# Verification and Validation of Cyber-Physical Systems

## *Model and Verify CPS using "Büchi Automata"*

Enkeledi Mema
enkeledi.mema@stud.hshl.de
Electronic Engineering

# Motivation for verification and validation of CPS

On January 1990, AT&T
Telephone Shortage

Costs: 100 Million US$
Source: Software flaw(Bug)

On June 1996 Ariane 5 crash

Costs: 500 Million US$
Source: Software flaw(Bug)



Picture source :Pixabay.com

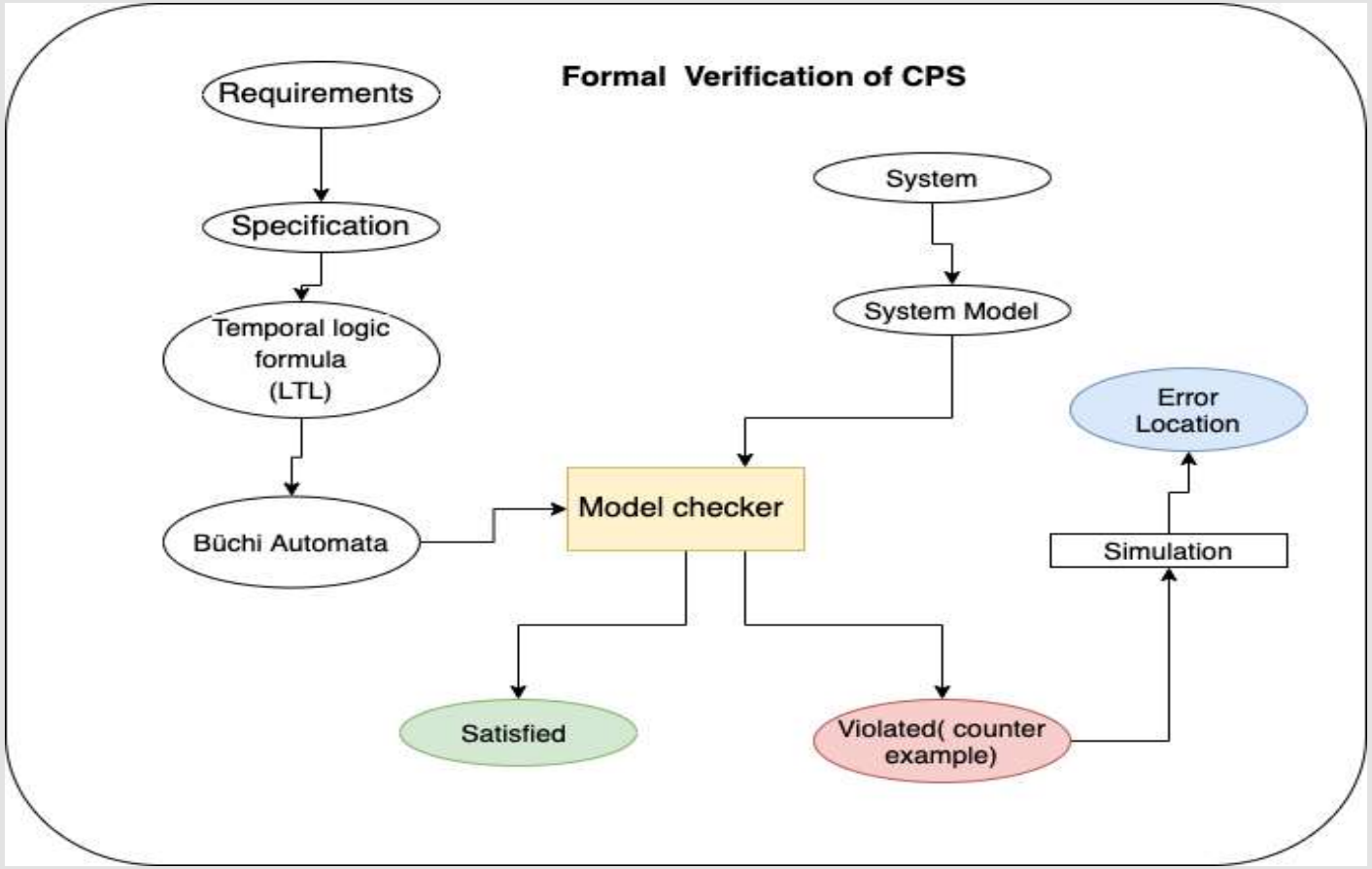
# Motivation for verification and validation of CPS

