

Exhibit J3

**EXHIBIT J3 - U.S. PATENT 9,173,100
Infringement Claim Chart**

U.S. Patent 9,173,100		Ford Activity
Row	Claim 1	Ford Vehicle Security Mechanisms
1A	<p>A vehicle, comprising:</p> <p>a plurality of on board computational components;</p> <p>a first security mechanism to enforce a security measure and form a perimeter network logically including the plurality of on board computational components; and</p>	<p>Ford has made, used, sold, offered for sale, and/or imported and are currently making, using, selling, offering for sale, and/or importing vehicles, vehicle systems (including in-vehicle security systems), and hardware and software components thereof, including non-transitory computer readable media that store computer-executable instructions and hardware and software that enable security measures in vehicles, in certain makes and models from at least the 2017 model year to the present, including those listed in Exhibit J2 (“the ’100 Accused Instrumentalities”).</p> <p>Upon information and belief, the ’100 Accused Instrumentalities implement security mechanisms described in the specifications of AUTOSAR AP (AUTomotive Open System Architecture Adaptive Platform) to enhance the safety and reliability of vehicles.¹ AUTOSAR defines an automotive open system architecture standard to support the needs of automotive applications, with AUTOSAR AP specifically designed to meet the requirements of highly automated vehicles and supports dynamic updates and reconfigurations of software systems.</p> <p>The ’100 Accused Instrumentalities include several on-board computational components, such as those that manage basic vehicle functions to advanced driver assistance systems. For example, AUTOSAR AP describes a plurality of on-board computational components that form the system architecture in the ’100 Accused Instrumentalities:</p>

¹ Ford joined AUTOSAR in 2003. Ford continues to be a core partner of the AUTOSAR partnership.

**EXHIBIT J3 - U.S. PATENT 9,173,100
Infringement Claim Chart**

<p>U.S. Patent 9,173,100</p>	<p>Ford Activity</p>
-------------------------------------	-----------------------------

In general, a security mechanism can be a technique or tool used to implement security services in a system. The '100 patent describes several exemplary security mechanisms, including encrypting access restrictions in critical components and processing modules, MAC ID filtering, privacy encryption, and various other protocols. Upon information and belief, the '100 Accused Instrumentalities include a first security mechanism to enforce a security measure and form a perimeter network logically including the plurality of on board computational components.

For example, AUTOSAR AP describes a firewall and Intrusion Detection System (IDS) in the '100 Accused Instrumentalities. The firewall supports the IDS by specifying a set of security events that can be raised in case of blocked messages. These security events are reported to the IdsM module, which is responsible for event qualification and further handling, including passing them to a Security Operations Center (SOC) or storing them persistently on the ECU. The IdsM provides a standardized interface for receiving notifications of security events, including from security sensors, that includes optional context data such as event type and suspicious data. AUTOSAR AP also includes a firewall pattern matching algorithm where

**EXHIBIT J3 - U.S. PATENT 9,173,100
Infringement Claim Chart**

U.S. Patent 9,173,100	Ford Activity
	<p>firewall rules can be configured and deployed to components operating under AUTOSAR AP. The firewall supports filtering within categories like stateless and stateful network inspection, and deep packet inspection of application layer protocols. The network packet inspection is carried out by a firewall engine, which acts based on the configured rules.</p> <p>In another example, AUTOSAR AP describes the update and configuration management (UCM) system in the '100 Accused Instrumentalities, which includes a security mechanism in the communication layer to prevent unauthorized access.</p> <div data-bbox="646 520 963 1312" style="border: 1px solid black; padding: 5px;"> <p>D.2 Securing Calls to UCM</p> <p>UCM provides a very critical functionality in the platform that allows modifying applications and platform components. In that sense, it is critical to prevent unauthorized access to UCM, meaning only legitimate callers should be allowed to reach the UCM service interface. This is primarily enforced in the communication layer supported by the Identity and Access Management. Additionally, the calls to the UCM interface shall be protected against altering, e.g. changing API arguments. When the service and client reside on the same machine, the security relies on the integrity of the operating system and the platform. In case, the service and the client are running on different machines, a secure communication, assuring authenticity and integrity of communication, is additionally required.</p> </div> <p><u>Exemplary Sources</u> https://www.autosar.org/ https://www.embitel.com/blog/embedded-blog/adaptive-autosar-vs-classic-autosar https://www.autosar.org/fileadmin/standards/R22-11/AP/AUTOSAR_EXP_PlatformDesign.pdf https://www.autosar.org/fileadmin/standards/R22-11/AP/AUTOSAR_SWS_UpdateAndConfigurationManagement.pdf https://www.autosar.org/search?tx_solr%5Bfilter%5D%5B0%5D=category%3AR22-11&tx_solr%5Bfilter%5D%5B1%5D=platform%3AAP&tx_solr%5Bq%5D=</p>

