A Model-based Decision Support Framework for Security Architecture Design Decision-Making

Robin Theveniaut, Brahim Hamid, Jason Jaskolka

Department of Systems and Computer Engineering
Carleton University, Ottawa, ON, Canada
RobinTheveniaut@carleton.ca
CyberSEA Research Lab

Toulouse Computer Science Research Institute
IRIT, Toulouse, France
robin.theveniaut@irit.fr
IRIT Research Lab

5th December 2025

SCADA scenario

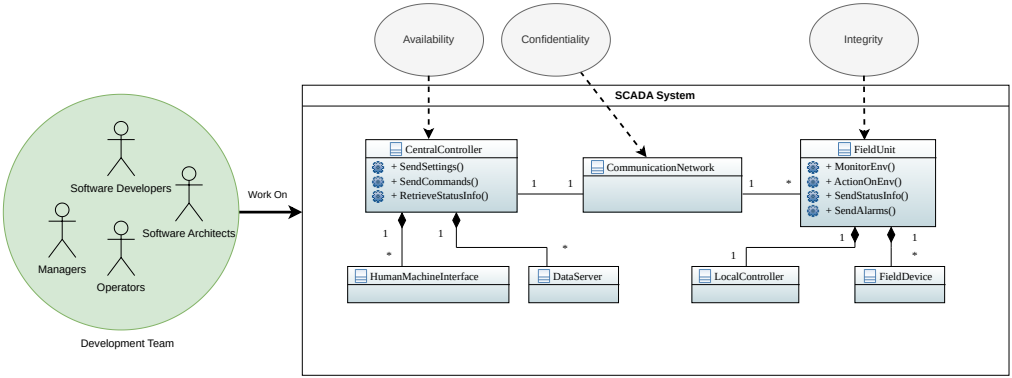

Figure: SCADA Scenario

How can we make decisions ?

State of the Art

- Collaborative decision-making methods
- Conflicts handling in decision-making
- Tools for Software Architecture decision-making

Decision-making methods

- **Brainstorming** : discussion by a team with a **facilitator**. Each member can give its opinion.
- **Voting** : each member casts vote with several solutions listed for each issue.
- **Delphi** : panel of experts and several iterations of questionnaire with pre-defined stop criterion. The mean or median scores of the final rounds are used to determine the results.
- **Consensus** : dynamic and iterative group discussion process coordinated by a **moderator** helping experts to bring their opinions closer. If a threshold for decision is not met, discussions continues in an iterative way until they get to a decision.
- **Analytic Hierarchy Process** : pairwise comparison of alternatives by each team member. Problem is modeled as goals alternatives and criteria.

Conflict resolution styles

- **Collaboration** (WinWin) : people give each other their point of view, explanation and reasons on their interest.
- **Compromise** : Both sides give up on something, may result in quick resolution but might not be the best solution.
- **Competition** : Compete to win and make the other person lose.
- **Accommodation** : Letting the other person win/do what they want.
- **Avoidance** : Knows there is a problem but acts like there is no problem at all.

Decision-Making Tools

Approach/Criteria	Preference Indication	Prioritizing group members	Provision for conflict resolution	Group decision rules	Information exchange and recall	Revisiting information
CoCoADvISE	-	++	-	-	+	+
Decision Buddy	++	-	-	-	++	++
SAW	++	-	-	-	++	+
GADget	++	-	-	-	+	++
LGDM	++	+	++	-	-	++
HFGDM	++	++	+	++	++	++

Table: Comparison of the different existing approaches for collaborative decision-making with our approach

Building a meta-model for Decision-Making Support

Concepts from existing meta-models

SADD : Project, Category, Design Decision, Alternative. (in orange)
TP : Actor, Development Team Profile. (in brown)

Decision-making support meta-model

Design Time : Concepts we need when setting up the support.
Run Time : Concepts used during execution of the decision-making process.
A Domain Specific Language has been developed for both of these phases.

