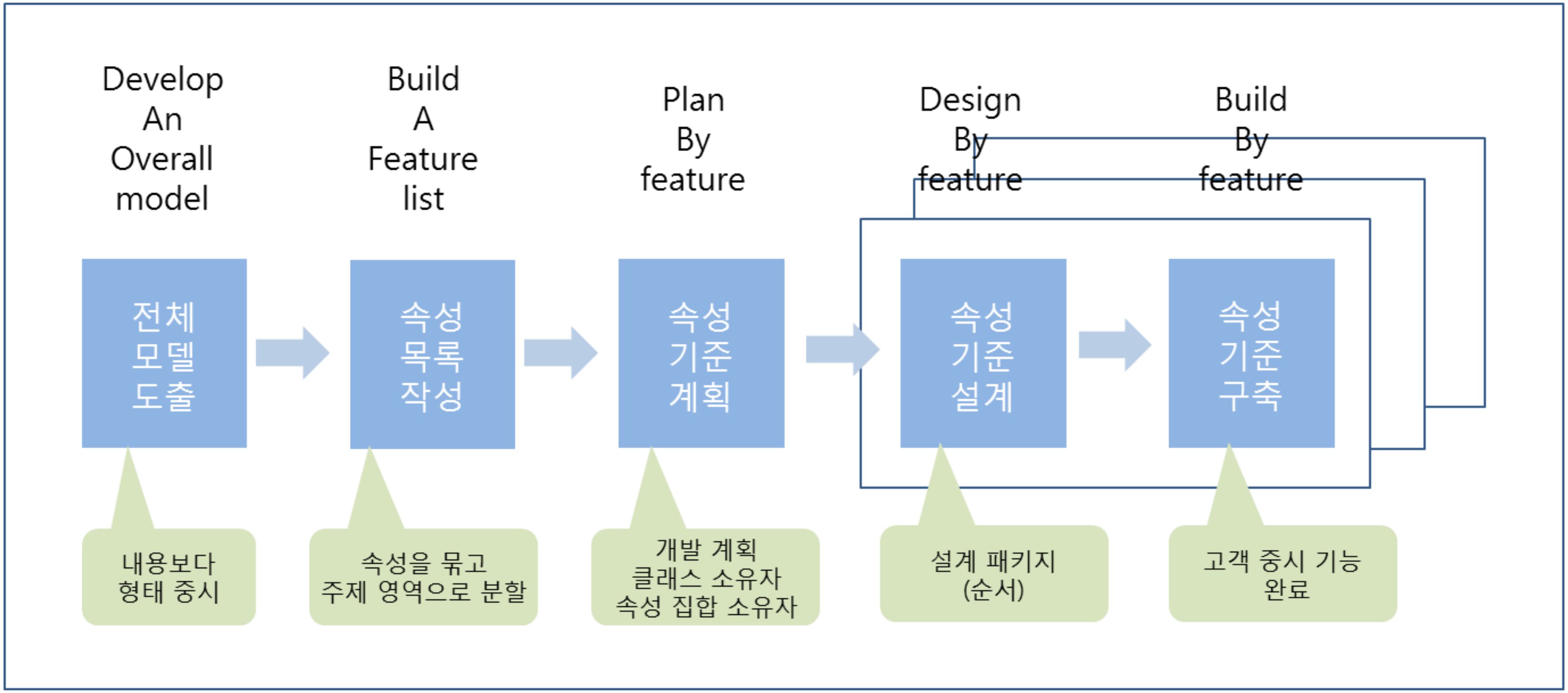
Dynamic Systems Development Method (DSDM) Model



