Workshop 4 (W4): 19 October 2021
Session 1 (S1): 1400 UTC
Session 2 (S2): 2200 UTC

Wksh	Time	ID	Src	Comment	Online Discussion	Disposition
W4S1	9:12:29	121	P2	Currently in Norway if you break the speed limit sign and get fined by the police, but later can prove that there was no formal/legal decision to erect that speed limit sign, you will get off the hook.		Agreed, it seems that in most countries, the individual is not held accountable for following what appear to be reasonable rules (even if unapproved), especially when there is ambiguity. However, we assume that it is also generally true that those responsible for posting unapproved information are likely to be held accountable, if they can be identified.
W4S1	9:15:36	122	P2	Discrepancy could be provided by the OEMs Volvo provided the Norwegian Public Roads Administration long lists with the detected location of speed limit signs.		Agreed. One approach would be to allow a user system to report to its disseminator; another would be to report through a trusted intermediate source, which might provide better protection of privacy.

Wkshp	Time	ID	Src	Comment	Online Discussion	Disposition
W4S1	9:15:42	123	P1	every Vehicle should report. That is very similar to what ETSI is developing in the Project Misbehaviour Reporting	P7->P1: MBR is in the context of determining misbehaviour by short range wireless broadcasters though, right? Like badly formatted CAMs and the like? P1->P7: Right, MBR is About reporting suspicious observations in Messages. Expanding this leads to reporting any Kind of suspicious observations.	Agreed; we will structure the ConOps such that every vehicle that has the ability to report any discrepancy that they detect; however, it should be noted that METR will not require vehicles to detect discrepancies nor will it require vehicles to report. Finally, METR will allow for the option of vehicles reporting to an alternate trusted third party that then provides the report. Nonetheless, specific jurisdictions can define their own detection and reporting requirements; but it appears that METR will need to be general enough to allow for multiple deployment scenarios.
W4S1	9:17:48	124	P1	Image file might be too large The ETSI MBR message contains only text		Accepted that sending an image file along with the discrepancy report might be too large for some connectivity environments; we will perhaps leave this as an optional capability

Wkshp	Time	ID	Src	Comment	Online Discussion	Disposition
W4S1	9:20:35	125	P1	[Discrepancies should not be reported] to other users - Risk of many fake reports		Agreed, that the disseminators need to be very careful so that they do not spread rumours based on a small number of reports. It is still unclear if a disseminator receives a large number of reports if the discrepancy can be publicised to users (e.g., perhaps to reduce the number of new reports generated). In other words, perhaps it is an option provided to disseminators without any recommendation.
W4S1	9:20:47	126	P8	Assumption that the vehicle may be designed to display the speed limit at all times given the segment of the roadway on which it is traveling. other than sensing signage or getting messages. Scenario noted by speaker could be likely for other more variable		Agreed, driver support systems are likely to display the speed limit at all times based on a combination of detected signage and electronic messages from a central source. Variable speed limits would be handled in a similar fashion, except current values would be based on C-ITS data.

Wksh	Time	ID	Src	Comment	Online Discussion	Disposition
W4S1	9:21:27	127	P1	METR Information to be changed only upon successful cross-checking of the real facts		The group seems to agree that the information should only be officially changed once an inconsistency has been confirmed. There remains some question whether a rule can be associated with a flag to indicate it has already been reported to be in conflict (e.g., to prevent a flood of the same report). The general sense was that this feature is likely not needed in the near future as few user systems are likely to be able to report conflicts.
W4S1	9:21:54	128	P2	In Norway it would be natural to notify the administrators of the National Road Database, which in turn would notify the responsible road office, county or city to check and correct the data.		Agreed that most issues will need to be resolved by the translator (if an error in data entry) of the regulator/competent authority (if a problem with the physical sign). However, we might allow a problem to be resolved at a lower level if that is the origin of the problem.
W4S1	9:23:06	129	P5	Reactivity may be an issue.	P7->P5: what do you mean by reactivity? P5->P7: Time constraints	Agreed, we do not expect the METR system to be able to resolve the conflicts in real-time; it will be up to the user system to determine how to handle the conflict. However, the entities responsible for managing METR should endeavour to minimize conflicts and in resolving them as quickly as possible once detected.