- Dependable
- Reliable
- Safe
- Secure

# Where are CPS used ?

- Precision farming
- Intelligent transportation
- Environmental control
- Avionics
- Traffic control and safety
- Process control
- Telemedicine
- Manufacturing
- Smart city

# Model checking overview



# Introduction to Büchi Automata

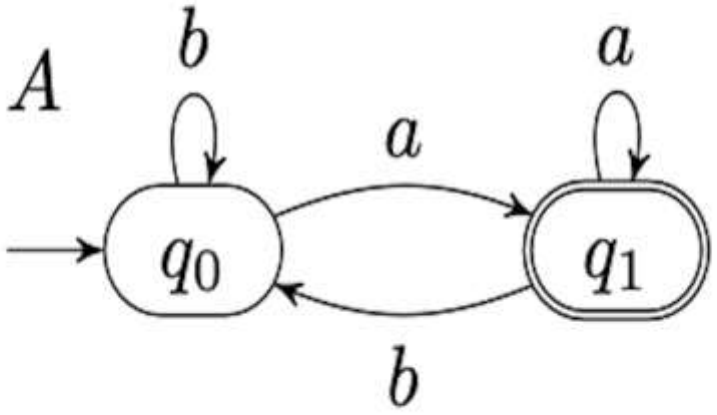
Let A($Q$,Σ,$\delta$,$q$0,$F$) a tuple be a deterministic Büchi automaton

- $Q$ *is a set of states;*
- Σ *is a finite set called the alphabet of A;*
- $\delta$ $Q$×Σ→$Q$*Is a transition function of A;*
- $q$0 *is initial state of A ;*
- $F$ *is the acceptance condition ;*