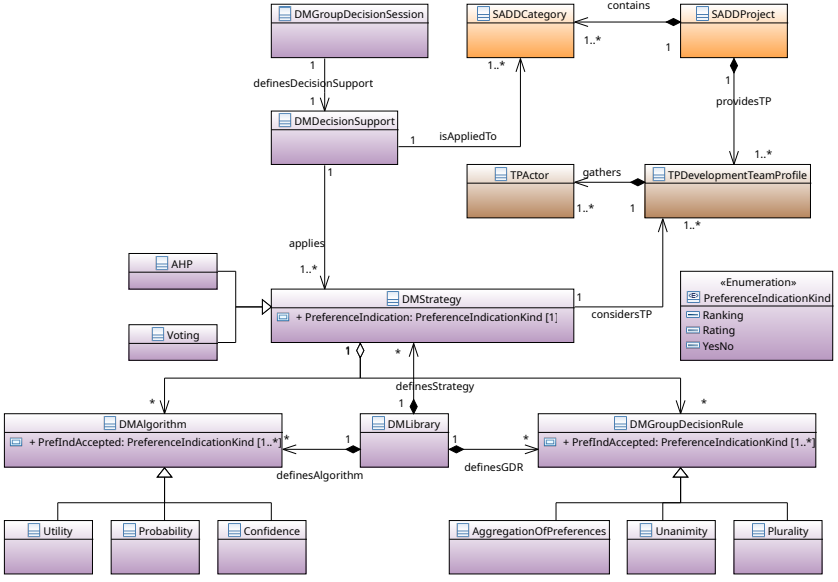

Figure: Decision-Making Support meta-model at Design Time

Decision-Making Support Design Time - DSL

```
1  Library rules
2  decisionrule Majority (Rating Ranking YesNo)"Selects the
       choices having more than 50% of the votes."
3  decisionrule RelativeMajority (Rating Ranking YesNo) "
       Selects the choices with the most votes."
4  decisionrule AggregationOfPreferences (Rating YesNo) "
       Aggregates preferences"
5  decisionrule pairwiseComparison (YesNo) "comparison of
       solutions in set of two with multiple iterations"
6  decisionrule weightingCriteria (Rating) "actors weight the
       criteria of the solutions"
7  algorithm Confidence (Rating Ranking YesNo) considersTP yes
        "Set weights on the different team profiles to
       select the choice with the most weight."
8  algorithm Utility (Rating) considersTP no "function
       associating a weight to each alternative indicating
       its expediency according to its consequences"
9  Strategy Brainstorming {decisionrule Unanimity}
10 Strategy Voting {decisionrule Majority }
11 Strategy Delphi {decisionrule numberIterations
12     then algorithm meanscore
13     then algorithm medianscore}
```

Listing: Decision-Making Support Library

```
1  import "scada_authentication.secadd"
2  import "scada.secadd"
3  import "library.dm"
4  import "scada.teamprofile"
5  DesignTime {
6    DecisionSupport SCADADecisionMaking
7      decidesFor CatAuthorizationActiveComponent {
8          Strategy rules.Voting with preference indication
               Rating
9          Strategy StratAuthorizaionActiveComponent with
               preference indication Rating {
10             decisionrule rules.Unanimity
11             for Expert_Authorization Advanced_Authorization
12             then decisionrule rules.SuperMajority
13             for Expert_Authorization Advanced_Authorization
14             then algorithm rules.Confidence}
15 }}
```

