Hierarchical Assessment of Safety Requirements for Configurations of Autonomous Driving Systems

I. Appendix

We illustrate definitions of Safety Metrics for the safety requirements discussed in the paper. Fig. 1 reports the safety requirements considered in this paper, whose description is as follows:

- R_1: avoid impossible steering angles. The Safety Metric for this vehicle stability requirement at time step k is the curvature $\mathcal{X}_1(k)$ between two consecutive time step of the planned trajectory. As the curvature should be LESS THAN the threhold K_{limit}, R_1 is viewed as violated if $\mathcal{X}_1 > K_{limit}$, otherwise, R_1 is satisfied. The violation degree is calculated as follows:

$$D_k^{R_1} = \frac{\max(\mathcal{X}_1(k) - K_{limit}, 0)}{K_{limit}}$$

- R_2: keep a safe distance from other objects. The Safety Metric $\mathcal{X}_2(k, o)$ for this safety requirement is the collision danger between the ego vehicle and other objects including vehicles, pedestrians, etc. The Euclidean distance between the ego vehicle and other objects should be MORE THAN the minimum separation as ϵ_{min} , otherwise, there could be collisions, and the danger can be described by their relative speed (v_{limit} is the speed limit).

$$\mathcal{X}_2(k, o) = \begin{cases} 0, & \|\boldsymbol{x}_k^e - \boldsymbol{x}_k^o\| \geq \epsilon_{min} \\ \dfrac{\|\boldsymbol{v}_k^e - \boldsymbol{v}_k^o\|}{v_{limit}}, & \|\boldsymbol{x}_k^e - \boldsymbol{x}_k^o\| < \epsilon_{min} \end{cases}$$

$$D_k^{R_2} = \max_{o \in \mathcal{O}} \mathcal{X}_2(k, o)$$

- R_3: keep the velocity below the speed limit. The Safety Metric of this requirement related to adherence to traffic regulation is that the speed of the vehicle along the trajectory $\mathcal{X}_3(k) = \boldsymbol{v}_k^e$. $\mathcal{X}_3(k)$ should be LESS THAN the speed limit v_{limit}. The violation degree is calculated as follows:

$$D_k^{R_3} = \frac{\max(\mathcal{X}_3(k) - v_{limit}, 0)}{v_{limit}}$$

- R_4: stay in the correct lane. The Safety Metric of this requirement related to adherence to traffic regulation is that the position deviation from the central lane line. $\mathcal{X}_4(k) = |\boldsymbol{p}_k^e - \boldsymbol{p}_c|$, where $\boldsymbol{p}_c$ is the position of the central lane line. $\mathcal{X}_4(k)$ should be LESS THAN a threshold of d_0 which means the ego vehicle cannot occupy the opposite lane too much. The evaluation function is formulated with function as follows:

$$D_k^{R_4} = \frac{\max(\mathcal{X}_4(k) - d_0, 0)}{d_0}$$

- R_5: avoid too much acceleration. The Safety Metric $\mathcal{X}_5(k)$ is the acceleration value during the trajectory. $\mathcal{X}_5(k)$ should be LESS THAN the maximal acceleration as a_{max}. The violation degree is calculated as follows:

$$D_k^{R_5} = \frac{\max(\mathcal{X}_5(k) - a_{max}, 0)}{a_{max}}$$

- R_6: avoid too much deceleration. The Safety Metric $\mathcal{X}_6(k)$ is the deceleration value along the trajectory. $\mathcal{X}_6(k)$ should be MORE THAN the minimal deceleration as a_{min}. The violation degree is calculated as follows:

$$D_k^{R_6} = \frac{\max(a_{min} - \mathcal{X}_6(k), 0)}{|a_{min}|}$$

- R_7: avoid too much lateral acceleration. The Safety Metric $\mathcal{X}_7(k)$ is the lateral acceleration value during the trajectory. $\mathcal{X}_7(k)$ should be LESS THAN the maximal lateral acceleration as $latg_{max}$. The violation degree is calculated as follows:

