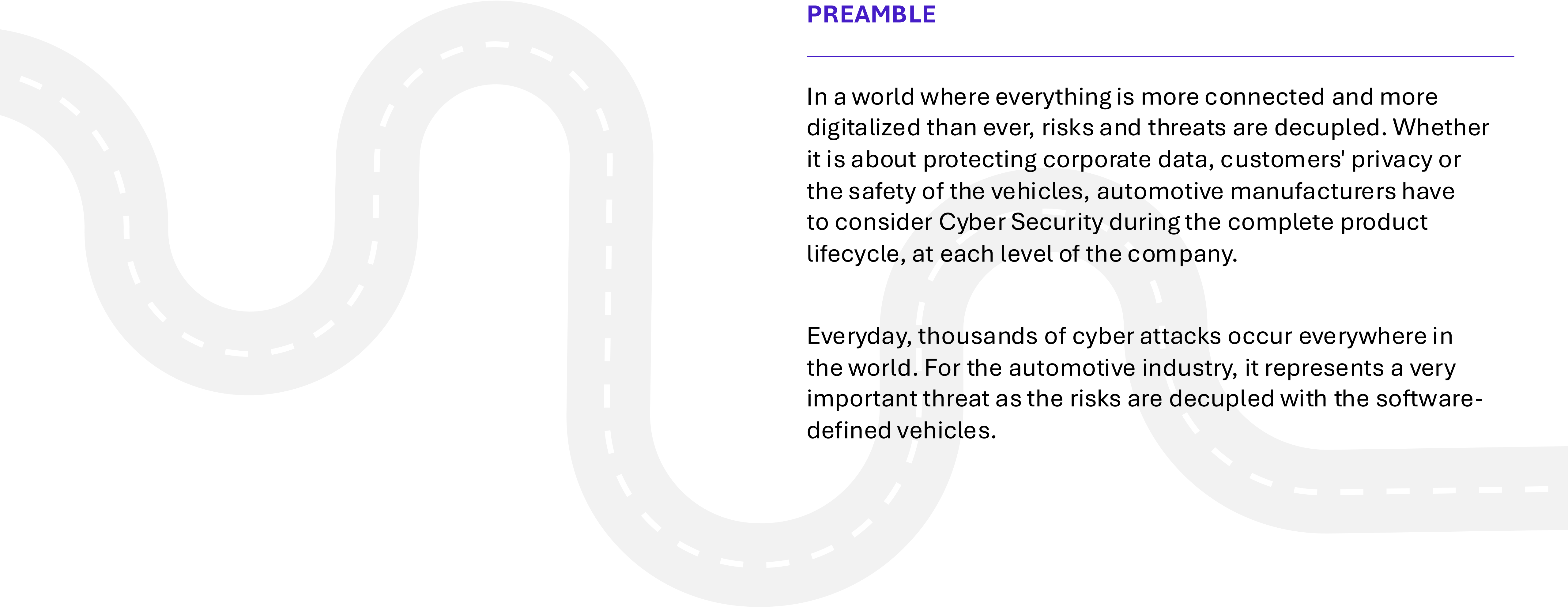
AUTOMOTIVE CYBER SECURITY FRAMEWORK

WAVESTONE

AUTOMOTIVE CYBER SECURITY FRAMEWORK



PREAMBLE

In a world where everything is more connected and more digitalized than ever, risks and threats are decupled. Whether it is about protecting corporate data, customers' privacy or the safety of the vehicles, automotive manufacturers have to consider Cyber Security during the complete product lifecycle, at each level of the company.

Everyday, thousands of cyber attacks occur everywhere in the world. For the automotive industry, it represents a very important threat as the risks are decupled with the software-defined vehicles.

STRATEGY

SECURITY BEGINS WITH A STRATEGY.

S1 – S6

R&D

SECURITY-BY-DESIGN.

RD1 – RD9

PRODUCTION

PRODUCTION PLAYS A CRUCIAL ROLE IN THE SECURITY CHAIN.

P1 – P3

ON THE ROAD

SECURITY MUST BE CONSIDERED ON THE ROAD.

OTR1 – OTR6

SECURITY BEGINS WITH A STRATEGY

WHAT & WHY

Threats and Risks have evolved very quickly over the past years in the **automotive industry.** To face them, companies have to address Cyber Security from end-to-end, which requires a **structured approach** and **organization**, a strong governance and strategy from the beginning.

