



UNIVERSITÀ
DEGLI STUDI
DI BERGAMO

Dipartimento
di Ingegneria Gestionale,
dell'Informazione e della Produzione

How to define if, when, and how a system works?

Reflections and experiences between industry and academia.

**"It Works Really Well!": Verification in Theory and Practice
Session: What Does "Works" Mean?**

Speaker

Claudio MENGHI



Date: Oct 5, 2023



What Does "Works" Mean?



UNIVERSITÀ
DEGLI STUDI
DI BERGAMO

Dipartimento
di Ingegneria Gestionale,
dell'Informazione e della Produzione

Robotics

Mission Specification Patterns for Mobile Robots: Providing Support for Quantitative Properties,
IEEE Transactions on Software Engineering, 2022
 Menghi, Claudio; Tsigkanos, Christos; Askarpour, Mehrnoosh;
 Pelliccione, Patrizio; Vazquez, Grisel; Calinescu, Radu; Garcia, Sergio

Specification patterns for robotic missions,
IEEE Transactions on Software Engineering, 2019
 Menghi, Claudio; Tsigkanos, Christos; Pelliccione, Patrizio; Ghezzi, Carlo; Berger, Thorsten

High-level mission specification for multiple robots,
ACM SIGPLAN international conference on software language engineering, 2019,
 Garcia, Sergio; Pelliccione, Patrizio; Menghi, Claudio; Berger, Thorsten; Bures, Tomas

Promise: high-level mission specification for multiple robots,
ACM/IEEE International Conference on Software Engineering: Companion Proceedings, 2020,
 Garcia, Sergio; Pelliccione, Patrizio; Menghi, Claudio; Berger, Thorsten; Bures, Tomas

A Survey on the Design Space of End-User-Oriented Languages for Specifying Robotic Missions,
International Journal of Software and Systems Modeling (SoSyM), 2021,
 Dragule, Swaib; Berger, Thorsten; Menghi, Claudio; Pelliccione, Patrizio;

Space

Evaluating Model Testing and Model Checking for Finding Requirements Violations in Simulink Models,
Foundations of Software Engineering, 2019,
 Nejati, Shiva; Gaaloul, Khouloud; Menghi, Claudio; Briand, Lionel C; Foster, Stephen; Wolfe, David

Approximation-Refinement Testing of Compute-Intensive Cyber-Physical Models: An Approach Based on System Identification,
International Conference on Software Engineering, 2020,
 Menghi, Claudio; Nejati, Shiva; Briand, Lionel C.; Parache, Yago Isasi;

Generating automated and online test oracles for Simulink models with continuous and uncertain behaviors, **Foundations of Software Engineering, 2019**,
 Menghi, Claudio; Nejati, Shiva; Gaaloul, Khouloud; Briand, Lionel C. Mining Assumptions for Software Components using Machine Learning, **Foundations of Software Engineering (ESEC/FSE), 2020**,
 Gaaloul, Khouloud; Menghi, Claudio; Nejati, Shiva; Briand, Lionel; Wolfe, David;

Trace-Checking Signal-based Temporal Properties: A Model-Driven Approach,
Automated Software Engineering (ASE), 2020,
 Boufaied, Chaima; Menghi, Claudio; Bianculli, Domenico; Briand, Lionel; Parache, Yago Isasi

Trace-Checking CPS Properties: Bridging the Cyber-Physical Gap,
International Conference on Software Engineering (ICSE), 2021,
 Menghi, Claudio; Viganò, Enrico; Bianculli, Domenico; Briand, Lionel C

Combining Genetic Programming and Model Checking to Generate Environment Assumptions,
IEEE Transactions on Software Engineering, 2021,
 Gaaloul, Khouloud; Menghi, Claudio; Nejati, Shiva; Briand, Lionel C; Parache, Yago Isasi

Authors.Title.Publication,Volume,Number,Pages,Year,Publisher

Trace Diagnostics for Signal-based Temporal Properties,
IEEE Transactions on Software Engineering, 2023,
 Boufaied, Chaima; Menghi, Claudio; Bianculli, Domenico; Briand, Lionel C;

Cyber-physical systems

Search-based Software Testing Driven by Automatically Generated and Manually Defined Fitness Functions,
ACM Transactions on Software Engineering and Methodology, 2023
 F. Formica; T. Fan; C. Menghi

Simulation-based Testing of Simulink Models with Test Sequence and Test Assessment Blocks,
Under Review
 F. Formica, T. Fan, A. Rajhans, V. Pantelic, M. Lawford, C. Menghi

Test Case Generation for Drivability Requirements of an Automotive Cruise Controller: An Experience with an Industrial Simulator,
ESEC/FSE Industry Track, 2023
 F. Formica, N. Petrunti, L. Bruck, V. Pantelic, M. Lawford, C. Menghi

Safety Analysis

Assurance Case Development as Data: A Manifesto,
International Conference on Software Engineering: New Ideas and Emerging Results (ICSE-NIER), 2023,
 Menghi, Claudio; Viger, Torin; Di Sandro, Alessio; Rees, Chris; Joyce, Jeff; Chechik, Marsha

Assurance Case Arguments in the Large - CERN LHC Machine Protection System,
International Conference on Computer Safety, Reliability and Security (SafeComp), 2023,
 Millet, Laure; Diemert, Simon; Rees, Chris; Viger, Torin; Chechik, Marsha; Menghi, Claudio; Joyce, Jeffrey

Supporting Assurance Case Development Using Generative AI,
SAFECOMP 2023, Position Paper, 2023,
 Viger, Torin; Murphy, Logan; Diemert, Simon; Menghi, Claudio; Di, Alessio; Chechik, Marsha

The ForeMoSt Approach To Building Valid Model-Based Safety Arguments,
Software and Systems Modeling, 2022,
 Viger, Torin; Murphy, Logan; Di Sandro, Alessio; Menghi, Claudio; Shahin, Ramy; Chechik, Marsha



Co4Robots
 European Union's Horizon 2020
 Grant agreement No 731869



TUNE
 European Research Council (ERC)
 Horizon 2020
 Grant agreement No 694277.