# Operations for BA application

- Determinization
- Emptiness checking
- Minimization

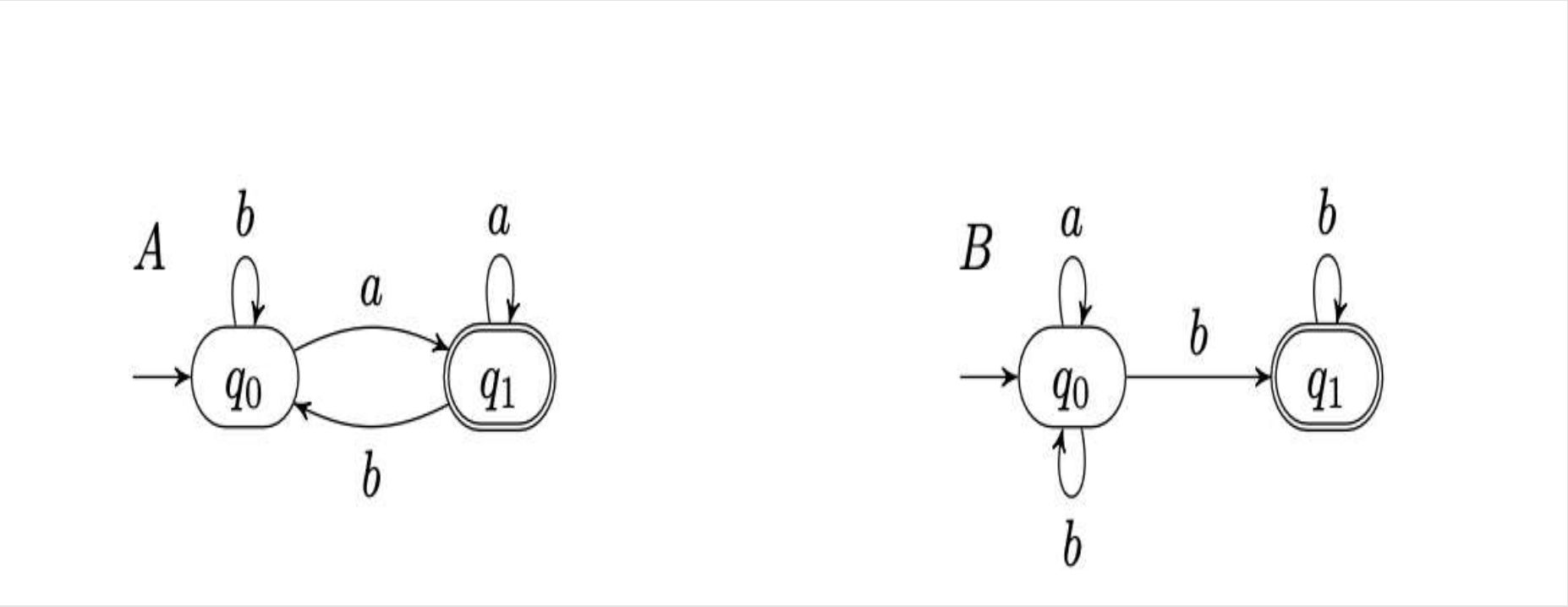
# Büchi automata example




- Σ = {$a$,$b$} which is the alphabet.
- $\delta$ = {($q0$, $a$, $q1$), ($q0$, $b$, $q0$), ($q1$, $a$, $q1$), ($q1$, $b$, $q0$)} the set of the transition.
- $F$ = {$q1$} the acceptance condition.
- $q0$ = {$q0$} the initial state.

Source:Li, Yong; Turrini, Andrea; Chen, Yu-Fang; Zhang, Lijun: Learning Büchi Automata and Its Applications. 11430:38–98. Series Title: Lecture Notes in Computer Science.

# Büchi automata and Generalized Büchi automata




Source:Li, Yong; Turrini, Andrea; Chen, Yu-Fang; Zhang, Lijun: Learning Büchi Automata and Its Applications. 11430:38–98. Series Title: Lecture Notes in Computer Science.

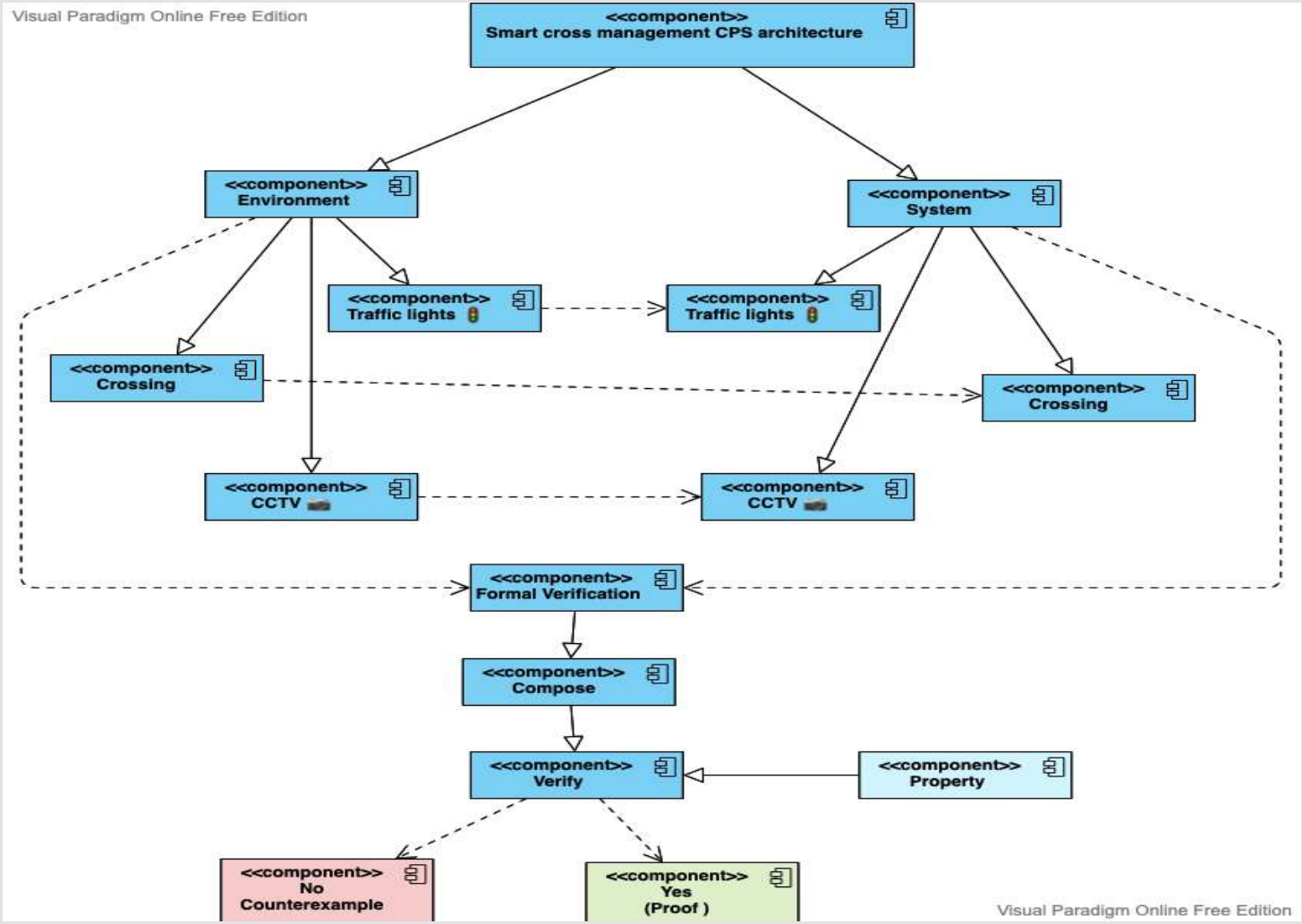
# CPS Use case (Smart cross-section)