Wksh	Time	ID	Src	Comment	Online Discussion	Disposition
W4S1	9:24:11	130	P9	There must be some kind of feedback loop when there is discrepancy between METR data or digital maps and the physical signs on roadside. This must go back to the regulator one way or another. The OEMs might be the link..		Agreed that in almost all cases the discrepancy will involve either the translator or regulator - and the regulator might require the translator to report any corrections for awareness. Agreed that the disseminator is not the only path back to the regulator/translator and relying upon the OEM (or another third party) might be preferred by the user to protect the user's privacy.
W4S1	9:25:27	131	P1	Whether it is a METR message or a metal plate, there is Always a disseminator. In case of the metal plate, the disseminator is e.g. the City authority. Procedures should be Independent of the type of disseminator.		Agreed that in both cases there is an entity responsible for conveying the information to the public; we recommend using separate terms to distinguish the physical and electronic worlds so that we do not confuse our requirements too much. Agreed that the procedures should be a mirror of one another; but one will be more electronic.

Wkshp	Time	ID	Src	Comment	Online Discussion	Disposition
W4S1	9:26:16	132	P9	In the end it is the regulator responsible for the physical and electronic regulations According to Norwegian legislation the regulator is responsible unless it is about private parking etc..		This assumes a particular deployment scenario. Some regions of the world have not (yet?) required regulators to translate existing rules into electronic format. It is likely in these areas that the private market will attempt to fill the gap by providing an independent service, in which case, it would be the private service that is liable for the electronic representation of the rules while the regulator will continue to be responsible for the rule itself.
W4S1	9:28:24	133	P2	If the origin of the conflict-detection-event is the onboard camera in the vehicle, then the OEM will be involved, because the vehicle is doing the comparison between METR data and the real world.		Agreed that if the reading from the camera is incorrect, the OEM might become involved in a court case in an extreme situation (e.g., one involving a collision). Separately, there is still a question as to who might own the on-board data; it is certainly the case that OEMs have expressed an interest in ownership (until that ownership becomes related to a liability). The ConOps should probably stay agnostic about what entity would be involved in the data ownership but recognize that the OEMs might be involved from the analysis and/or ownership perspectives.
W4S1	9:31:11	134	P5	[Slide 9] situation-dependent		Agreed that the exact agency response is likely to be situation dependent.

Wksh	Time	ID	Src	Comment	Online Discussion	Disposition
W4S1	9:31:46	135	P2	The ITS user could report the conflict back to its Disseminator (which may in turn be the OEM Backend system or a Road Operators Central ITS Station). If the disseminator receive many conflict reports from the same area, it can propagate the reporting up the chain.		Agreed, the ConOps will be written to allow this option
W4S1	9:34:20	136	P8	[Slide 10] Assuming that the error instance is less than 0.1%, seems overkill listening to presentation. Conflict resolution process to be determined in operating procedures that is uniform among translators and center operation..		The ConOps needs to ensure that we cover standardized mechanisms to report conflicts so that they can be resolved in a timely manner before a safety-related event occurs.
W4S1	9:34:44	137	P1	All suspicious observations should be reported the same way		Agreed that road work conflicts do not appear to require any additional needs for this use case.
W4S1	9:34:58	138	P2	In all these cases, it would be wise that the vehicle chose the safest/slowest alternative. ... and then report the conflict		Agreed that this is generally true; although there are potential scenarios that pose more challenging conditions (e.g., a conflict between a 25 speed limit and a 80 speed limit)

Wkshp	Time	ID	Src	Comment	Online Discussion	Disposition
W4S1	9:36:00	139	P3	a sign on the road is always mandatory, despite any other regulation so when not covered the static sign on the road should be mandatory		You are likely correct in the sense that a court of law would rule that the intent of the lower (road work) speed limit was ambiguous and would only assess a fine based on the higher speed limit; however, the actual rule that was passed (and distributed electronically) might technically be the lower speed limit (even if unenforceable). The result, is there is a potential for vehicles travelling at different speeds, which results in the need to report the conflict.
W4S1	9:37:10	140	P5	[Slide 11] What's new?		Rules can change at any point in time, but it is expected that most rules will remain the same from one download to the next. We assume the refresh downloads will only include new/changed/deleted rules rather than a complete download.
W4S1	9:37:32	141	P2	For DENM (TIM) C-Roads recommends a very short validity duration (less than a minute) and then retransmit the DENM for as long as the situation is ongoing. The idea is that without an active ITS-G5 connection, the DENM will vanish from the vehicle		Agreed that the C-ITS data will need a very short refresh period, our question was intended to focus on the more static data rather than the C-ITS data.