Automated Support for Cyber-Physical
 Systems Design: from Theory to Practice



UNIVERSITÀ
 DEGLI STUDI
 DI BERGAMO

Dipartimento
 di Ingegneria Gestionale,
 dell'Informazione e della Produzione

Robotics

Mission Specification Patterns for Mobile Robots: Providing Support for Quantitative Properties,

IEEE Transactions on Software Engineering, 2022

Menghi, Claudio; Tsigkanos, Christos; Askarpour, Mehrnoosh;

Pelliccione, Patrizio; Vazquez, Gricel; Calinescu, Radu; García, Sergio

Specification patterns for robotic missions,

IEEE Transactions on Software Engineering, 2019

Menghi, Claudio; Tsigkanos, Christos; Pelliccione, Patrizio; Ghezzi,

Carlo; Berger, Thorsten

High-level mission specification for multiple robots,

ACM SIGPLAN international conference on software language

engineering, 2019,

García, Sergio; Pelliccione, Patrizio; Menghi, Claudio; Berger, Thorsten;

Bures, Tomas

Promise: high-level mission specification for multiple robots,

ACM/IEEE International Conference on Software Engineering:

Companion Proceedings, 2020,

García, Sergio; Pelliccione, Patrizio; Menghi, Claudio; Berger, Thorsten;

Bures, Tomas

A Survey on the Design Space of End-User-Oriented Languages for

Specifying Robotic Missions,

International Journal of Software and Systems Modeling

(SoSyM), 2021,

Dragule, Swaib; Berger, Thorsten; Menghi, Claudio; Pelliccione,

Patrizio;



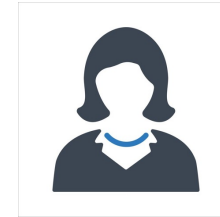
Co4Robots
European Union's Horizon 2020
Grant agreement No 731869



UNIVERSITÀ
DEGLI STUDI
DI BERGAMO

Dipartimento
di Ingegneria Gestionale,
dell'Informazione e della Produzione

Problem Definition



The robot should
bring the coffee to a
user

**Mission
Requirement**



```
def quadratic():
    with open('quadratic.txt') as f:
        # read-only file
        with open('quadratic.txt') as f:
            # opens and writes on file
            for line in f:
                a, b, c = (int(x) for x in line.split())
                d = (b**2 - 4 * int(a) * int(c)) # discriminant
                if d < 0:
                    print(f'a = {a}, b = {b}, c = {c} which has no x-intercepts')
                elif d == 0:
                    x = (-int(b) - int(b) * 2 - 4 * int(a) * int(c)) / 2 * int(a) # one solution
                    print(f'a = {a}, b = {b}, c = {c} which only has x-intercept at {x}')
                else:
                    x1 = (-int(b) + int(b) * 2 - 4 * int(a) * int(c)) / 2 * int(a)
                    x2 = (-int(b) - int(b) * 2 - 4 * int(a) * int(c)) / 2 * int(a) # two solutions
                    print(f'a = {a}, b = {b}, c = {c} with x-intercepts at {x1} and {x2}')
                    format(x1, '.2f'), ' and ', format(x2, '.2f') # print to two decimal places
            example:
            if len(line) == 3:
                print('Wrong amount of coefficients')
            else:
                if not all(x.isdigit() for x in line):
                    print('Invalid coefficients or constants')
    quadratic()
```

**Mission
Specification**

x



UNIVERSITÀ
DEGLI STUDI
DI BERGAMO

Dipartimento
di Ingegneria Gestionale,
dell'Informazione e della Produzione

Mission Specification Patterns for Mobile Robots: Providing Support for Quantitative Properties,
IEEE Transactions on Software Engineering, 2022
Menghi, Claudio; Tsigkanos, Christos; Askarpour, Mehrnoosh; Pelliccione, Patrizio; Vazquez, Grisel; Calinescu, Radu; García, Sergio

Specification patterns for robotic missions,
IEEE Transactions on Software Engineering, 2019
Menghi, Claudio; Tsigkanos, Christos; Pelliccione, Patrizio; Ghezzi, Carlo; Berger, Thorsten

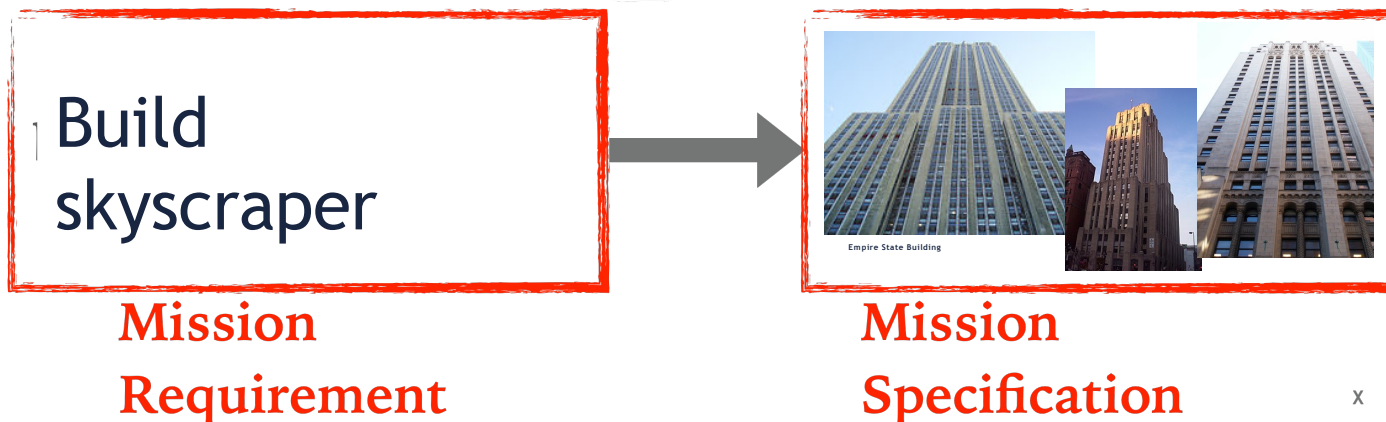


Funded by the Horizon 2020
Framework Programme of the
European Union

Solution: Mission Specification Patterns and DSL

Mission Specification Pattern

- A **template solution** for a **recurrent specification problem**
- Maps a recurrent requirement to a specification (LTL/CTL)



x



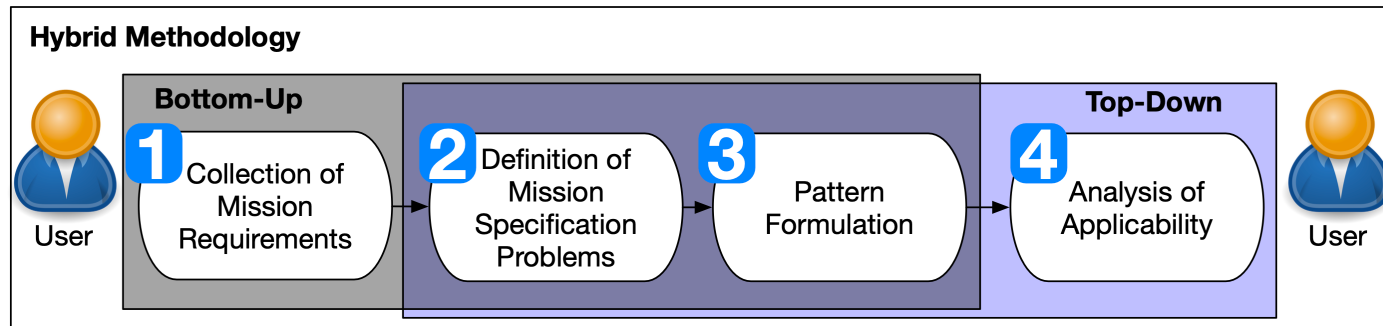
UNIVERSITÀ
DEGLI STUDI
DI BERGAMO

Dipartimento
di Ingegneria Gestionale,
dell'Informazione e della Produzione

Mission Specification Patterns for Mobile Robots: Providing Support for Quantitative Properties,
IEEE Transactions on Software Engineering, 2022
Menghi, Claudio; Tsigkanos, Christos; Askarpour, Mehrnoosh; Pelliccione, Patrizio; Vazquez, Grisel; Calinescu, Radu; García, Sergio