Benefits:

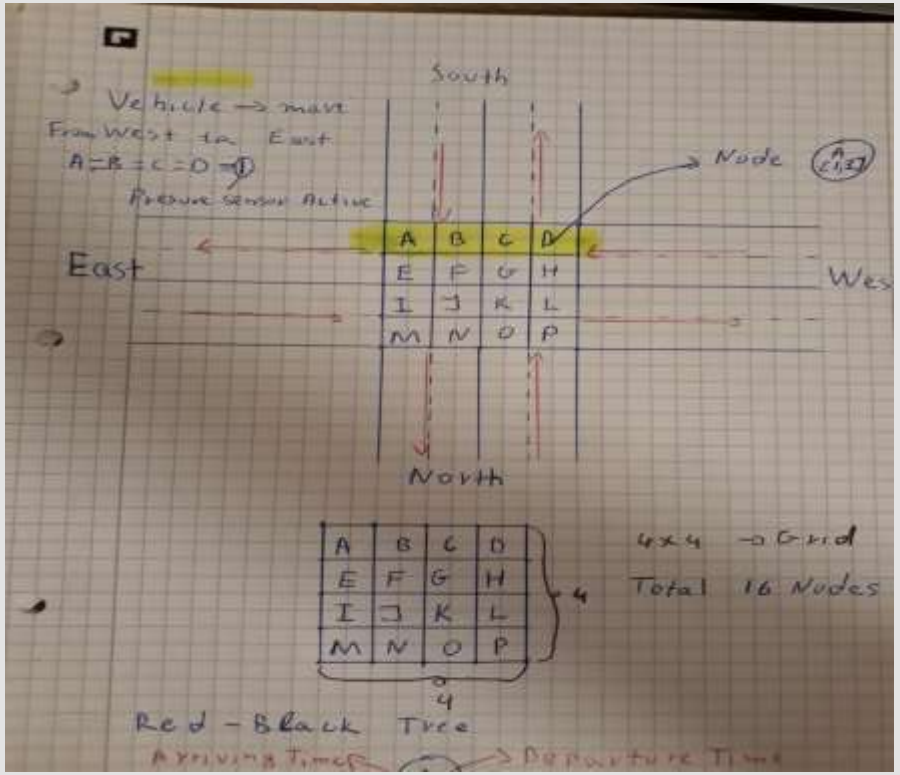
- Dealing  with safety critical systems.
- Facilitation in construction of smart
  cross-section.
- Time efficiency.