**EXHIBIT J3 - U.S. PATENT 9,173,100
Infringement Claim Chart**

U.S. Patent 9,173,100		Ford Activity
<p>1B</p> <p>a microprocessor executable network controller operable to (i) detect an instance of a breach of the security measure,</p>	<p>The '100 Accused Instrumentalities include a microprocessor executable network controller that can detect the instance of a breach of a security measure. For example, the UCM master acts as a network controller by detecting a breach in vehicle safety during an update.</p> <div data-bbox="464 506 639 1310" style="border: 1px solid black; padding: 5px;"> <p>[SWS_UCM_01117](DRAFT) UCM Master safetyState field [UCM_Master shall provide to vehicle driver interface the SafetyConditions field containing the required safety condition for the campaign as configured in safetyCondition.] (RS_UCM_00038; RS_UCM_00037)</p> <p>UCM_Master can notify vehicle driver with SafetyState field if the vehicle safety is breached during the update, by for instance popping-up a message.</p> </div> <p>Exemplary Sources https://www.autosar.org/fileadmin/standards/R22-11/AP/AUTOSAR_SWS_UpdateAndConfigurationManagement.pdf</p>	
<p>1C</p> <p>(ii) determine whether a computational component affected by the instance of a breach of the security measure can be isolated from at least one on board computational component not affected by or potentially affected by the instance of a breach of the security measure, and</p>	<p>The network controller of the '100 Accused Instrumentalities determines whether a computational component affected by the instance of a breach of the security measure can be isolated from at least one on board computational component not affected by or potentially affected by the instance of a breach of the security measure.</p> <p>For example, AUTOSAR AP describes a distributed computing architecture in the '100 Accused Instrumentalities, which makes each component independent and capable of being isolated from other components and processes. AUTOSAR AP further includes a resource monitoring component that protects unaffected parts by isolating the erroneous processes.</p>	

EXHIBIT J3 - U.S. PATENT 9,173,100 Infringement Claim Chart

U.S. Patent 9,173,100	Ford Activity
	<p>7.7.2 Resource Monitoring</p> <p>As far as technically possible, the resources which are actually used by a process should be controlled at any given time. For the entire system, the monitoring part of this activity is fulfilled by the Operating System. For details on CPU time monitoring see 7.7.3.1. For RAM monitoring see 7.7.3.4. The monitoring capabilities depend on the used Operating System. Depending on system requirements and safety goals, an appropriate Operating System has to be chosen and configured accordingly, in combination with other monitoring mechanisms (e.g. for execution deadlines) which are provided by Platform Health Management.</p> <p>Resource monitoring can serve several purposes, e.g.</p> <ul style="list-style-type: none">• Detection of misbehavior of the monitored process to initiate appropriate Recovery Actions, like process restart or state change, to maintain the provided functionality and guarantee functional safety.• Protection of other parts of the system by isolating the erroneous processes from unaffected ones to avoid resource shortage. <p>In another example, the UCM protects against downgrade attacks by ensuring that only newer software packages (i.e., packages containing newer versions of installed software) can be installed. This prevents attackers, for example, from manipulating the system by replaying an authentic but older software update package, which could potentially introduce vulnerabilities that have been fixed in newer versions. The UCM also ensures the integrity and authenticity of software packages to isolate compromised software from affecting other system components. The UCM is also tasked with preventing processing of compromised vehicle packages, which isolates other components of the vehicle from vehicle packages that constitute a security breach.</p> <p>See <i>also</i> Row 1B.</p> <p><u>Exemplary Sources</u> https://www.autosar.org/fileadmin/standards/R22-11/AP/AUTOSAR_SWS_UpdateAndConfigurationManagement.pdf</p>