$$D_k^{R_7} = \frac{\max(\mathcal{X}_7(k) - latg_{max}, 0)}{latg_{max}}$$

TABLE I: Sampling spaces for six traffic situations

Objects		Variables	Intervals
$t_{\mathcal{SA}}$	*vehicle-a*	$\boldsymbol{p}_0^a[x]$, $\boldsymbol{p}_0^a[y]$, $\boldsymbol{v}_0^a$, $\boldsymbol{a}_0^a$	[10, 40], [15, 29], [4, 15], [0, 2]
	vehicle-b	$\boldsymbol{p}_0^b[x]$, $\boldsymbol{p}_0^b[y]$, $\boldsymbol{v}_0^b$, $\boldsymbol{a}_0^b$	[10, 40], [31, 45], [4, 15], [0, 2]
$t_{\mathcal{M}}$	*vehicle-a*	$\boldsymbol{p}_0^a[y]$, $\boldsymbol{v}_0^a$, θ_0^a	[35, 45], [8, 15], $[-\frac{3}{5}\pi, -\frac{1}{2}\pi]$
$t_{\mathcal{H}}$	*ego vehicle*	$\boldsymbol{v}_0^e$	[8, 15]
	vehicle-a	$\boldsymbol{p}_0^a[x]$, $\boldsymbol{p}_0^a[y]$, $\boldsymbol{v}_0^a$, $\boldsymbol{a}_0^a$	[5, 7], [220, 260], [8, 15], [0, 2]
$t_{\mathcal{DA}}$	*vehicle-b*	$\boldsymbol{p}_0^b[x]$, $\boldsymbol{v}_0^b$	[20, 70], [15, 30]
$t_{\mathcal{O}}$	*vehicle-a*	$\boldsymbol{p}_0^a[x]$, $\boldsymbol{v}_0^a$, $\boldsymbol{a}_0^a$	[20, 30], [5, 10], [-2, 1]
	vehicle-b	$\boldsymbol{p}_0^b[x]$, $\boldsymbol{v}_0^b$, $\boldsymbol{a}_0^b$	[-10, 15], [4, 15], [0, 2]
$t_{\mathcal{T}}$	*vehicle-b*	$\boldsymbol{p}_0^b[x]$, $\boldsymbol{a}_0^b$	[30, 65], [0, 3]

θ_0^a is the initial direction for *vehicle-a*.

Theorem 1 (**Transitivity**). *Let $\boldsymbol{c}_1, \boldsymbol{c}_2, \boldsymbol{c}_3$ be three configurations for the ADS. Under RVC, if $\boldsymbol{c}_1$ ranks higher than $\boldsymbol{c}_2$ (i.e., $\boldsymbol{c}_1 \succeq \boldsymbol{c}_2$) and $\boldsymbol{c}_2 \succeq \boldsymbol{c}_3$, then $\boldsymbol{c}_1 \succeq \boldsymbol{c}_3$.*

Proof. Suppose $\boldsymbol{c}_1$ and $\boldsymbol{c}_2$ are distinguished under $RVCres = (\mathtt{K}, \mathcal{M}_s[i], j, \boldsymbol{c}_1 \succeq \boldsymbol{c}_2)$, and $\boldsymbol{c}_2$ and $\boldsymbol{c}_3$ are distinguished under $RVCres = (\mathtt{K}', \mathcal{M}_s[i'], j', \boldsymbol{c}_2 \succeq \boldsymbol{c}_3)$. There could be three

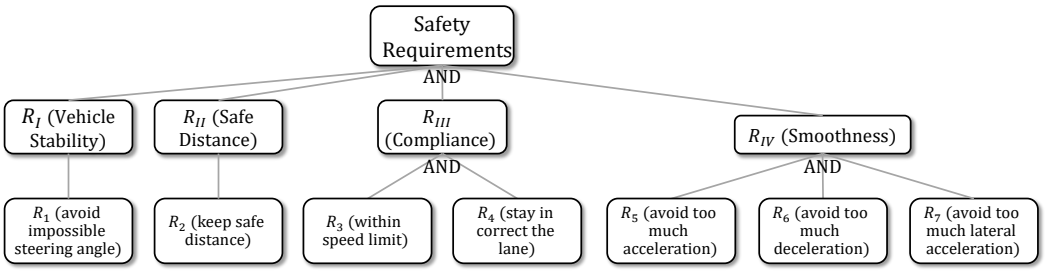

Fig. 1: The requirements considered in the ADS.

Algorithm 1: Requirements Violation Comparison

Input: $\mathcal{M}_{\boldsymbol{c}}, \mathcal{M}_{\boldsymbol{c}'}$: two sets of requirements violation mode;
$\mathcal{S}_{\boldsymbol{c}}, \mathcal{S}_{\boldsymbol{c}'}$: two sets of requirements violation severity;
$\mathtt{N}$: total number of requirements importance levels.
Output: $RVCres$: comparison results of $\boldsymbol{c}$ and $\boldsymbol{c}'$