Specification patterns for robotic missions,
IEEE Transactions on Software Engineering, 2019
Menghi, Claudio; Tsigkanos, Christos; Pelliccione, Patrizio; Ghezzi, Carlo; Berger, Thorsten

Methodology



UNIVERSITÀ
DEGLI STUDI
DI BERGAMO

Dipartimento
di Ingegneria Gestionale,
dell'Informazione e della Produzione

Mission Specification Patterns for Mobile Robots: Providing Support for Quantitative Properties,
IEEE Transactions on Software Engineering, 2022
Menghi, Claudio; Tsigkanos, Christos; Askarpour, Mehrnoosh; Pelliccione, Patrizio; Vazquez, Gricel; Calinescu, Radu; García, Sergio

Specification patterns for robotic missions,
IEEE Transactions on Software Engineering, 2019
Menghi, Claudio; Tsigkanos, Christos; Pelliccione, Patrizio; Ghezzi, Carlo; Berger, Thorsten



Funded by the Horizon 2020
Framework Programme of the
European Union

Domain-Specific Language

Mission	<code>miss</code>	<code>::= miss and miss miss or miss not miss rob shall pat e_qpat c_qpat</code>
Pattern	<code>pat</code>	<code>::= visit (in sequence in order in strict order fairly)? locs patrol (in sequence in order in strict order fairly)? locs visit (more than less than exactly) n times loc avoid (loc until cond loc loc after cond) react (instantly with a delay promptly) to cond by (exec act pat reach loc) counteract (instantly with a delay) when reach loc by cond wait in location loc until cond</code>
Elementary Patterns	<code>e_qpat</code>	<code>::= maximize m miss minimize m miss m at most v miss m less than v miss m at least v miss m greater than v miss m exactly v miss m within v₁ and v₂ miss m strictly within v₁ and v₂ miss</code>
Composite Patterns	<code>c_qpat</code>	<code>::= conserve m while miss preserve m within [v₁,v₂] while miss pause v miss timeout v miss repeat miss every v end miss exactly at v time of miss₁ proportional to miss₂ by factor v execute rob actions act₁,act₂...act_n rob accrue m while miss achieve miss with reliability m (greater less) than v achieve miss with confidence m (greater less) than v rob miss equidistance rob₁ rob₂ rob trail o with distance v</code>
Condition	<code>cond</code>	<code>::= condition is true act is ended rob in loc</code>
Locations	<code>locs</code>	<code>::= {loc (, loc)*}</code>

* miss, miss₁, miss₂ are missions; v, v₁, v₂ are values; rob is a robot, o is an object, m is the name of the quantitative measure.



UNIVERSITÀ
DEGLI STUDI
DI BERGAMO

Dipartimento
di Ingegneria Gestionale,
dell'Informazione e della Produzione

Mission Specification Patterns for Mobile Robots: Providing Support for Quantitative Properties,
IEEE Transactions on Software Engineering, 2022
Menghi, Claudio; Tsigkanos, Christos; Askarpour, Mehrnoosh; Pelliccione, Patrizio; Vazquez, Grisel; Calinescu, Radu; García, Sergio

Specification patterns for robotic missions,
IEEE Transactions on Software Engineering, 2019
Menghi, Claudio; Tsigkanos, Christos; Pelliccione, Patrizio; Ghezzi, Carlo; Berger, Thorsten



Funded by the Horizon 2020
Framework Programme of the
European Union

Domain-Specific Language

```
runtime-EclipseXtext - demoQuartet/Examples/Example1.mydsl - Eclipse Platform
File Edit Navigate Search Project Run Window Help

Project Explorer
demoQuartet
├── Examples
│   └── Example1.mydsl
└── src-gen
    └── Example1.mydsl.pm

Example1.mydsl
problem specifications
{
    locations: goal, CP, TA, HA
    robots: r1
    conditions:
        record: ActionRecord is true
        close: CloseAction is true
    missions:
        m1: (reward minimize Time r1 shall visit goal) and
            ((r1 shall react instantly to close by visit CP, TA, HA) and
             ((r1 shall counteract instantly when reach CP by record) and
              ((r1 shall counteract instantly when reach TA by record) and
               (r1 shall counteract instantly when reach HA by record)))));
        m2: reward minimize Time r1 shall visit goal;
        m3: (r1 shall react instantly to close by visit CP,TA,HA) and
            ((r1 shall counteract instantly when reach CP by record) and
             ((r1 shall counteract instantly when reach TA by record) and
              (r1 shall counteract instantly when reach HA by record)))
}

Example1.mydsl.pm
m1: WARNING. Translation into Prism not supported.
m2: R{"Time"}min=?[F "r1goal"]
m3: (A[G"close" => ((F "r1CP") & (F "r1TA") & (F "r1HA"))]) &
    ((A[G"record" <=> (X"CP")]) & ((A[G"record" <=> (X"TA")]) &
    (A[G"record" <=> (X"HA")]) ) ) )
```