**EXHIBIT J3 - U.S. PATENT 9,173,100
Infringement Claim Chart**

U.S. Patent 9,173,100	Ford Activity
<p>1D (iii) when the computational component affected by the instance of a breach of the security measure can be isolated from the at least one on board computational component not affected by or potentially affected by the instance of a breach of the security measure, at least one of;</p> <p>(a) isolate the at least one on board computational component not affected by or potentially affected by the instance of a breach of a security measure from the computational component affected by the instance of a breach of a security measure and (b) isolate the computational component affected by the instance of a breach of a security measure from the at least one on board computational component not affected by or potentially affected by the instance of a breach of a security measure,</p> <p>Examples of isolation measures performed by the '100 Accused Instrumentalities are described in Row 1C. For example, AUTOSAR AP includes a resource monitoring component that protects unaffected parts by isolating the erroneous processes. The UCM protects against downgrade attacks by ensuring that only newer software packages (i.e., packages containing newer versions of installed software) can be installed.</p>	<p>https://www.autosar.org/fileadmin/standards/R22-11/AP/AUTOSAR_SWS_ExecutionManagement.pdf</p> <p>In the network controller of the '100 Accused Instrumentalities, when the computational component affected by the instance of a breach of the security measure can be isolated from the at least one on board computational component not affected by or potentially affected by the instance of a breach of the security measure, at least one of: (a) isolate the at least one on board computational component not affected by or potentially affected by the instance of a breach of a security measure from the computational component affected by the instance of a breach of a security measure and (b) isolate the computational component affected by the instance of a breach of a security measure from the at least one on board computational component not affected by or potentially affected by the instance of a breach of a security measure,</p> <p>Examples of isolation measures performed by the '100 Accused Instrumentalities are described in Row 1C. For example, AUTOSAR AP includes a resource monitoring component that protects unaffected parts by isolating the erroneous processes. The UCM protects against downgrade attacks by ensuring that only newer software packages (i.e., packages containing newer versions of installed software) can be installed.</p>
<p>1E wherein the isolation is one or more of: (1) denying vehicular wireless network access to the computational component affected by the instance of a breach of a security measure, (2) directing communications to and from the</p>	<p>In the network controller of the '100 Accused Instrumentalities, the isolation is one or more of: (1) denying vehicular wireless network access to the computational component affected by the instance of a breach of a security measure, (2) directing communications to and from the computational component affected by the instance of a breach of a security measure to a firewall and/or gateway to enforce a security measure, (3) blocking communications to and from the computational component affected by the instance of a breach of a security measure,</p>