Picture source :Pixabay.com

# CPS components for the use case

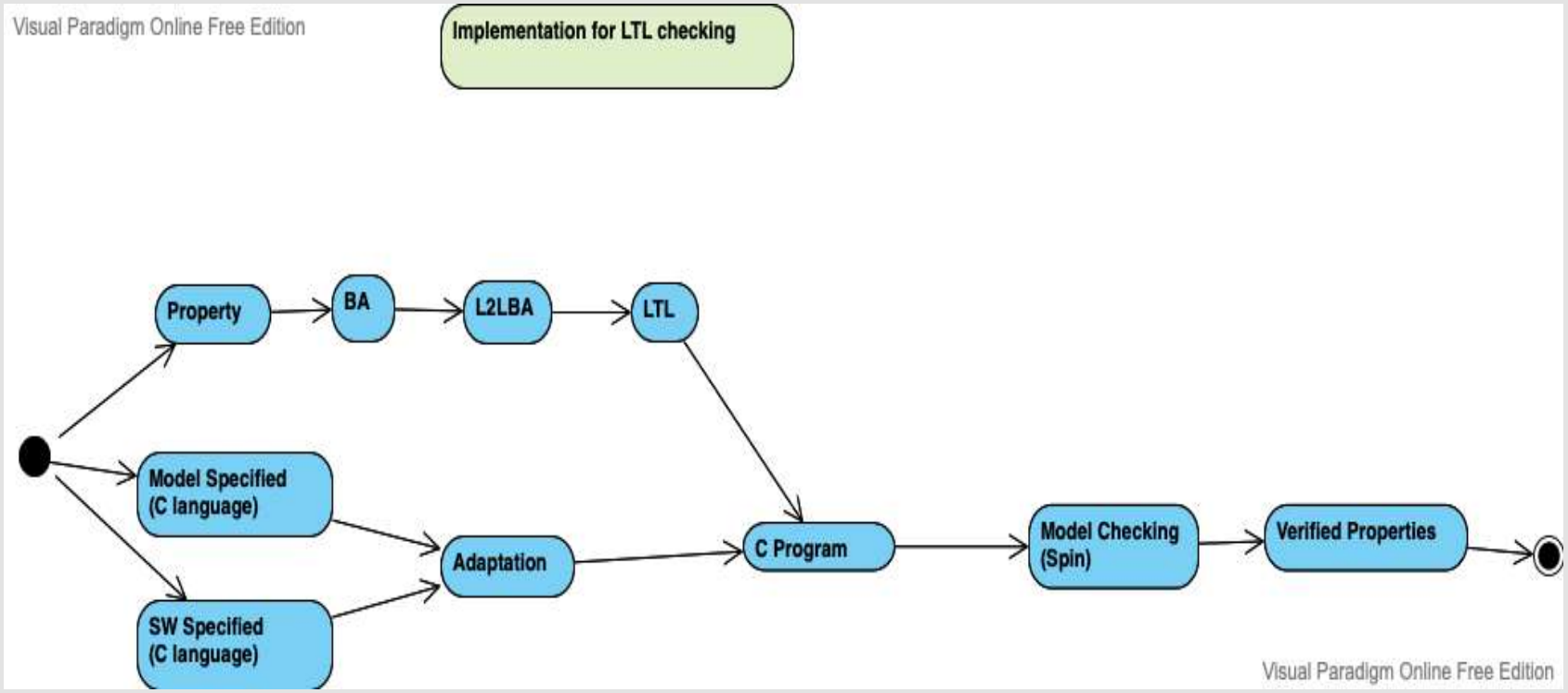


# Example for the use case

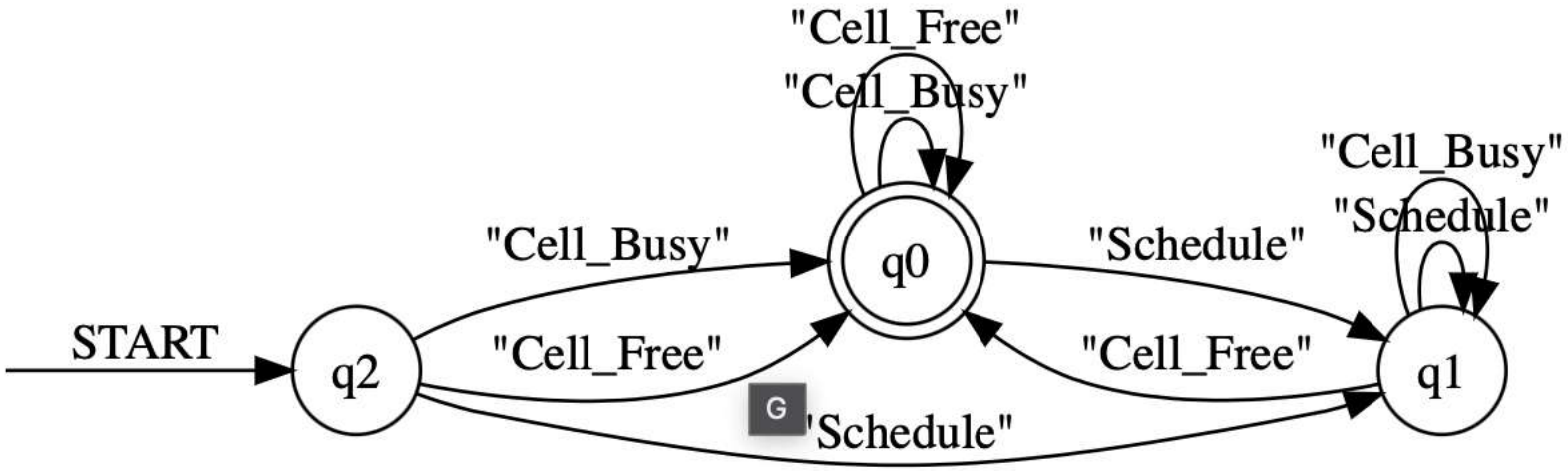



```