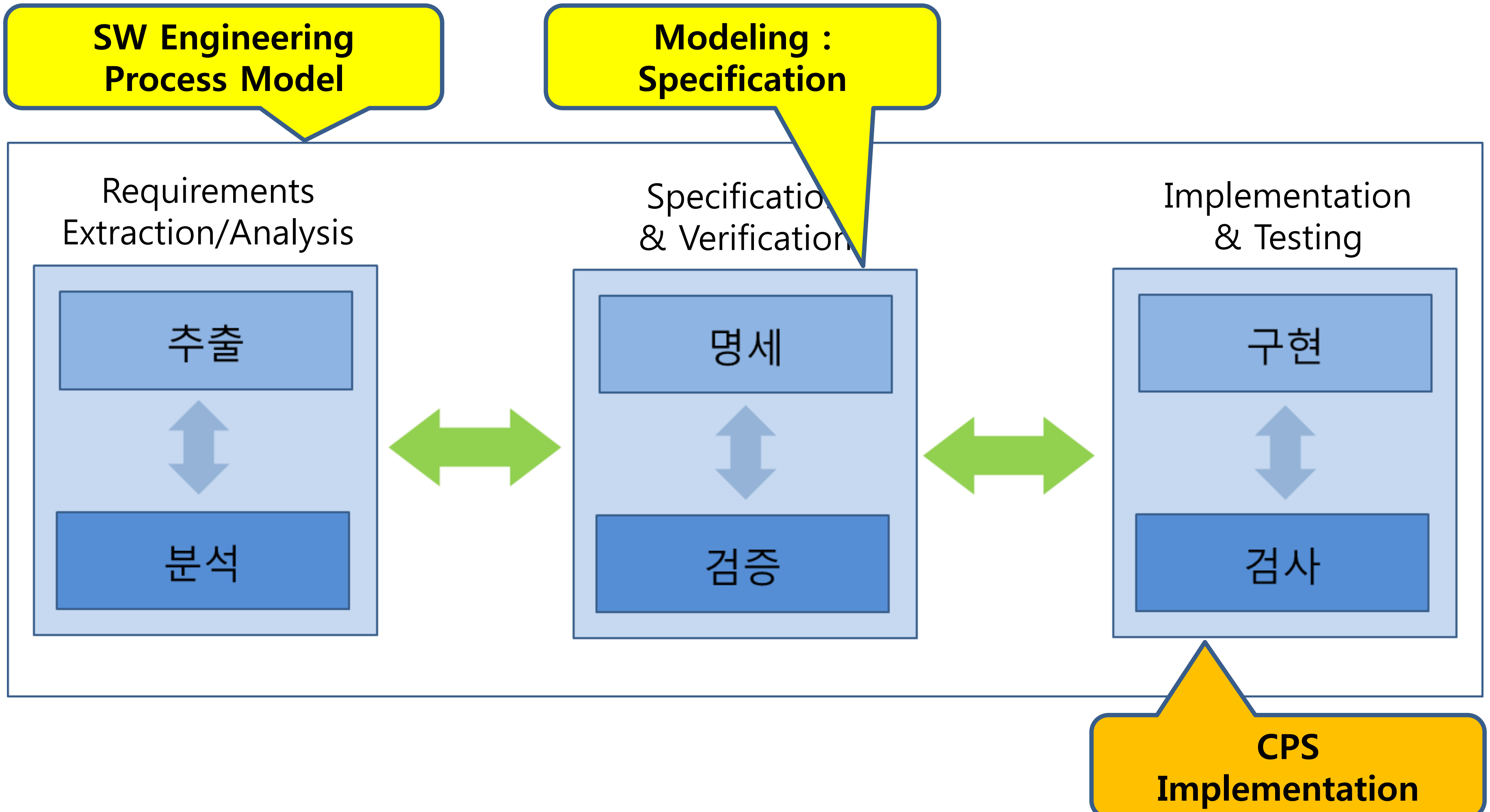
SCRUM Model


SCRUM: 매일 15분 회의
1) 마지막 Scrum 회의 이 후의 업무는?
2) 장애는 없었나?
3) 다음 회의까지의 업므는?
매 24시간
Every 24 Hours
30일
Every 30 Days
Sprint Backlog
추가 확정 요소들
우선순위로
구분된
속성들
Characteristics
By Priority
제품 Backlog
매 Sprint 마다
새 기능성 데모