MAJOR CHALLENGES

Considered for long as a niche topic, Cyber Security was delegated by executives to operational teams and experts. Poor attention was paid to it, resulting in low budgets and only partial risk understanding and mitigation.

OUR CONVICTION

Deploying technical solutions alone does not define the security of a product or entity. The executive level must increase their understanding of the new risks and threats and show a strong commitment to their product security lifecycle. Cyber Security can become a competitive differentiating factor for Automotive players if addressed with the right budget and at the right level.

HOW TO MANAGE SECURITY AT THE CORPORATE LEVEL?

S1

BUSINESS SECURITY NEEDS ASSESSMENT

What risks are you afraid of? What is the balance between security and operations?
These are questions a Business Security Needs assessment aims to answer. By improving your knowledge about your own security needs, you can make informed decisions with a constrained budget.

S2

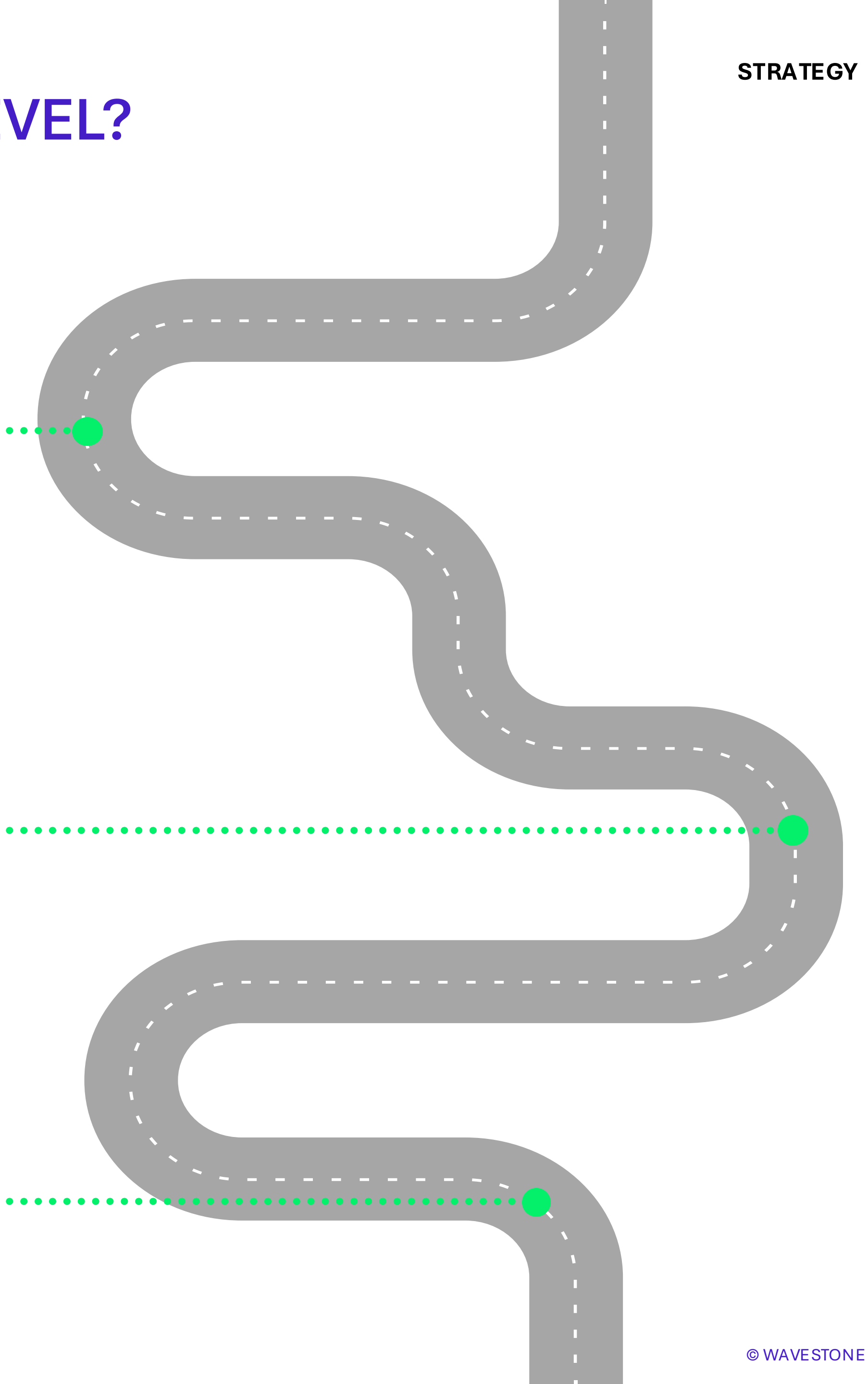
THREATS LANDSCAPE

Know your enemy! Defining the threats landscape will help you to understand who the malicious actors are, where they come from and why and how they would target your business.
The understanding of this landscape is a pre-requisite to establish your Cyber Security strategy.

