



oMAC: Open Model for Automotive Cybersecurity

Vincent Hugot, Adrien Jousse, Christian Toinard, Benjamin Venelle

► To cite this version:

Vincent Hugot, Adrien Jousse, Christian Toinard, Benjamin Venelle. oMAC: Open Model for Automotive Cybersecurity. escar Europe 2019, Nov 2019, Stuttgart, Germany. hal-02498302

HAL Id: hal-02498302

<https://hal.science/hal-02498302>

Submitted on 4 Mar 2020

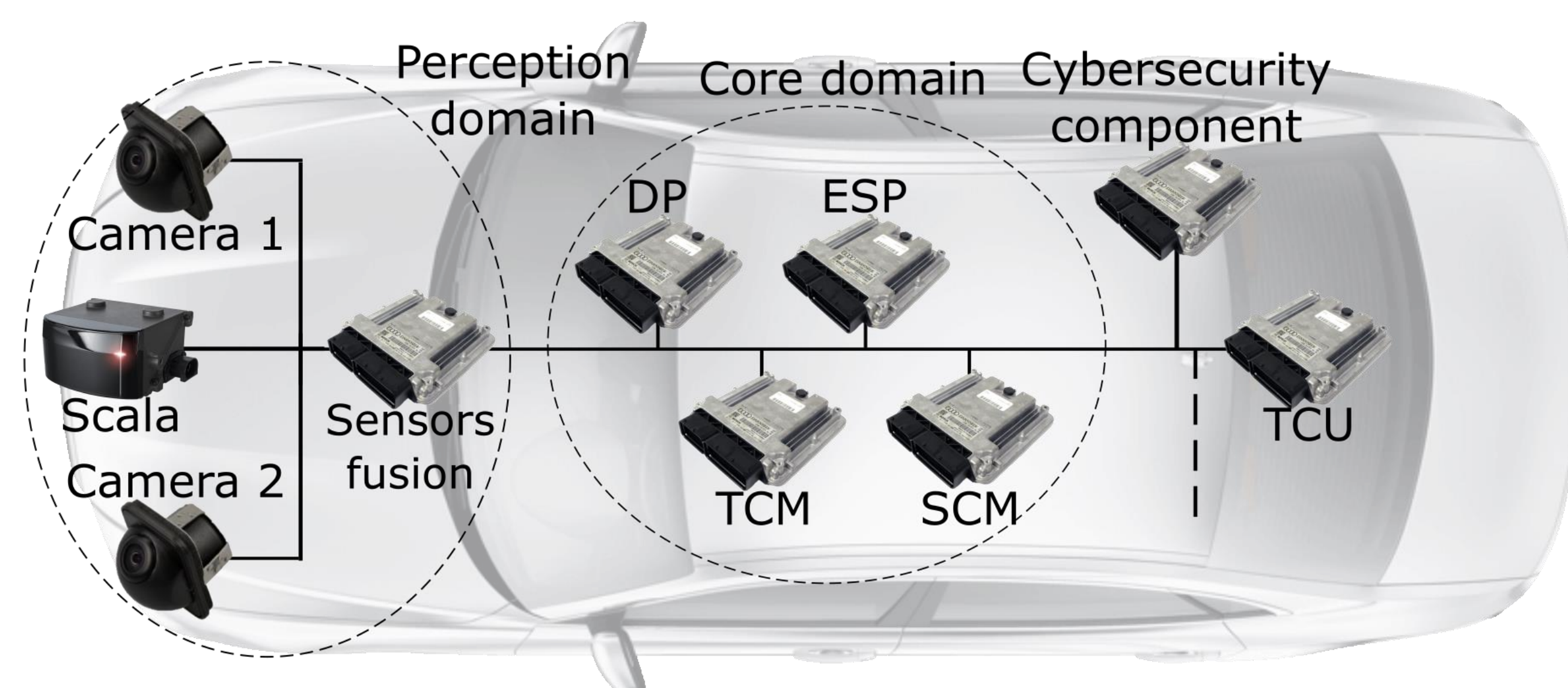
HAL is a multi-disciplinary open access archive for the deposit and dissemination of scientific research documents, whether they are published or not. The documents may come from teaching and research institutions in France or abroad, or from public or private research centers.