LTL = G ("Schedule" IMP (F "Cell_Free" AND NOT "Cell_Busy")),
ALPHABET = [Cell_Free, Schedule, Cell_Busy]
```

# Steps for the CPS verification



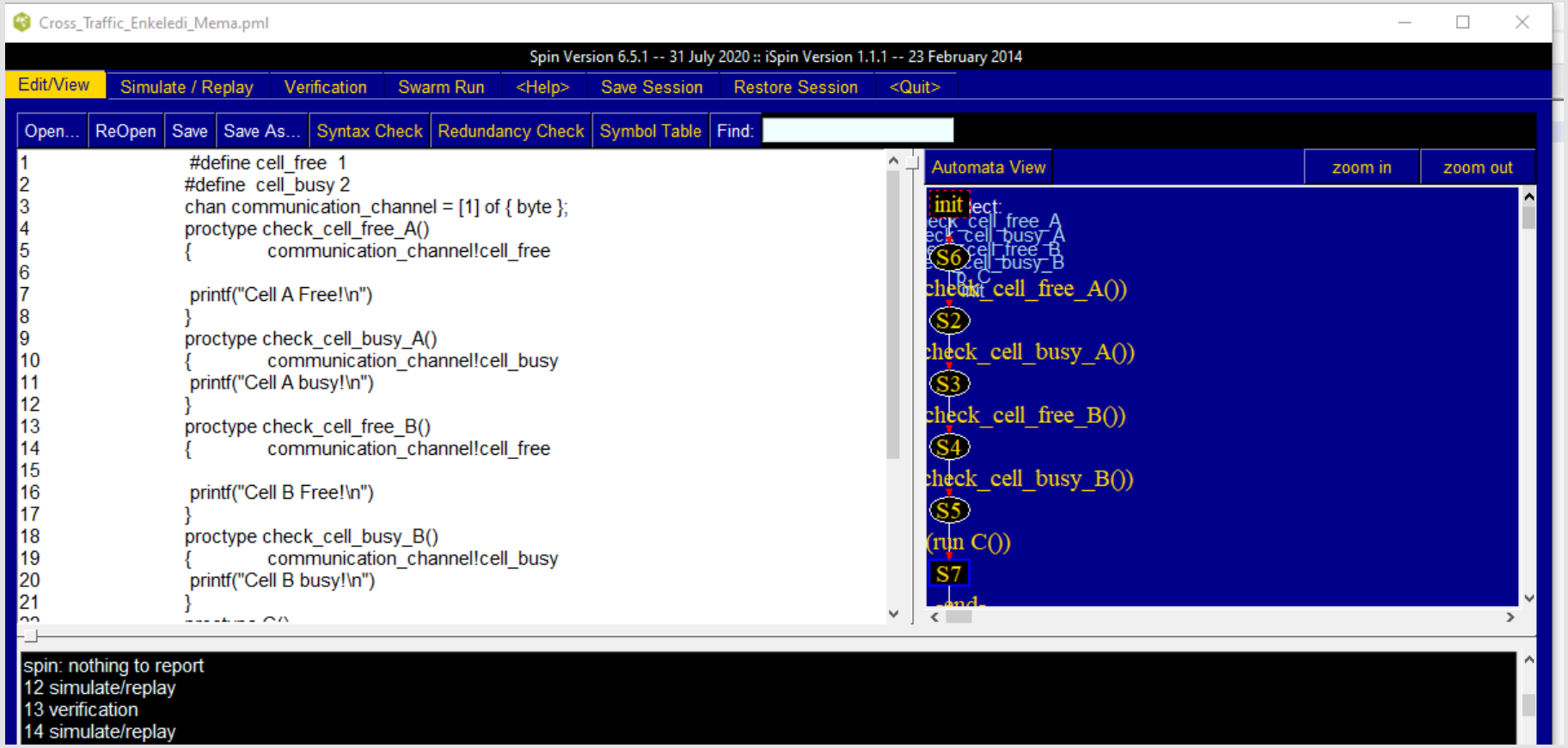
# BA for formal verification of Property