S3

CYBER SECURITY STRATEGY

Cyber Security is not a sprint, but a marathon. You will have to build teams, tools, processes to support the activities. Once you have assessed your risks and the threats you face, it becomes essential to draw a roadmap with priority actions.



HOW TO MANAGE SECURITY AT THE CORPORATE LEVEL?

S1

BUSINESS SECURITY NEEDS ASSESSMENT

What risks are you afraid of? What is the balance between security and operations? These are ques
assessment aims to answer. By
your own security needs, you ca
a constrained budget.

S2

THREATS LANDSCAPE

Know your enemy! Defining the t
understand who the malicious a
and why and how they would tar
The understanding of this landsc
your Cyber Security strategy.

S3

CYBER SECURITY STRATEGY

Cyber Security is not a sprint, but a marathon. You will have to build teams, tools, processes to support the activities. Once you have assessed your risks and the threats you face, it becomes essential to draw a roadmap with priority actions.

HOW WE CAN SUPPORT YOU?

We help you to identify the risks associated with your business and we support the definition of your Cyber Security strategy.

HOW CAN GOVERNANCE SUPPORT YOUR SECURITY?

S4

SECURITY POLICIES & GUIDELINES

Cyber Security is not (only) a technical topic. It is also organizational and requires clear directions: roles and responsibilities must be defined, as well as security policies and guidelines. It aims at giving clear high level requirements to ease the risk management decisions.