L'archive ouverte pluridisciplinaire **HAL**, est destinée au dépôt et à la diffusion de documents scientifiques de niveau recherche, publiés ou non, émanant des établissements d'enseignement et de recherche français ou étrangers, des laboratoires publics ou privés.

oMAC : Open Model for Automotive Cybersecurity

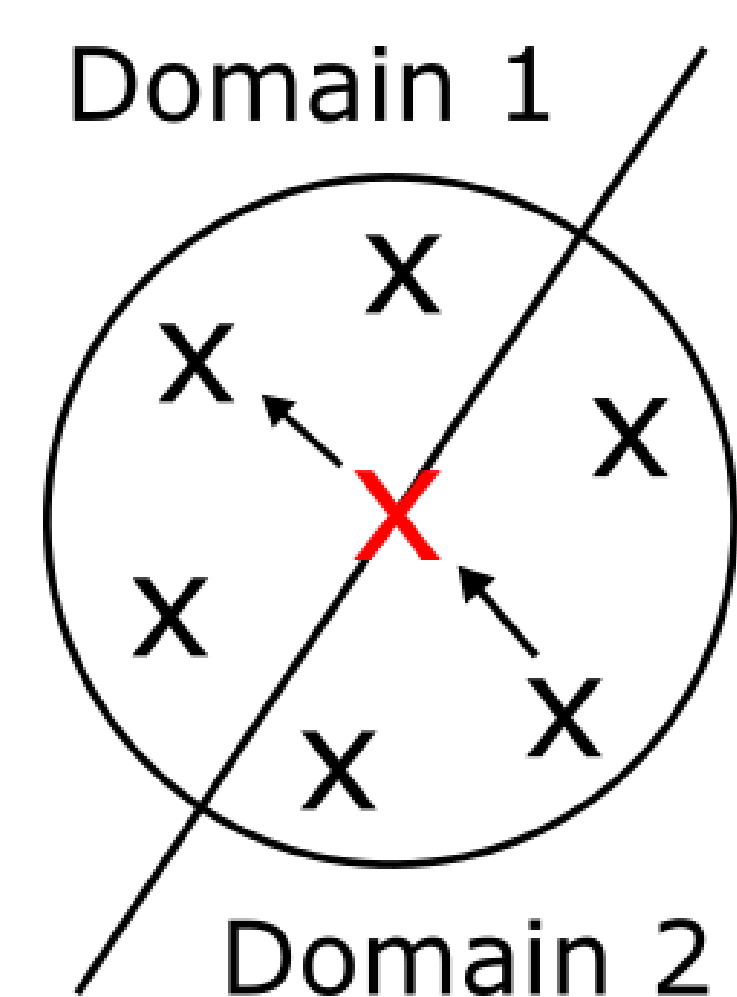
Vincent Hugot, Adrien Jousse, Christian Toinard, Benjamin Venelle

Cybersecurity has become mandatory to preserve safety. Mandatory Access Control (MAC) is needed to provide defense-in-depth to automotive architectures.