**EXHIBIT J3 - U.S. PATENT 9,173,100
Infringement Claim Chart**

<p>U.S. Patent 9,173,100</p>	<p>Ford Activity</p>
<p>computational component affected by the instance of a breach of a security measure to a firewall and/or gateway to enforce a security measure, (3) blocking communications to and from the computational component affected by the instance of a breach of a security measure, and (4) activating a second security mechanism in response to the instance of a breach of a security measure.</p>	<p>and (4) activating a second security mechanism in response to the instance of a breach of a security measure.</p> <p>Examples of isolation measures performed by the '100 Accused Instrumentalities are described in Rows 1A-1C. For example, the UCM in the '100 Accused Instrumentalities prevents unauthorized access to the UCM to ensure that only legitimate communications are allowed to reach the service interface. The UCM also ensures secure communications by using authentication measures, such as a Crypto Interface. In addition, AP includes a framework designed to enforce access control to resources at runtime. This isolates adaptive applications to prevent them from bypassing access control. The system also enforces access control decisions by either blocking or allowing the requests. Further, a firewall may be used to detect security events and filter network packets.</p> <div data-bbox="792 483 1258 1312" style="border: 1px solid black; padding: 5px;"> <p>14.2 Scope and Focus of the IAM framework:</p> <p>The IAM framework provides a mechanism for developers of AUTOSAR Adaptive Platform stacks and Adaptive Applications to model the intents of each application, to provide access control decisions upon access requests, and to enforce the access control. IAM focuses on providing means to limit access from Adaptive Applications to interfaces of the Adaptive Platform Foundation, Service Interfaces, and well-defined resources related to Function Clusters (e.g. KeySlots). In particular enforcing quotas on system resources like CPU or RAM is not covered by IAM.</p> <p>During runtime, the process of IAM is transparent to Adaptive Applications unless a request gets rejected and a notification is raised.</p> <p>The framework is designed to enforce access control to AUTOSAR resources at runtime. It is assumed that Adaptive Applications will be authenticated during startup and that an existing protected runtime environment ensures that Adaptive Applications are properly isolated and prevented from escalating their privileges (i.e., by-passing access control).</p> </div>

**EXHIBIT J3 - U.S. PATENT 9,173,100
Infringement Claim Chart**

<p>U.S. Patent 9,173,100</p>	<p>Ford Activity</p>
	<div data-bbox="316 457 1219 1310"> <p>Figure 20.2: Firewall architecture</p> <p>Additionally, the Firewall supports the following use-cases:</p> <ul style="list-style-type: none"> • State-dependent filtering: It is possible to define OEM-specific firewall states, where the network traffic is expected to be different (e.g. since the vehicle is currently driving, parked or in a diagnostic session). Firewall rules can be associated with a firewall state and only the rules that are associated with the currently active firewall state are used to inspect and filter network packets. The current firewall state can be set by a user-application by using an API exposed by the FC Firewall. • Security Events: The FC Firewall supports the Intrusion Detection System by specifying a set of security events that can be raised in case of blocked messages. The security events are reported to the AUTOSAR IdSM module, which takes care of event qualification and further handling of the events (passing them to a SOC or storing them persistently on the ECU). </div>
	<p>Exemplary Sources https://www.autosar.org/fileadmin/standards/R22-11/AP/AUTOSAR_SWS_UpdateAndConfigurationManagement.pdf</p>

**EXHIBIT J3 - U.S. PATENT 9,173,100
Infringement Claim Chart**

U.S. Patent 9,173,100		Ford Activity
		https://www.autosar.org/fileadmin/standards/R22-11/AP/AUTOSAR_EXP_PlatformDesign.pdf
Row	Claim 9	Ford Vehicle Security Mechanisms
9A	A method, comprising: in a vehicle comprising a plurality of on board computational components, a first security mechanism to enforce security measure and form a perimeter network logically including the plurality of on board computational components, and	Upon information and belief, the '100 Accused Instrumentalities perform the method described in Claim 9 for the reasons described previously for Claim 1 in Rows 1A through 1E. For example, the '100 Accused Instrumentalities include vehicles comprising a plurality of on board computational components and a first security mechanism to enforce security measure and form a perimeter network logically including the plurality of on board computational components. See Claim 1, Row 1A.
9B	a microprocessor executable network controller, the microprocessor executable network controller identifying a possible security breach instance;	The '100 Accused Instrumentalities include a microprocessor executable network controller, the microprocessor executable network controller identifying a possible security breach instance. See Claim 1, Row 1B.
9C	in response, the microprocessor executable network controller determining whether a computational component affected by the possible security breach instance can be isolated from at least one on board computational component not affected by the possible security breach instance; and	In response to identifying a possible security breach instance, the network controller of the '100 Accused Instrumentalities determines whether a computational component affected by the possible security breach instance can be isolated from at least one on board computational component not affected by the possible security breach instance. See Claim 1, Row 1C.