Wksh	Time	ID	Src	Comment	Online Discussion	Disposition
W4S1	9:40:47	142	P5	It is important to highlight what is really new.		Agreed, when the user has already downloaded a recent rule set for the jurisdictional area, the refresh should only provide the changed rules rather than requiring a complete download. At some point, a user might need to download the complete data set.
W4S1	9:44:24	143	P2	Aviation authorities provide similar rules and restrictions to pilot before take off - like no-fly-zones		Good to know; we are recommending a similar approach where the vehicle would request rule updates at start-up, but many of the challenges occur when the user system does not have coverage on start-up. It is likely desirable to allow some flexibility as long as the on-board rule data set has not yet expired.
W4S1	9:46:50	144	P5	We must be able to handle emergency situations.		Agreed; this will be handled with C-ITS data.
W4S1	9:47:32	145	P2	It should be possible to give every individual METR-item (within a batch of rules) separate validity times, based on type of traffic rule.		Agreed that each individual rule will have its own "validity" period (i.e., the times at which the rules are enforceable such as the hours for a parking restriction). Also agreed that every batch of rules will have its own "expiration" time (i.e., the time after which the information can no longer be considered trustworthy without a rule set refresh)

Wksh	Time	ID	Src	Comment	Online Discussion	Disposition
W4S1	9:50:32	146	P5	Hybrid communications		Agreed that C-ITS data will likely use a hybrid of communications and the ConOps should provide an example of a mixture of types of communications.
W4S1	9:51:44	147	P8	[Slide 12] Is the assumption that the messages are sent in the clear or encrypted? Wrong key or key error could add to operational procedure.		In general, the assumption is that the rule information will be sent in the clear and signed so that it can be verified with a public key; this will minimize the processing requirements on the receiver.
W4S1	9:52:14	148	P2	The Central ITS Station or OEM Backend System must give the vehicle permission to drive autonomously, once the regulations are updated to an acceptable version.		Accepted that the ConOps should indicate the assumption that vehicles will need to ensure that they have unexpired rules in order to operate in ADS mode.
W4S1	9:52:21	149	P1	As I know from modern private cars, they are more or less continuously connected to the OEM's Cloud. METR-updates missing for a long time probably happens only in case of a communication failure (devices or simply Coverage)		Agreed that the problem occurs when connectivity is lost, which is typically due to no coverage. However, some areas have vast regions without coverage, which might mean prolonged periods without coverage, even at start-up.
W4S1	9:53:37	150	P8	Assumption is that tow truck does not have service capability to do electronic repair kit or authorized without special equipment.		The group largely concluded that this will be left for a future effort. It is probably possible to have a tow truck equipped for this function, but it is probably not needed until we have ADS-only vehicles (i.e., not equipped for human drivers), and that is likely a distant reality.

Wkshp	Time	ID	Src	Comment	Online Discussion	Disposition
W4S1	9:53:46	151	P2	This is a perfect job for EU CCMS	P7->P2: The CCMS gives out credentials that can be used for signing and providing auth/integrity protection. Are you suggesting a larger role?	Agreed, we expect that the CCMS for each region will provide the certificates to enable much of what is being achieved. With the CCMS-issued certificates, conflict reports can be sent to any trusted entity that is willing to take on the role. While this could, in theory, be the CCMS, we do not see a reason for the ConOps to try to constrain who might perform this role nor do we envision the US SCMS performing this role. Thus, it is better to leave it as a separate and distinct role that can be assigned to any entity.
W4S1	9:55:06	152	P1	The last Question Points to the General fall-back state. Well, if METR fails, switch on your eyes and look on the metal plates no vehicles without manual control capabilities in a near" future"		Agreed, if the user system includes the equipment to allow a human operator, then absolutely. However, a future ADS-equipped vehicle might not provide this capability. Nonetheless, the participants concluded that such vehicles are not expected in the near-term and even when they are initially deployed, they will likely be deployed primarily in urban areas where coverage will be less of an issue.

Wkshp	Time	ID	Src	Comment	Online Discussion	Disposition
W4S1	9:55:39	153	P2	I think you would need roadside assistance authorized to give the vehicle an update of rules.		The group seemed to agree that it would need to be provided from a "trusted source" with the indicated service permissions. It is still to be seen what this would exactly entail, but as vehicles without human driver controls are not envisioned in the near-term, we have some time to address this.
W4S1	9:58:26	154	P2	[Slide 13] Contractors maintaining roads could be a stakeholder		Agreed, we will conduct focused outreach to them as we near the relevant workshops (e.g., Workshop 9 on 23 Nov)
W4S1	9:58:39	155	P8	Who does the design? OEMs or first and second tier suppliers?	Design of what?	The on-board design issues are outside of the scope of the ConOps and of ISO/TC 204.
W4S1	9:58:52	156	P5	Conflicts between METR sources		Yes, in previous workshops we have agreed to assign the responsibility to each of the roles with the disseminator having primary responsibility as it should have the most comprehensive view of all rules for a given location.
W4S1	9:59:53	157	P1	METR must fully be based on standardized issues - thus there is no real room for private designs of parts of it.		Agreed that the METR interfaces should all be standardized. The implementation of specific systems might be performed by private entities.