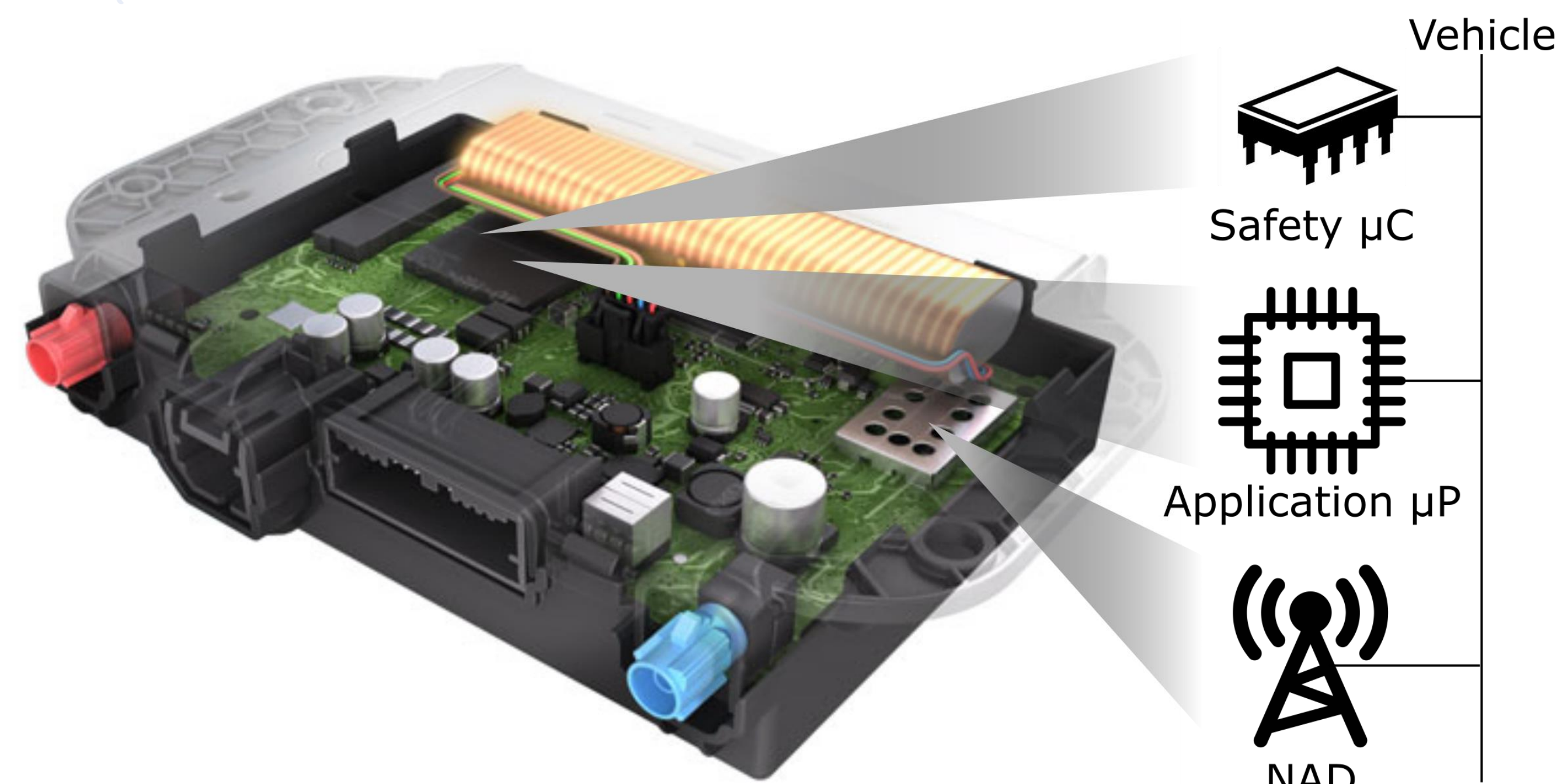


DP: Decisional Pilot TCM: Transmission Control Module
ESP: Electronic Stability Program SCM: Steering Control Module
TCU: Telematics and Communication Unit

The access control policy shall be enforced in the middleware. SOME/IP is used as a proof-of-concept. Effective access control mechanisms require enforcing the least privilege principle.



- Privilege separation: An entity with a fixed set of privileges shall not obtain further privileges.
- Duties separation: An entity can legitimately require new privileges through a mediating entity.



The following example is focused on a Telematics and Communication Unit (TCU), a privileged attack point. For the above TCU, two use cases are considered: a remote diagnostic (RD) and a remote control (RC).

$Allow\ NAD \xrightarrow{4G\ invoke\ RD} \mu P \xrightarrow{RD\ invoke\ Diag} \mu C$ (1)

$Allow\ NAD \xrightarrow{4G\ invoke\ RC} \mu P \xrightarrow{RC\ invoke\ Ctrl} \mu C$ (2)