UNIVERSITÀ
DEGLI STUDI
DI BERGAMO

Dipartimento
di Ingegneria Gestionale,
dell'Informazione e della Produzione

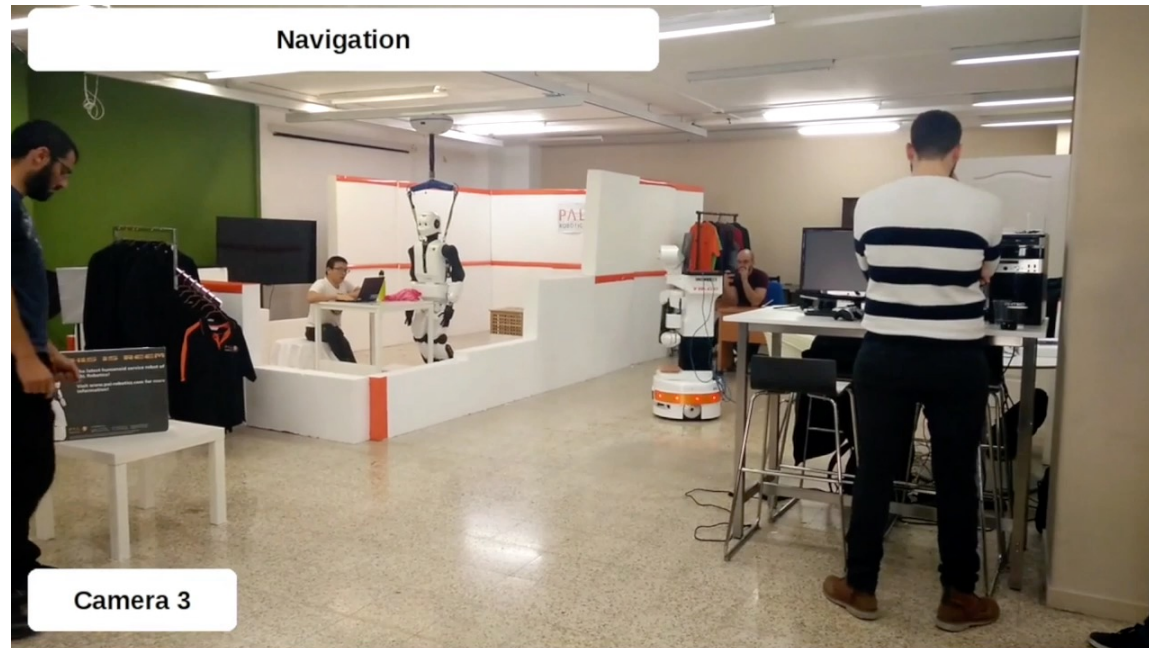
Mission Specification Patterns for Mobile Robots: Providing Support for Quantitative Properties,
IEEE Transactions on Software Engineering, 2022
Menghi, Claudio; Tsigkanos, Christos; Askarpour, Mehrnoosh; Pelliccione, Patrizio; Vazquez, Grisel; Calinescu, Radu; García, Sergio

Specification patterns for robotic missions,
IEEE Transactions on Software Engineering, 2019
Menghi, Claudio; Tsigkanos, Christos; Pelliccione, Patrizio; Ghezzi, Carlo; Berger, Thorsten



Funded by the Horizon 2020
Framework Programme of the
European Union

Evaluation



UNIVERSITÀ
DEGLI STUDI
DI BERGAMO

Dipartimento
di Ingegneria Gestionale,
dell'Informazione e della Produzione

Mission Specification Patterns for Mobile Robots: Providing Support for Quantitative Properties,
IEEE Transactions on Software Engineering, 2022
Menghi, Claudio; Tsigkanos, Christos; Askarpour, Mehrnoosh; Pelliccione, Patrizio; Vazquez, Gricel; Calinescu, Radu; García, Sergio

Specification patterns for robotic missions,
IEEE Transactions on Software Engineering, 2019
Menghi, Claudio; Tsigkanos, Christos; Pelliccione, Patrizio; Ghezzi, Carlo; Berger, Thorsten



Funded by the Horizon 2020
Framework Programme of the
European Union

Robotics

End-user: final customers,
mission specification
engineers

Domain: robotics

Product: a domain-
specific language inspired
by natural language

Meaning of Work: does
what is expected to do



Co4KODOTS
European Union's Horizon 2020
Grant agreement No 731869



TUNE
European
Research
Council
European Research Council (ERC)
Horizon 2020
Grant agreement No 694277.



Automated Support for Cyber-Physical
Systems Design: from Theory to Practice



UNIVERSITÀ
DEGLI STUDI
DI BERGAMO

Dipartimento
di Ingegneria Gestionale,
dell'Informazione e della Produzione

Space

Evaluating Model Testing and Model Checking for Finding Requirements Violations in Simulink Models, **Foundations of Software Engineering, 2019**, Nejati, Shiva; Gaaloul, Khoulood; Menghi, Claudio; Briand, Lionel C; Foster, Stephen; Wolfe, David

Approximation-Refinement Testing of Compute-Intensive Cyber-Physical Models: An Approach Based on System Identification, **International Conference on Software Engineering, 2020**, Menghi, Claudio; Nejati, Shiva; Briand, Lionel C.; Parache, Yago Isasi;

Generating automated and online test oracles for Simulink models with continuous and uncertain behaviors, **Foundations of Software Engineering, 2019**,

Menghi, Claudio; Nejati, Shiva; Gaaloul, Khoulood; Briand, Lionel C. Mining Assumptions for Software Components using Machine Learning, **Foundations of Software Engineering (ESEC/FSE), 2020**, Gaaloul, Khoulood; Menghi, Claudio; Nejati, Shiva; Briand, Lionel; Wolfe, David;

Trace-Checking Signal-based Temporal Properties: A Model-Driven Approach, **Automated Software Engineering (ASE), 2020**, Boufaied, Chaima; Menghi, Claudio; Bianculli, Domenico; Briand, Lionel; Parache, Yago Isasi

Trace-Checking CPS Properties: Bridging the Cyber-Physical Gap, **International Conference on Software Engineering (ICSE), 2021**, Menghi, Claudio; Viganò, Enrico; Bianculli, Domenico; Briand, Lionel C

Combining Genetic Programming and Model Checking to Generate Environment Assumptions, **IEEE Transactions on Software Engineering, 2021**, Gaaloul, Khoulood; Menghi, Claudio; Nejati, Shiva; Briand, Lionel C; Parache, Yago Isasi

Authors, Title, Publication, Volume, Number, Pages, Year, Publisher
Trace Diagnostics for Signal-based Temporal Properties, **IEEE Transactions on Software Engineering, 2023**, Boufaied, Chaima; Menghi, Claudio; Bianculli, Domenico; Briand, Lionel C;



Co4Robots
European Union's Horizon 2020
Grant agreement No 731869



TUNE
European Research Council (ERC)
Horizon 2020
Grant agreement No 694277.



Automated Support for Cyber-Physical
Systems Design: from Theory to Practice



UNIVERSITÀ
DEGLI STUDI
DI BERGAMO

Dipartimento
di Ingegneria Gestionale,
dell'Informazione e della Produzione

Problem Definition

How can we support engineers
in **verifying** and **validating** CPS?



UNIVERSITÀ
DEGLI STUDI
DI BERGAMO

Dipartimento
di Ingegneria Gestionale,
dell'Informazione e della Produzione

Solution

Provide appropriate logic-based language to specify requirements
+
automated trace-checking procedure supporting this language



UNIVERSITÀ
DEGLI STUDI
DI BERGAMO

Dipartimento
di Ingegneria Gestionale,
dell'Informazione e della Produzione

Trace-Checking CPS Properties: Bridging the Cyber-Physical Gap,
International Conference on Software Engineering (ICSE), 2021,
Menghi, Claudio; Viganò, Enrico; Bianculli, Domenico; Briand, Lionel C

Hybrid Logic of Signals

HLS supports specifications that use

- a signal **at** a certain **timestamp**
- a signal **at** a certain **index**
- the **timestamp** of an **index** (and vice versa)
- **expressions** combining **timestamps**, **indices**, and **real-valued** variables

exists ρ such that ($\rho < 1.5$ and
for all σ_0 in $[0;5]$ such that
((mode $@i \sigma_0$) = 0 and (mode $@i (\sigma_0 + 1)$) = 3)
implies
exists τ_0 in $[0s;10s]$ such that
(ang-rate $@t (\tau_0 + i2t(\sigma_0)) < \rho$)))