Listing: Decision-Making Support at Design Time

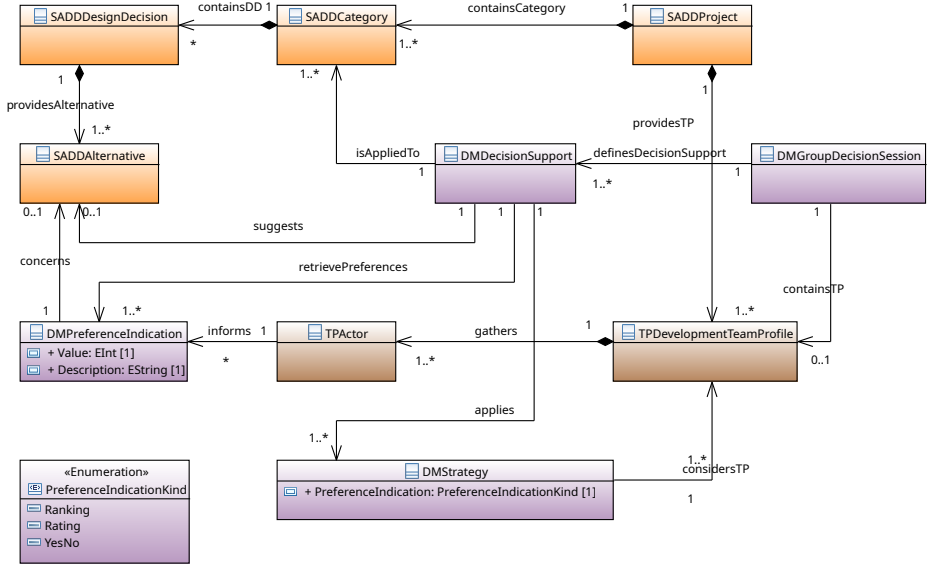

Figure: Decision-Making Support meta-model at Run Time

Inputs - Security Human Factors and Team Profiles

Security HF	Authentication		Authorization	
Actors	Skill	Exp	Skill	Exp
Alice	5	4	4	5
Bob	4	2	4	5
Carlos	2	1	1	1
David	2	1	3	2

Table: Evaluation results of each actor's security human factors

Actors	TP Authentication	TP Authorization
Alice	Expert	Expert
Bob	Advanced	Expert
Carlos	Beginner	Beginner
David	Beginner	Advanced

Table: Team profile assignment to actors

Decision-Making Support Run Time - DSL

```
1  import "scada_authentication.secadd"
2  import "library.dm"
3  import "scada.teamprofile"
4  RunTime {
5    Bob selected (
6      3 for SADDAuthorization.RBAC rationale "Not sufficient"
7      4 for SADDAuthorization.ABAC rationale "Would be more relevant for our purpose than RBAC"
8      5 for SADDAuthorization.RBAC_ABAC rationale "Combination might be what we need")
9    Alice selected (
10     5 for SADDAuthorization.RBAC rationale "Best solution"
11     2 for SADDAuthorization.ABAC rationale "Not relevant"
12     1 for SADDAuthorization.RBAC_ABAC rationale "Too much of a burden")
13   Carlos selected (
14     3 for SADDAuthorization.RBAC rationale "..."
15     2 for SADDAuthorization.ABAC rationale "..."
16     2 for SADDAuthorization.RBAC_ABAC rationale "...")
17   David selected (
18     5 for SADDAuthorization.RBAC rationale "Needed in our project to strengthen authorization process of our users"
19     2 for SADDAuthorization.ABAC rationale "Never used this solution"
20     3 for SADDAuthorization.RBAC_ABAC rationale "Too complex to combine them as I don't know anything about their
           combination")
21 }
```

Listing: Decision-Making Support at Run Time

Preference Indication

Strategy Configuration

- Strategy 1 : Voting with rating.
- Strategy 2 : Rating with decision rule Unanimity for Expert and Advanced TP in Authorization
  ⇒ then SuperMajority for Expert and Advanced TP in Authorization
  ⇒ then Confidence

Actors	RBAC	ABAC	RBAC and ABAC
Alice	5 (10)	2 (4)	1 (2)
Bob	3 (6)	4 (8)	5 (10)
Carlos	3 (1.5)	2 (1)	2 (1)
David	5 (7.5)	2 (3)	3 (4.5)
Total	16 (25)	10 (16)	11 (15.5)

Table: Preferences indication for each actor and in parenthesis after applying Confidence algorithm

Articles

Published Paper

- *Interplay of Human Factors and Secure Architecture Design using Model-Driven Engineering*, published in ASEW' 24

Paper Submitted

- *A Model-based Decision Support Framework for Security Architecture Design Decision-Making*
- *A systematic and structured process to provide security solutions to development teams*

Papers in preparation

- *Questionnaires to record Architectural Decisions and guide development teams during Decision-Making*

Future Work

- Building a Questionnaire for Security Architectural Design Decisions
- Connecting the different parts of the framework and building it
- Passing questionnaires for Human Factors
- Passing questionnaires for Security Architectural Design Decisions

Thank You

CyberSEA
Research Lab
Carleton University

Institut de Recherche
en Informatique de Toulouse
CNRS - INP - UT3 - UT1 - UT2J

Robin Theveniaut
RobinTheveniaut@carleton.ca
robin.theveniaut@irit.fr
@robin-theveniaut

CyberSEA Research Lab
https://carleton.ca/cybersea/
CyberSEA Research Lab

IRIT Research Lab
https://www.irit.fr/
IRIT Research Lab