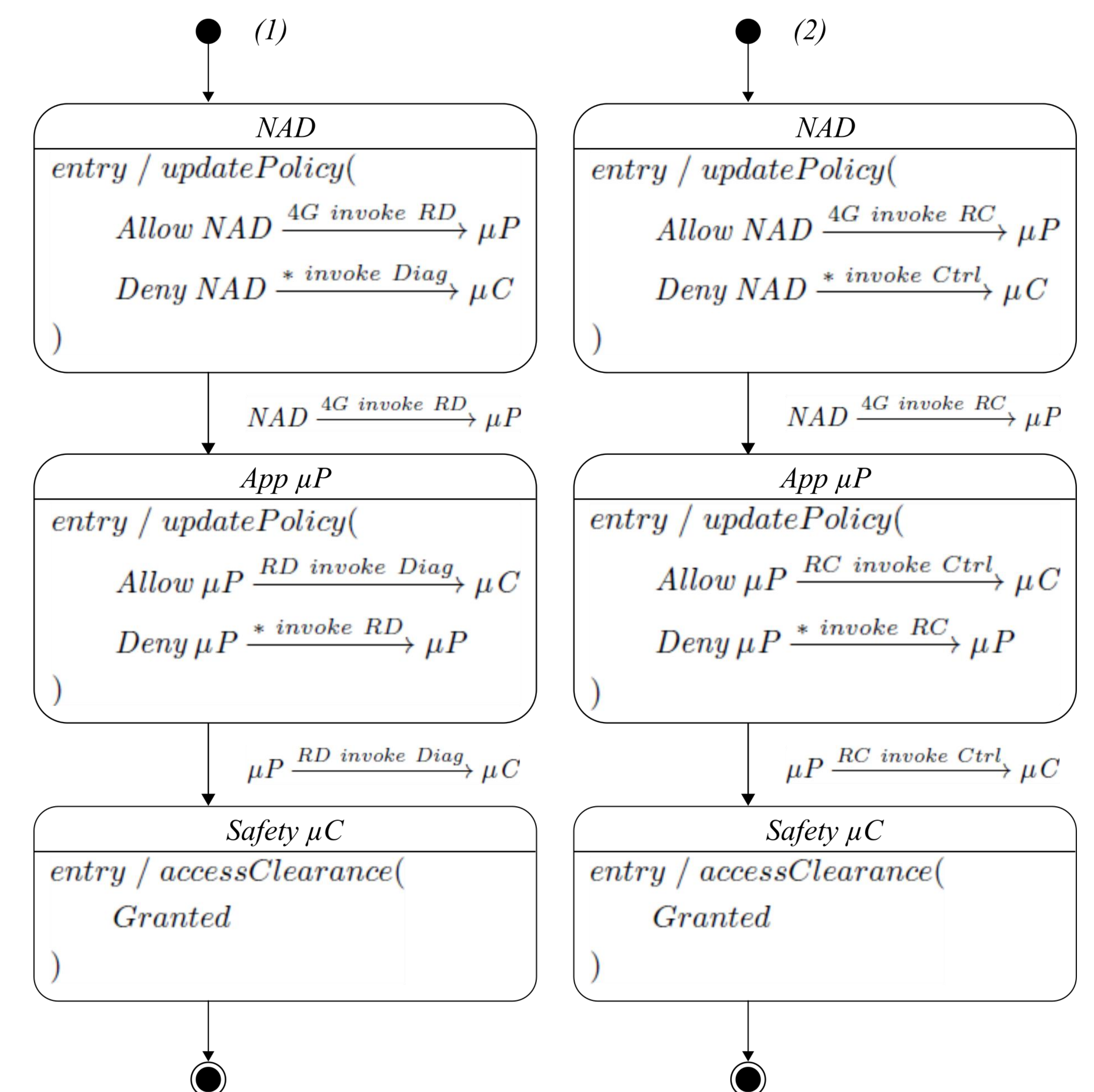
With the following ruleset and without rules sequencing, duties and privileges separation are not guaranteed. The TCU cannot guarantee these cybersecurity properties.

$Allow\ NAD \rightarrow \mu P$ $Allow\ \mu P \rightarrow \mu C$

↓ Refined access control policy ↓

$Allow\ NAD \xrightarrow{4G\ invoke\ RD} \mu P$ $Allow\ \mu P \xrightarrow{RD\ invoke\ Diag} \mu C$
 $Allow\ NAD \xrightarrow{4G\ invoke\ RC} \mu P$ $Allow\ \mu P \xrightarrow{RC\ invoke\ Ctrl} \mu C$

Access control rules must be activated according to previous access decisions. Access control automata can implement this behavior by describing the evolution of the access control policy.



The automaton changes state according to observed relations, leading to a dynamic evolution of the access control policy.