$RVCres \leftarrow (\boldsymbol{c}' = \boldsymbol{c})$;
for $K = I \dots N$ **do**
  $A \leftarrow \{\boldsymbol{M}^t_{\boldsymbol{c}}[\mathtt{I}:\mathtt{K}] \mid \boldsymbol{M}^t_{\boldsymbol{c}} \in \mathcal{M}_{\boldsymbol{c}}\}$;
  $B \leftarrow \{\boldsymbol{M}^t_{\boldsymbol{c}'}[\mathtt{I}:\mathtt{K}] \mid \boldsymbol{M}^t_{\boldsymbol{c}'} \in \mathcal{M}_{\boldsymbol{c}'}\}$;
  $\mathcal{M}_s \leftarrow prioritize(A \cup B)$;
  for $i = 1, \dots, |\mathcal{M}_s|$ **do**
    $SS_{\boldsymbol{c}} \leftarrow \sum_t \boldsymbol{S}^t_{\boldsymbol{c}}, t \in \{x \in \mathcal{TS} \mid \boldsymbol{M}^t_{\boldsymbol{c}}[\mathtt{I}:\mathtt{K}] = \mathcal{M}_s[i]\}$;
    $SS_{\boldsymbol{c}'} \leftarrow \sum_t \boldsymbol{S}^t_{\boldsymbol{c}'}, t \in \{t \in \mathcal{TS} \mid \boldsymbol{M}^t_{\boldsymbol{c}'}[\mathtt{I}:\mathtt{K}] = \mathcal{M}_s[i]\}$;
    for $j = I, \dots, K$ **do**
      if $SS_{\boldsymbol{c}}[j] > SS_{\boldsymbol{c}'}[j]$ **then**
        $RVCres \leftarrow (\mathtt{K}, \mathcal{M}_s[i], j, \boldsymbol{c}' \succ \boldsymbol{c})$;
        Return comparison results $RVCres$;
      else if $SS_{\boldsymbol{c}}[j] < SS_{\boldsymbol{c}'}[j]$ **then**
        $RVCres \leftarrow (\mathtt{K}, \mathcal{M}_s[i], j, \boldsymbol{c} \succ \boldsymbol{c}')$;
        Return comparison results $RVCres$;
Return comparison results $RVCres$

cases as follows:
Case 1: $\mathtt{K} < \mathtt{K}'$. By assumption, in the $\mathtt{K}$-th layer, we have $\boldsymbol{c}_1 \succeq \boldsymbol{c}_2$ and $\boldsymbol{c}_2 = \boldsymbol{c}_3$; since $SS_{\boldsymbol{c}_2}$ and $SS_{\boldsymbol{c}_3}$ are the same, it is guaranteed that $\boldsymbol{c}_1 \succeq \boldsymbol{c}_3$.
Case 2: $\mathtt{K} > \mathtt{K}'$. By assumption, in the $\mathtt{K}'$-th layer, we have $\boldsymbol{c}_2 \succeq \boldsymbol{c}_3$, and $\boldsymbol{c}_1 = \boldsymbol{c}_2$; since $SS_{\boldsymbol{c}_1}$ and $SS_{\boldsymbol{c}_2}$ are the same, it is guaranteed that $\boldsymbol{c}_1 \succeq \boldsymbol{c}_3$.
Case 3: $\mathtt{K} = \mathtt{K}'$,

- Case 3.1: $\mathcal{M}_s[i]$ ranks higher than $\mathcal{M}_s[i']$ in $\mathcal{M}_s$, when comparing the sum of violation severity SS of $\mathcal{M}_s[i]$, we have $\boldsymbol{c}_1 \succeq \boldsymbol{c}_2$ and $\boldsymbol{c}_2 = \boldsymbol{c}_3$; then $\boldsymbol{c}_1 \succeq \boldsymbol{c}_3$.
- Case 3.2: $\mathcal{M}_s[i']$ ranks higher than $\mathcal{M}_s[i]$ in $\mathcal{M}_s$, when comparing the sum of violation severity SS of $\mathcal{M}_s[i']$, we have $\boldsymbol{c}_1 = \boldsymbol{c}_2$ and $\boldsymbol{c}_2 \succeq \boldsymbol{c}_3$; then $\boldsymbol{c}_1 \succeq \boldsymbol{c}_3$.
- Case 3.3: $\mathcal{M}_s[i'] = \mathcal{M}_s[i]$,
  - Case 3.3.1: $j < j'$. We have $SS_{\boldsymbol{c}_1}[j] \leq SS_{\boldsymbol{c}_2}[j]$ and $SS_{\boldsymbol{c}_2}[j] = SS_{\boldsymbol{c}_3}[j]$; so $SS_{\boldsymbol{c}_1}[j] \leq SS_{\boldsymbol{c}_3}[j]$, and $\boldsymbol{c}_1 \succeq \boldsymbol{c}_3$.
  - Case 3.3.2: $j > j'$. We have $SS_{\boldsymbol{c}_1}[j'] = SS_{\boldsymbol{c}_2}[j']$ and $SS_{\boldsymbol{c}_2}[j'] \leq SS_{\boldsymbol{c}_3}[j']$; so, $SS_{\boldsymbol{c}_1}[j'] \leq SS_{\boldsymbol{c}_3}[j']$, and $\boldsymbol{c}_1 \succeq \boldsymbol{c}_3$.
  - Case 3.3.3: $j = j'$. We have $SS_{\boldsymbol{c}_1}[j'] \leq SS_{\boldsymbol{c}_2}[j']$ and $SS_{\boldsymbol{c}_2}[j'] \leq SS_{\boldsymbol{c}_3}[j']$; so, $SS_{\boldsymbol{c}_1}[j'] \leq SS_{\boldsymbol{c}_3}[j']$, and $\boldsymbol{c}_1 \succeq \boldsymbol{c}_3$.

In all the cases we have that $\boldsymbol{c}_1 \succeq \boldsymbol{c}_3$. □