UNIVERSITÀ
DEGLI STUDI
DI BERGAMO

Dipartimento
di Ingegneria Gestionale,
dell'Informazione e della Produzione

Trace-Checking CPS Properties: Bridging the Cyber-Physical Gap,
International Conference on Software Engineering (ICSE), 2021,
Menghi, Claudio; Viganò, Enrico; Bianculli, Domenico; Briand, Lionel C

ThEodorE: Trace-checker

ThEodorE:

- Reduces trace-checking problem to a SMT problem
- Allows the use of efficient off-the-shelf SMT solvers



UNIVERSITÀ
DEGLI STUDI
DI BERGAMO

Dipartimento
di Ingegneria Gestionale,
dell'Informazione e della Produzione

Trace-Checking CPS Properties: Bridging the Cyber-Physical Gap,
International Conference on Software Engineering (ICSE), 2021,
Menghi, Claudio; Viganò, Enrico; Bianculli, Domenico; Briand, Lionel C

Evaluation

Evaluated from 212 industrial requirements

- **ThEodorE** computed a verdict for **74.5%** trace-requirement **combinations**.
- **ThEodorE** produced a verdict for **67.9%** of the 337 trace-requirement **combinations that could not be checked by the other tools**.



UNIVERSITÀ
DEGLI STUDI
DI BERGAMO

Dipartimento
di Ingegneria Gestionale,
dell'Informazione e della Produzione

Trace-Checking CPS Properties: Bridging the Cyber-Physical Gap,
International Conference on Software Engineering (ICSE), 2021,
Menghi, Claudio; Viganò, Enrico; Bianculli, Domenico; Briand, Lionel C

Robotics

End-user: final customers, mission specification engineers

Domain: robotics

Product: a domain-specific language inspired by natural language

Meaning of Work: does what is expected to do

Space

End-users: space engineers/developers

Domain: space

Product: logic-based language

Meaning of Work: does not violate requirements



UNIVERSITÀ
DEGLI STUDI
DI BERGAMO

Dipartimento
di Ingegneria Gestionale,
dell'Informazione e della Produzione

Cyber-physical systems

Search-based Software Testing Driven by Automatically Generated and Manually Defined Fitness Functions,
ACM Transactions on Software Engineering and Methodology, 2023
F. Formica; T. Fan; C. Menghi

Simulation-based Testing of Simulink Models with Test Sequence and Test Assessment Blocks,

Under Review

F. Formica, T. Fan, A. Rajhans, V. Pantelic, M. Lawford, C. Menghi

Test Case Generation for Drivability Requirements of an Automotive Cruise Controller: An Experience with an Industrial Simulator,
ESEC/FSE Industry Track, 2023

F. Formica, N. Petrunti, L. Bruck, V. Pantelic, M. Lawford, C. Menghi



Co4Robots
European Union's Horizon 2020
Grant agreement No 731869



TUNE
European Research Council (ERC)
Horizon 2020
Grant agreement No 694277.



Automated Support for Cyber-Physical
Systems Design: from Theory to Practice

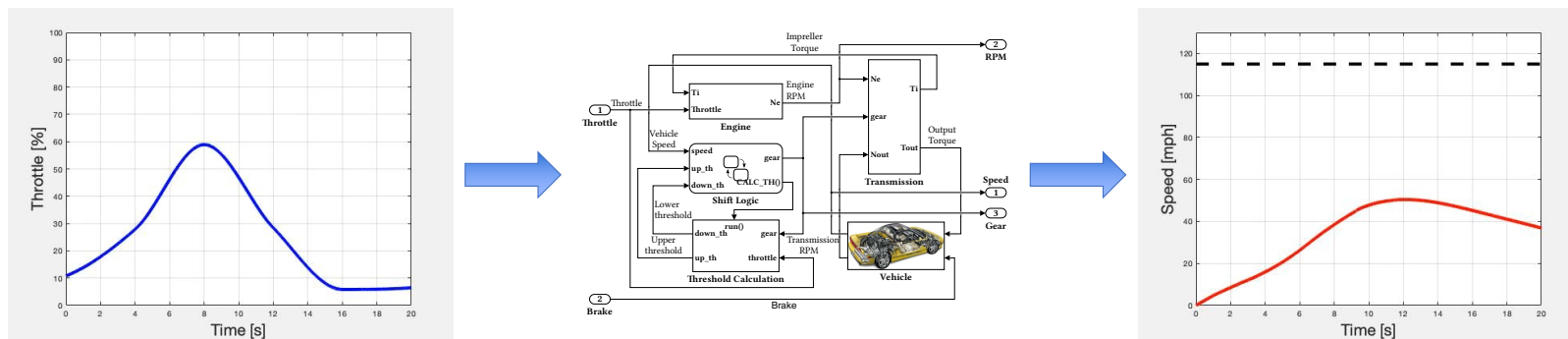


UNIVERSITÀ
DEGLI STUDI
DI BERGAMO

Dipartimento
di Ingegneria Gestionale,
dell'Informazione e della Produzione

SBST – Example

$speed \leq 115 \text{ mph for } t \in [0,20]s$



Problem Definition

How can we combine/use the knowledge of engineers to detect violations of the system requirements?

Title: Automated Support for Cyber-Physical Systems Design: from Theory to Practice

Overall Goal: ``support engineers in developing safe CPS by defining novel software engineering solutions.”