# BA converted to Spin

```
T0_init :    /* init */
        if
        :: (((! ((cell_free))) || ((schedule)))) -> goto accept_S20
        :: (! ((cell_busy))) -> goto T0_S39
        :: (((! ((cell_free)) && (cell_busy)) || ((cell_busy) && (schedule)))) -> goto accept_all
        fi;
accept_S20 :    /* 1 */
        if
        :: (((! ((cell_free))) || ((schedule)))) -> goto T0_init
        :: (! ((cell_busy))) -> goto T0_S39
        :: (((! ((cell_free)) && (cell_busy)) || ((cell_busy) && (schedule)))) -> goto accept_all
        fi;
accept_S39 :    /* 2 */
        if
        :: ((schedule)) -> goto T0_init
        :: (! ((cell_busy))) -> goto T0_S39
        :: ((cell_busy) && (schedule)) -> goto accept_all
        fi;
T0_S39 :    /* 3 */
        if
        :: ((schedule)) -> goto accept_S20
        :: (! ((cell_busy))) -> goto T0_S39
        :: (! ((cell_busy)) && (schedule)) -> goto accept_S39
        :: ((cell_busy) && (schedule)) -> goto accept_all
        fi;
accept_all :    /* 4 */
        skip
```

# Spin example



# Video or live simulation

# Conclusion

- CPS verification and validation.
- Omega expression languages such as BA and GBA.
- CPS has huge potential to change the traffic behaviour in a smart city.

# Bibliography


- [AAF] Angluin, Dana; Antonopoulos, Timos; Fisman, Dana: Strongly Unambiguous Büchi Automata Are Polynomially Predictable With Membership Queries. p. 17 pages. Artwork Size: 17 pages Medium: application/pdf Publisher: Schloss Dagstuhl - Leibniz-Zentrum fuer Informatik GmbH, Wadern/Saarbruecken, Germany Version Number: 1.0.
- [Al] Alur, Rajeev: Principles of cyber-physical systems. The MIT Press.
- [Ch] Chechik, Marsha: Automata-Theoretic LTL Model-Checking. p. 12.
- [EL] Eid, Abdulla; Lavalle, Steven M: Finite -Automata and Buchi Automata. p. 17.
- [Fi] Fisher, Corey S: A More Robust Corpus of Büchi Automata. p. 47.
- [Go] Goos, Gerhard; Hartmanis, Juris; van Leeuwen, Jan; Hutchison, David; Kanade, Takeo; Kittler, Josef; Kleinberg, Jon M; Mattern, Friedemann; Mitchell, John C; Naor, Moni; Nierstrasz, Oscar; Rangan, C Pandu; Steffen, Bernhard: Lecture Notes in Computer Science. p. 646.
- [Gr] Greer, Christopher; Burns, Martin; Wollman, David; Griffor, Edward: , Cyber-physical systems and internet of things.
- [He] Hempfling, Christina: Julius-Maximilians-Universitat Wurzburg Faculty of Mathematics and Computer Science Course of Studies: Computer Science. p. 120.
- [Li] Li, Yong; Turrini, Andrea; Chen, Yu-Fang; Zhang, Lijun: Learning Büchi Automata and Its Applications. 11430:38–98. Series Title: Lecture Notes in Computer Science.

# Thank you for attention!
# Questions?