**EXHIBIT J3 - U.S. PATENT 9,173,100
Infringement Claim Chart**

U.S. Patent 9,173,100	Ford Activity
<p>9D when the computational component affected by the possible security breach instance can be isolated from the at least one on board computational component not affected by or potentially affected by the possible security breach instance, the microprocessor executable network controller at least one of (a) isolating the at least one on board computational component not affected by or potentially affected by the possible security breach instance from the computational component affected by the possible security breach instance and (b) isolating the computational component affected by the possible security breach instance from the computational component affected by the possible security breach instance, (3) blocking enforcement to a firewall and/or gateway to enforce a security measure, (4) activating a second security mechanism in response to the possible security breach instance.</p>	<p>In the '100 Accused Instrumentalities, when the computational component affected by the possible security breach instance can be isolated from the at least one on board computational component not affected by or potentially affected by the possible security breach instance, the microprocessor executable network controller at least one of (a) isolating the at least one on board computational component not affected by or potentially affected by the possible security breach instance and (b) isolating the computational component affected by the possible security breach instance from the at least one on board computational component not affected by or potentially affected by the possible security breach instance.</p> <p><i>See Claim 1, Row 1D.</i></p>
<p>9E wherein the isolation is one or more of: (1) denying vehicular wireless network access to the computational component affected by the possible security breach instance, (2) directing communications to and from the computational component affected by the possible security breach instance to a firewall and/or gateway to enforce a security measure, (3) blocking communications to and from the computational component affected by the possible security breach instance to a firewall and/or gateway to enforce a security measure, (4) activating a second security mechanism in response to the possible security breach instance.</p>	<p>In the '100 Accused Instrumentalities, the isolation is one or more of: (1) denying vehicular wireless network access to the computational component affected by the possible security breach instance, (2) directing communications to and from the computational component affected by the possible security breach instance to a firewall and/or gateway to enforce a security measure, (3) blocking communications to and from the computational component affected by the possible security breach instance, and (4) activating a second security mechanism in response to the possible security breach instance.</p> <p><i>See Claim 1, Row 1E.</i></p>

**EXHIBIT J3 - U.S. PATENT 9,173,100
Infringement Claim Chart**

U.S. Patent 9,173,100		Ford Activity
	communications to and from the computational component affected by the possible security breach instance, and (4) activating a second security mechanism in response to the possible security breach instance.	
Row	Claim 17	Ford Vehicle Security Mechanisms
17A	In a vehicle comprising a plurality of on board computational components, a non-transient, tangible computer readable medium comprising a first security mechanism to enforce security measure and form a perimeter network logically including the plurality of on board computational components	The '100 Accused Instrumentalities include a plurality of on board computational components, a non-transient, tangible computer readable medium comprising a first security mechanism to enforce security measure and form a perimeter network logically including the plurality of on board computational components. <i>See Claim 1, Row 1A.</i>
17B	and a microprocessor executable network controller on board a selected vehicle that, when executed,	The '100 Accused Instrumentalities include a microprocessor executable network controller on board a selected vehicle that, when executed, satisfies the requirements set forth in Rows 17C-17E, as explained below. <i>See Claim 1, Row 1B.</i>
17C	detects an instance of a breach of the security measure, determines whether a computational component affected by the instance of a breach of the security measure can be isolated from at least one on board computational component not affected by or potentially affected by the instance of a breach of the security measure	The network controller of the '100 Accused Instrumentalities detects an instance of a breach of the security measure, determines whether a computational component affected by the instance of a breach of the security measure can be isolated from at least one on board computational component not affected by or potentially affected by the instance of a breach of the security measure. <i>See Claim 1, Rows 1B and 1C.</i>

**EXHIBIT J3 - U.S. PATENT 9,173,100
Infringement Claim Chart**

U.S. Patent 9,173,100	Ford Activity
instance of a breach of the security measure to a firewall and/or gateway to enforce a security measure, (3) blocking communications to and from the computational component affected by the instance of a breach of the security measure, and (4) activating a second security mechanism in response to the instance of a breach of the security measure.	activating a second security mechanism in response to the instance of a breach of the security measure. See Claim 1, Row 1E.