UNIVERSITÀ
DEGLI STUDI
DI BERGAMO

Dipartimento
di Ingegneria Gestionale,
dell'Informazione e della Produzione



Solution: Use Additional Knowledge from Engineers

Engineers are experts about their design

Use their knowledge to search test cases more effectively



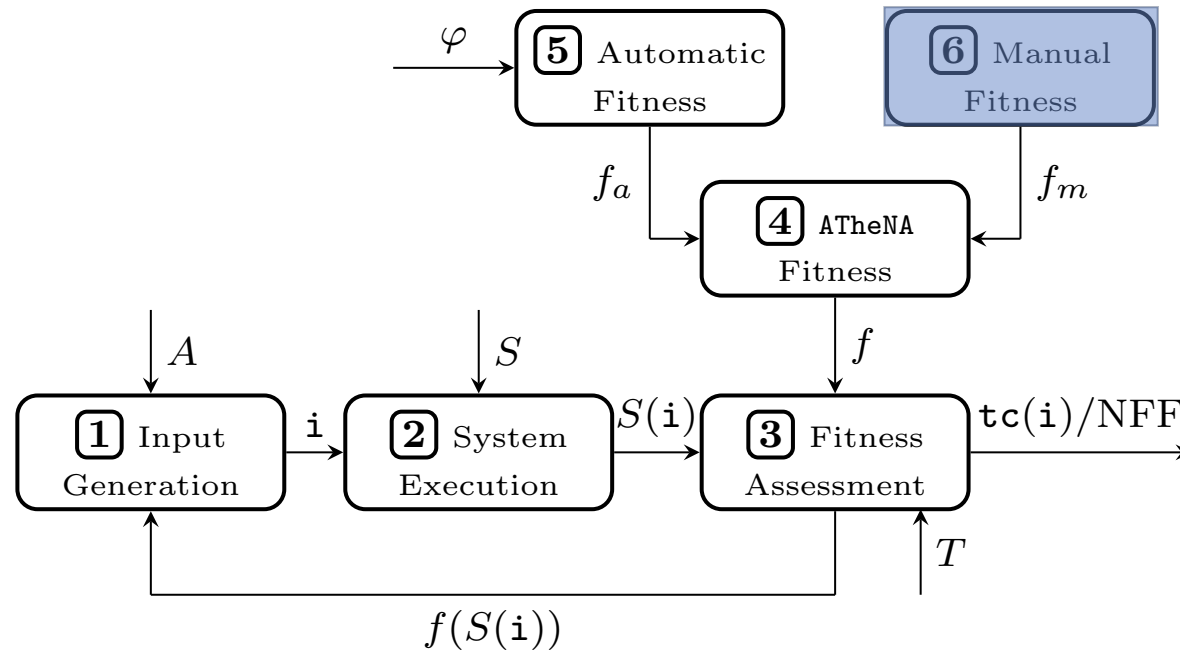
UNIVERSITÀ
DEGLI STUDI
DI BERGAMO

Dipartimento
di Ingegneria Gestionale,
dell'Informazione e della Produzione

Search-based Software Testing Driven by Automatically Generated and Manually Defined Fitness Functions,
ACM Transactions on Software Engineering and Methodology, 2023
F. Formica; T. Fan; C. Menghi



ATheNA



Reuse Engineers Knowledge

Engineers are already defining test cases

Reuse of Information Contained in Test Sequences and Test Assessment Blocks



UNIVERSITÀ
DEGLI STUDI
DI BERGAMO

Dipartimento
di Ingegneria Gestionale,
dell'Informazione e della Produzione

Simulation-based Testing of Simulink Models with Test Sequence and Test Assessment Blocks,
Under Review (arXiv preprint arXiv:2212.11589)

F. Formica, T. Fan, A. Rajhans, V. Pantelic, M. Lawford, C. Menghi



Hecate

Step	Transition	Next Step
PressNeitherButton RedButtonIN = false; GreenButtonIN = false;	1. after(1,sec)	PressBothButtons ▼
PressBothButtons RedButtonIN = true; GreenButtonIN = true;	1. after(1,sec)	PressRedButton ▼
PressRedButton RedButtonIN = true; GreenButtonIN = false;	1. after(1,sec)	PressGreenButton ▼
PressGreenButton RedButtonIN = false; GreenButtonIN = true;	1. after(1,sec)	EndTest ▼
EndTest		

[Test Sequence]

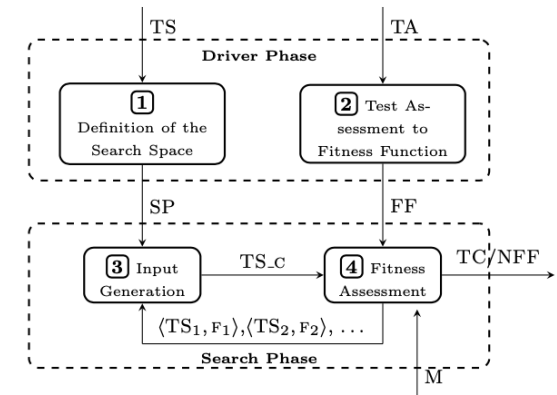
Test Input

Step	Transition	Next Step
Assessments		
Check1st when gear == 1 verify(speed < 45)		
Check2nd when gear == 2 verify(speed < 75)		
Check3rd when gear == 3 verify(speed < 105)		
Else		

[Test Assessment]

Test Oracle

Hecate



UNIVERSITÀ
DEGLI STUDI
DI BERGAMO

Dipartimento
di Ingegneria Gestionale,
dell'Informazione e della Produzione

Simulation-based Testing of Simulink Models with Test Sequence and Test Assessment Blocks,
Under Review (arXiv preprint arXiv:2212.11589)

F. Formica, T. Fan, A. Rajhans, V. Pantelic, M. Lawford, C. Menghi



Drivability Failure



UNIVERSITÀ
DEGLI STUDI
DI BERGAMO

Dipartimento
di Ingegneria Gestionale,
dell'Informazione e della Produzione

Test Case Generation for Drivability Requirements of an Automotive Cruise Controller: An Experience with an Industrial Simulator,
ESEC/FSE Industry Track, 2023

F. Formica, N. Petrunti, L. Bruck, V. Pantelic, M. Lawford, C. Menghi



Robotics

End-user: final customers, mission specification engineers

Domain: robotics

Product: a domain-specific language inspired by natural language

Meaning of Work: does what is expected to do

Space

End-users: space engineers/developers

Domain: space

Product: logic-based language

Meaning of Work: does not violate requirements

Cyber-physical systems

End-users: developers of Simulink models

Domain: automotive, medical

Product: block-based languages

Meaning of Work: does not violate requirements



Co4KODOS
European Union's Horizon 2020
Grant agreement No 731869



TUNE
European Research Council (ERC)
Horizon 2020
Grant agreement No 694277.



Automated Support for Cyber-Physical
Systems Design: from Theory to Practice



UNIVERSITÀ
DEGLI STUDI
DI BERGAMO

Dipartimento
di Ingegneria Gestionale,
dell'Informazione e della Produzione

Safety Analysis

Assurance Case Development as Data: A Manifesto,
**International Conference on Software Engineering: New Ideas and
Emerging Results (ICSE-NIER), 2023**,
Menghi, Claudio; Viger, Torin; Di Sandro, Alessio; Rees, Chris; Joyce,
Jeff; Chechik, Marsha

Assurance Case Arguments in the Large - CERN LHC Machine Protection
System,
**International Conference on Computer Safety, Reliability and
Security (SafeComp), 2023**,
Millet, Laure; Diemert, Simon; Rees, Chris; Viger, Torin; Chechik,
Marsha; Menghi, Claudio; Joyce, Jeffrey

Supporting Assurance Case Development Using Generative AI,
SAFECOMP 2023, Position Paper, 2023,
Viger, Torin; Murphy, Logan; Diemert, Simon; Menghi, Claudio; Di,
Alessio; Chechik, Marsha

The ForeMoSt Approach To Building Valid Model-Based Safety
Arguments, Software and Systems Modeling, 2022,
Viger, Torin; Murphy, Logan; Di Sandro, Alessio; Menghi, Claudio;
Shahin, Ramy; Chechik, Marsha



Co4Robots
European Union's Horizon 2020
Grant agreement No 731869



TUNE
European Research Council (ERC)
Horizon 2020
Grant agreement No 694277.