Feature Driven Development (FAA) Model



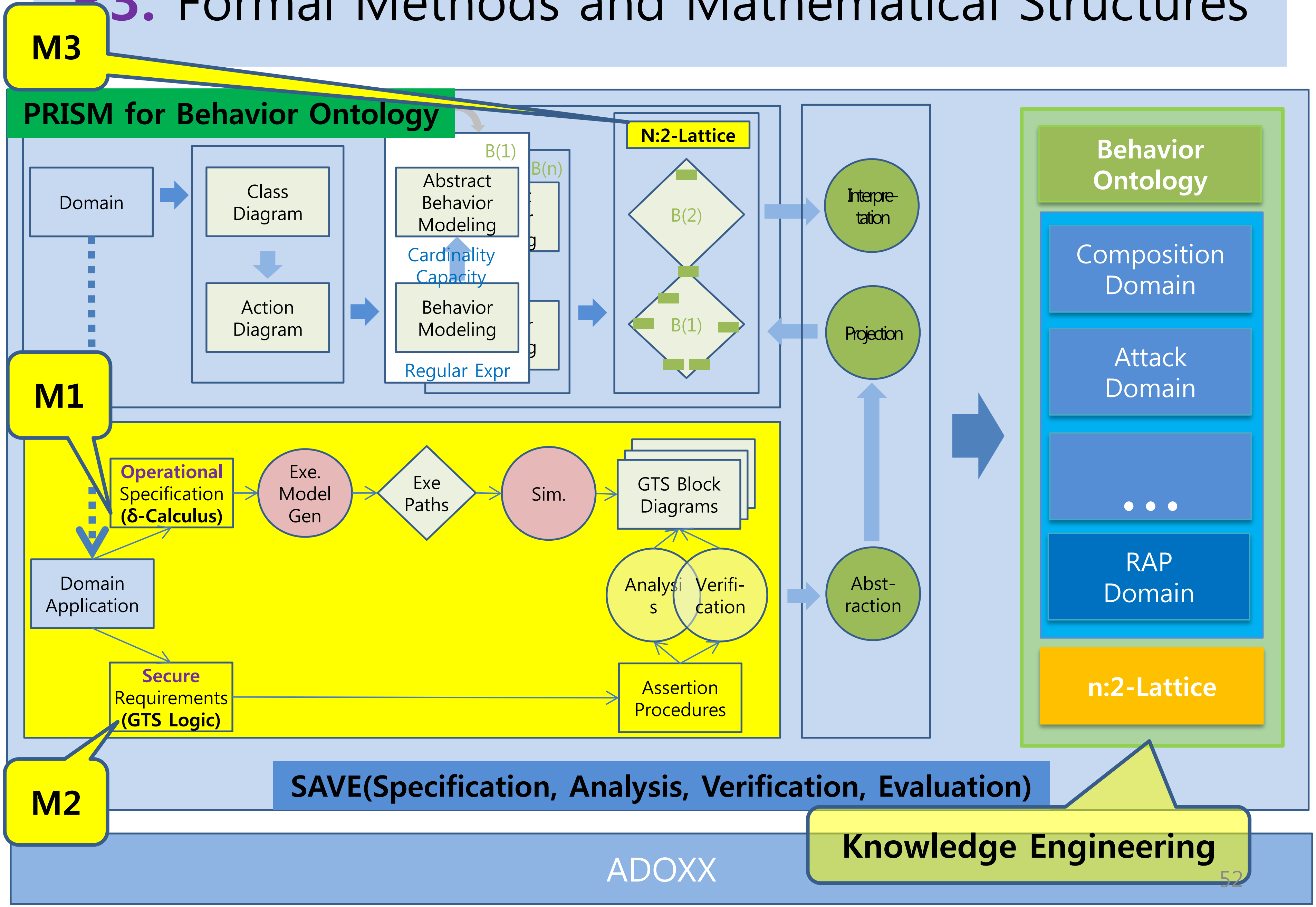
R1 & R2: FMM: Formal Method Model



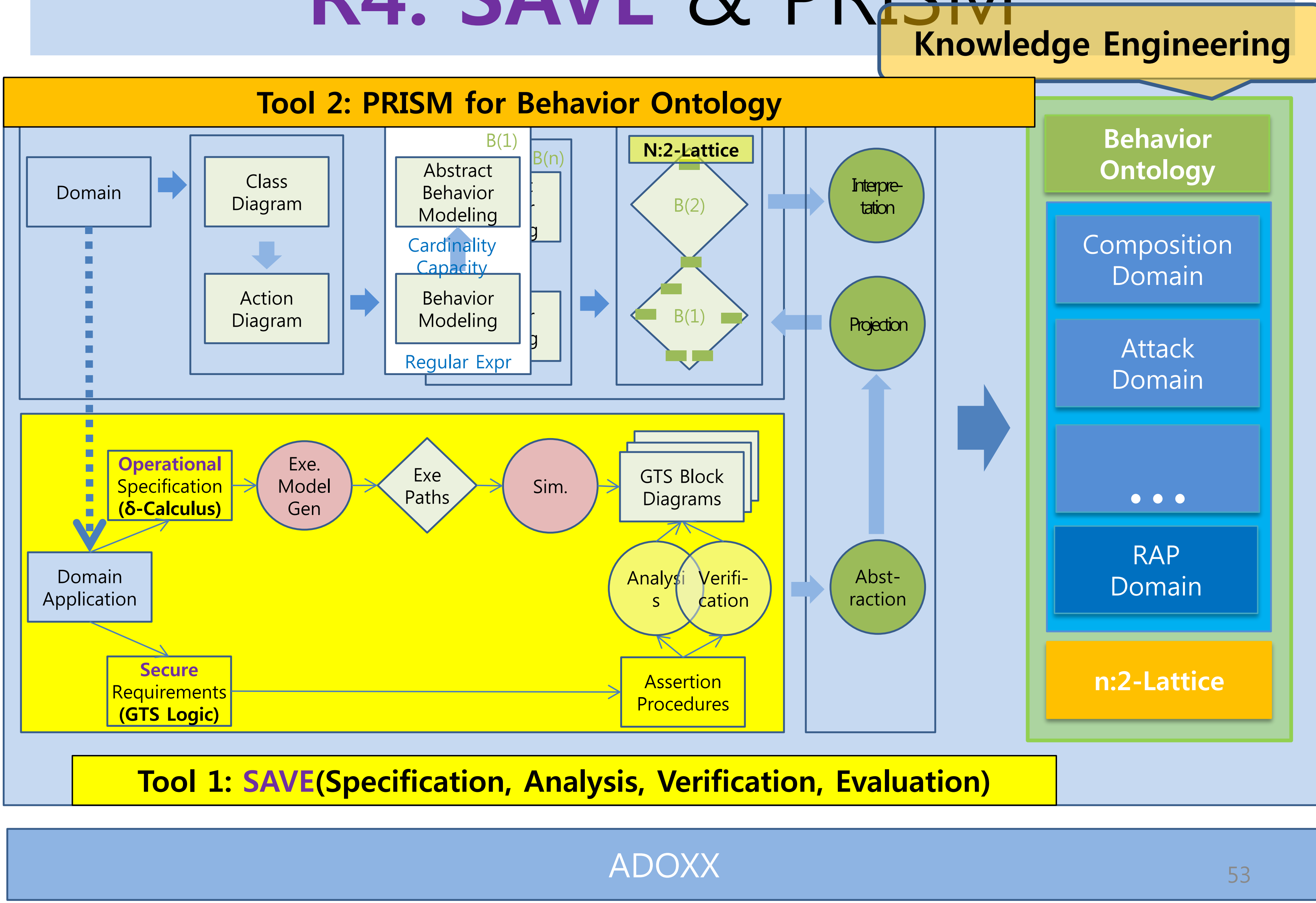
Formal Methods

Types	Typical Methods	Characteristics	Cons
Data/Logic-Based	Z Temporal Logic CASL, etc.	- Formal - Text-based - Consistency - Validity - Completeness - Soundness	
State Machine-Based	Statechart Modechart Petri Net Timed Petri Net, etc.	- Reachability - Graph-based - Structured/Hierarchy - Reactive System - Priority - Temporal properties	- Abstraction - Mobility - Syntax
Process Algebra-Based	CCS CSP ACP ACSR LOTOS Pi-Calculus Mobile Ambient, etc.	- In The Large - In The Small - Formal/Algebra - Abstraction - Equivalence: weak/strong - Bisimulation - Resource - Priority - Time - Mobility	- Understandability - Visualization

P3: Formal Methods and Mathematical Structures



R4: SAVE & PRISM



R5: Object-Oriented Paradigm