Automated Support for Cyber-Physical
Systems Design: from Theory to Practice




UNIVERSITÀ
DEGLI STUDI
DI BERGAMO


Dipartimento
di Ingegneria Gestionale,
dell'Informazione e della Produzione


Problem Definition


Assurance Case (AC): Argument decomposing high-level safety claims into refined sub-claims that are supported by evidence


GSN Syntax:

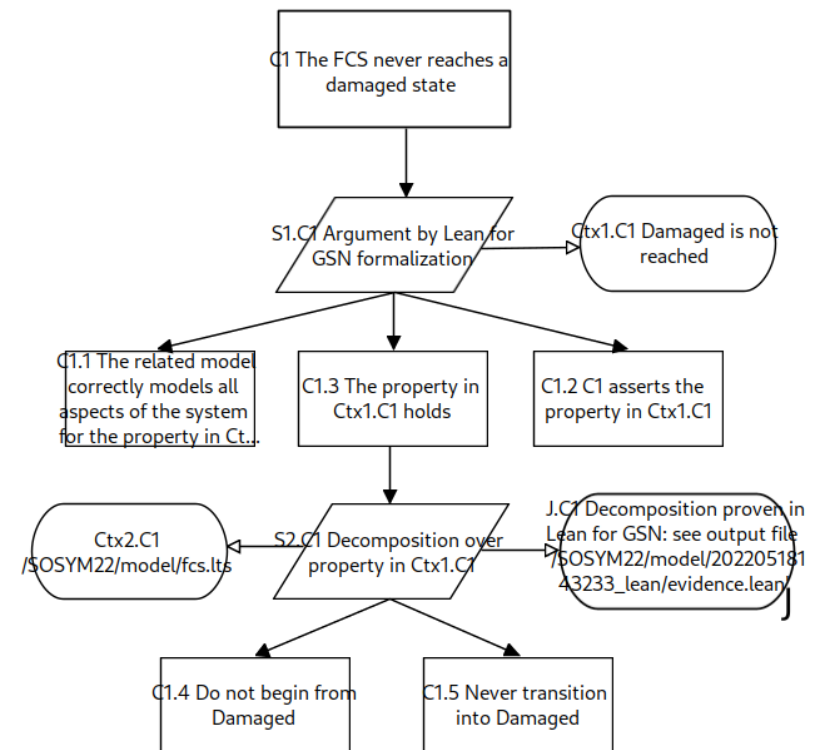
Claims/Goals: 

Strategies: 

Assumptions/
Justifications/
Contexts: 

Solution (evidence): 

Undeveloped node: 



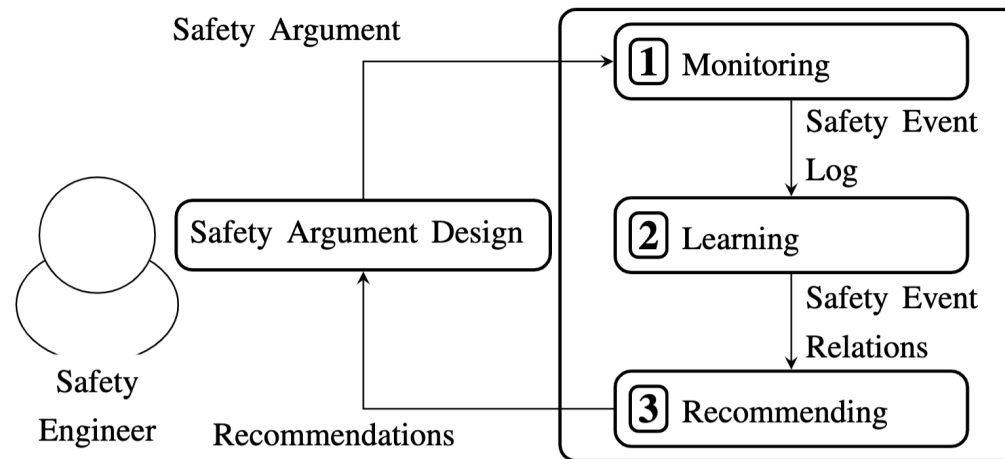
Problem Definition

How can we support engineers
in the automated analysis of assurance cases?

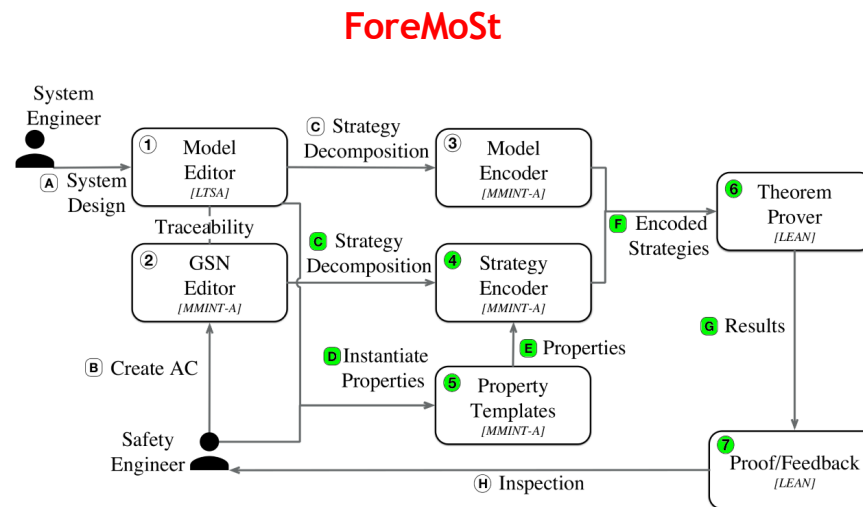


Solution

- Threat Assurance Cases as Data



- Exploit the Power of Formal Reasoning



Solution

- describes a medium-size assurance case argument for the CERN Large Hadron Collider Machine Protection System expressed using Eliminate Argumentation.
- the assurance case has 509 nodes
- validated in collaboration with CERN experts
- is publicly available.



UNIVERSITÀ
DEGLI STUDI
DI BERGAMO

Dipartimento
di Ingegneria Gestionale,
dell'Informazione e della Produzione

Assurance Case Arguments in the Large - CERN LHC Machine Protection System,
International Conference on Computer Safety, Reliability and Security (SafeComp), 2023,
Millet, Laure; Diemert, Simon; Rees, Chris; Viger, Torin; Chechik, Marsha; Menghi, Claudio; Joyce,
Jeffrey

Questions

Robotics	Space	Cyber-physical systems	Safety Analysis
End-user: final customers, mission specification engineers	End-users: space engineers/developers	End-users: developers of Simulink models	End-users: safety engineers
Domain: robotics	Domain: space	Domain: automotive, medical	Domain: nuclear
Product: a domain-specific language inspired by natural language	Product: logic-based language	Product: block-based languages	Product: semi-structured arguments
Meaning of Work: does what is expected to do	Meaning of Work: does not violate requirements	Meaning of Work: does not violate requirements	Meaning of Work: it is adequately safe



Co4KODOS
European Union's Horizon 2020
Grant agreement No 731869



TUNE
European Research Council (ERC)
Horizon 2020
Grant agreement No 694277.



Automated Support for Cyber-Physical
Systems Design: from Theory to Practice



UNIVERSITÀ
DEGLI STUDI
DI BERGAMO

Dipartimento
di Ingegneria Gestionale,
dell'Informazione e della Produzione

What Does "Works" Mean?

- L1. It is highly context and domain-dependent
(automotive, space, service robots, ...)
- L2. It depends on the target users
(end-users, requirements engineers, safety experts, ...)
- L3. It depends on the goal of specific activities
(mission specification, testing, safety analysis, ...)



Questions

Robotics

Mission Specification Patterns for Mobile Robots: Providing Support for Quantitative Properties,
IEEE Transactions on Software Engineering, 2022
Menghi, Claudio; Tsigkanos, Christos; Askarpour, Mehrnoosh;
Pelliccione, Patrizio; Vazquez, Grisel; Calinescu, Radu; Garcia, Sergio

Specification patterns for robotic missions,
IEEE Transactions on Software Engineering, 2019
Menghi, Claudio; Tsigkanos, Christos; Pelliccione, Patrizio; Ghezzi, Carlo; Berger, Thorsten

High-level mission specification for multiple robots,
ACM SIGPLAN international conference on software language engineering, 2019
Garcia, Sergio; Pelliccione, Patrizio; Menghi, Claudio; Berger, Thorsten; Bures, Tomas

Promise: high-level mission specification for multiple robots,
ACM/IEEE International Conference on Software Engineering: Companion Proceedings, 2020
Garcia, Sergio; Pelliccione, Patrizio; Menghi, Claudio; Berger, Thorsten; Bures, Tomas

A Survey on the Design Space of End-User-Oriented Languages for Specifying Robotic Missions,
International Journal of Software and Systems Modeling (SoSyM), 2021
Dragule, Swab; Berger, Thorsten; Menghi, Claudio; Pelliccione, Patrizio;



Space

Evaluating Model Testing and Model Checking for Finding Requirements Violations in Simulink Models,
Foundations of Software Engineering, 2019
Nejati, Shiva; Gaaloul, Khouloud; Menghi, Claudio; Briand, Lionel C; Foster, Stephen; Wolfe, David

Approximation-Refinement Testing of Compute-Intensive Cyber-Physical Models: An Approach Based on System Identification,
International Conference on Software Engineering, 2020
Menghi, Claudio; Nejati, Shiva; Briand, Lionel C.; Parache, Yago Isasi;

Generating automated and online test oracles for Simulink models with continuous and uncertain behaviors, **Foundations of Software Engineering, 2019**,
Menghi, Claudio; Nejati, Shiva; Gaaloul, Khouloud; Briand, Lionel C.
Mining Assumptions for Software Components using Machine Learning, **Foundations of Software Engineering (ESEC/FSE), 2020**,
Gaaloul, Khouloud; Menghi, Claudio; Nejati, Shiva; Briand, Lionel; Wolfe, David;

Trace-Checking Signal-based Temporal Properties: A Model-Driven Approach,
Automated Software Engineering (ASE), 2020,
Boufaied, Chaima; Menghi, Claudio; Bianculli, Domenico; Briand, Lionel; Parache, Yago Isasi

Trace-Checking CPS Properties: Bridging the Cyber-Physical Gap,
International Conference on Software Engineering (ICSE), 2021,
Menghi, Claudio; Viganò, Enrico; Bianculli, Domenico; Briand, Lionel C

Combining Genetic Programming and Model Checking to Generate Environment Assumptions,
IEEE Transactions on Software Engineering, 2021,
Gaaloul, Khouloud; Menghi, Claudio; Nejati, Shiva; Briand, Lionel C;

Authors, Title, Publication, Volume, Number, Pages, Year, Publisher
Trace Diagnostics for Signal-based Temporal Properties,
IEEE Transactions on Software Engineering, 2023,
Boufaied, Chaima; Menghi, Claudio; Bianculli, Domenico; Briand, Lionel C;

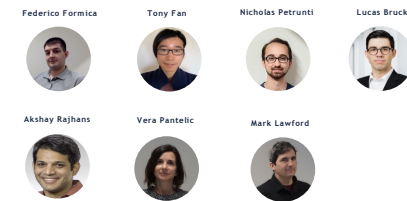


Cyber-physical systems

Search-based Software Testing Driven by Automatically Generated and Manually Defined Fitness Functions,
ACM Transactions on Software Engineering and Methodology, 2023
F. Formica; T. Fan; C. Menghi

Simulation-based Testing of Simulink Models with Test Sequence and Test Assessment Blocks,
Under Review

F. Formica, T. Fan, A. Rajhans, V. Pantelic, M. Lawford, C. Menghi
Test Case Generation for Drivability Requirements of an Automotive Cruise Controller: An Experience with an Industrial Simulator,
ESEC/FSE Industry Track, 2023
F. Formica, N. Petrunti, L. Bruck, V. Pantelic, M. Lawford, C. Menghi



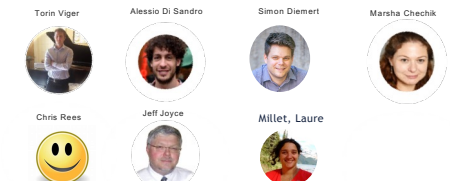
Safety Analysis

Assurance Case Development as Data: A Manifesto,
International Conference on Software Engineering: New Ideas and Emerging Results (ICSE-NIER), 2023,
Menghi, Claudio; Viger, Torin; Di Sandro, Alessio; Rees, Chris; Joyce, Jeff; Chechik, Marsha

Assurance Case Arguments in the Large - CERN LHC Machine Protection System,
International Conference on Computer Safety, Reliability and Security (SafeComp), 2023,
Millet, Laure; Diemert, Simon; Rees, Chris; Viger, Torin; Chechik, Marsha; Menghi, Claudio; Joyce, Jeffrey

Supporting Assurance Case Development Using Generative AI,
SAFECOMP 2023, Position Paper, 2023,
Viger, Torin; Murphy, Logan; Di Sandro, Alessio; Menghi, Claudio; Di, Alessio; Chechik, Marsha

The ForeMoSt Approach To Building Valid Model-Based Safety Arguments,
Software and Systems Modeling, 2022,
Viger, Torin; Murphy, Logan; Di Sandro, Alessio; Menghi, Claudio; Shahin, Rami; Chechik, Marsha



Automated Support for Cyber-Physical Systems Design: from Theory to Practice



UNIVERSITÀ
DEGLI STUDI
DI BERGAMO

Dipartimento
di Ingegneria Gestionale,
dell'Informazione e della Produzione



**UNIVERSITÀ
DEGLI STUDI
DI BERGAMO**

Dipartimento
di Ingegneria Gestionale,
dell'Informazione e della Produzione