S5

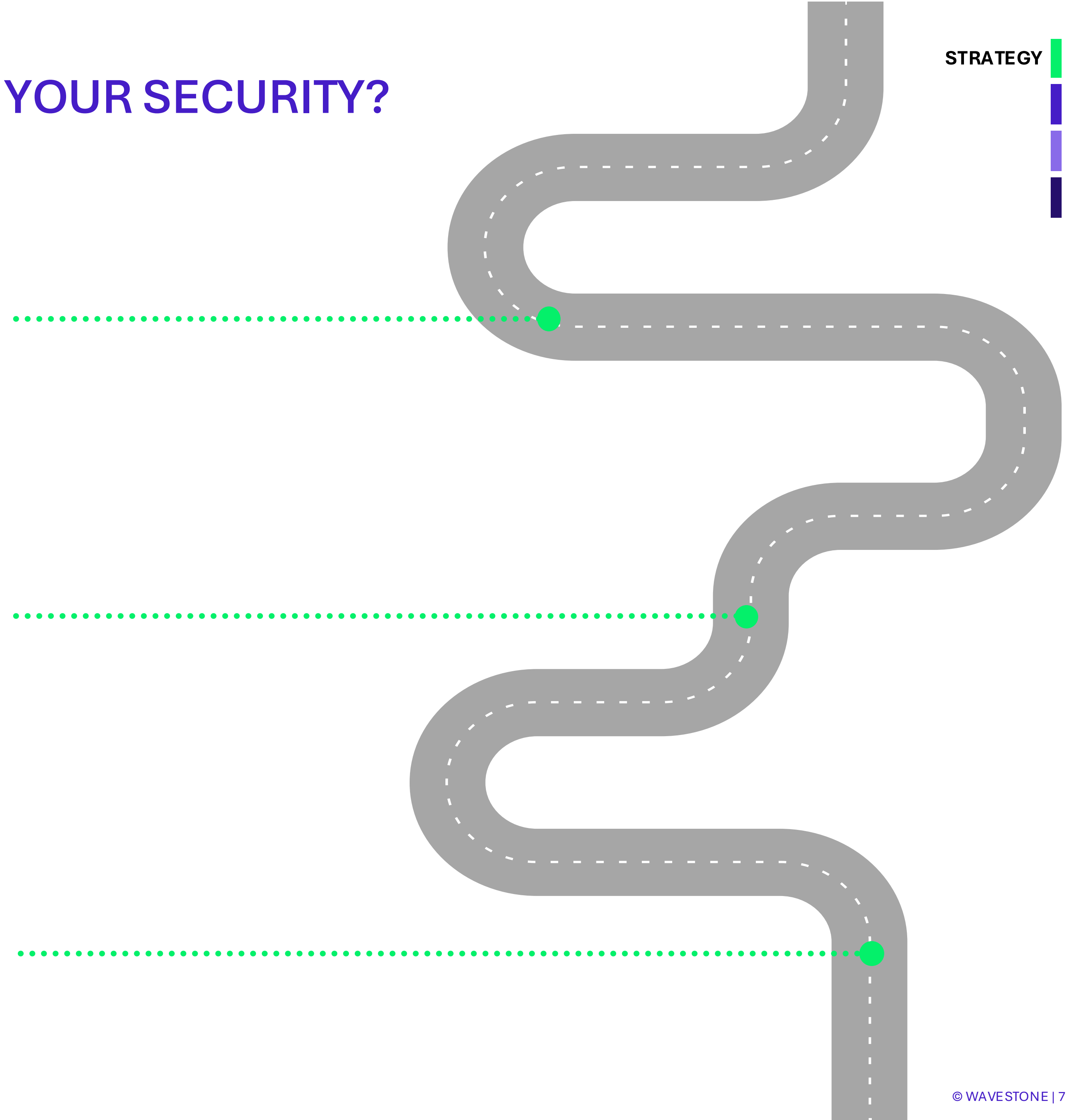
CYBER SECURITY MANAGEMENT SYSTEM

Your strategy and your policies have been established? You need now to make it happen. This is the role of a Cyber Security Management System (CSMS), a structure that will implement, control and improve continuously all your Cyber Security activities according to your pre-defined strategy.

S6

ROLES & RESPONSIBILITIES

Because Cyber Security is a complex topic, one needs to have a clear organization and role separation within the company. Who accepts or refuses the risk? Who controls the good implementation of security measures? Who takes the decision, who supports it? Risk management is highly based on a good RASIC matrix at the company level.



HOW CAN GOVERNANCE SUPPORT YOUR SECURITY?

S4

SECURITY POLICIES & GUID

Cyber Security is not (only) a tec
and requires clear directions: ro
defined, as well as security polic
clear high level requirements to

S5

CYBER SECURITY MANAGE

Your strategy and your policies h
to make it happen. This is the rol
System (CSMS), a structure that
continuously all your Cyber Sec
defined strategy.

S6

ROLES & RESPONSIBILITIES

Because Cyber Security is a complex topic, one needs to have a clear organization and role separation within the company. Who accepts or refuses the risk? Who controls the good implementation of security measures? Who takes the decision, who supports it? Risk management is highly based on a good RASIC matrix at the company level.

HOW WE CAN SUPPORT YOU?

We help you to achieve your strategic goals for Cyber Security by defining your Security policies and processes – both for corporate IT and products.

We bring your security to the next level with the implementation of a Cyber Security Management System (CSMS) in accordance with the UN R155 requirements.

R&D SECURITY-BY-DESIGN

WHAT & WHY

Integrating security into a product can be expensive – especially during later development stages. That is why development must follow a "security-by-design" approach. This concept involves a risk-based analysis, clear requirements and architecture focused on security.

MAJOR CHALLENGES

Identifying risks and aligning security objectives with business strategy can be a source of internal conflicts.

Moreover, multiple stakeholders are involved in security activities, from system architects to developers, together with many suppliers.

OUR CONVICTION

Delivering a secure product relies heavily on teams that can take the necessary actions in a security-by-design approach. This requires a strong security mindset within the teams.

Security must become one of the core driven-principles for the product design, at the same level than the business strategy or market demands.

HOW TO DESIGN A SECURE PRODUCT?

RD1

RISK MANAGEMENT IN PROJECTS

Alike to the corporate governance, a clear communication regarding roles and responsibilities is necessary for the security in project development. Assessed risks or findings from a penetration test must be addressed, but depending on the nature of the risks, it could be done in different ways, i.e., by accepting the risk if it is deemed necessary or acceptable on business terms. This requires a clear path of escalation and process for triggering the decisions and the correct people to be able to make this decision.

RD2

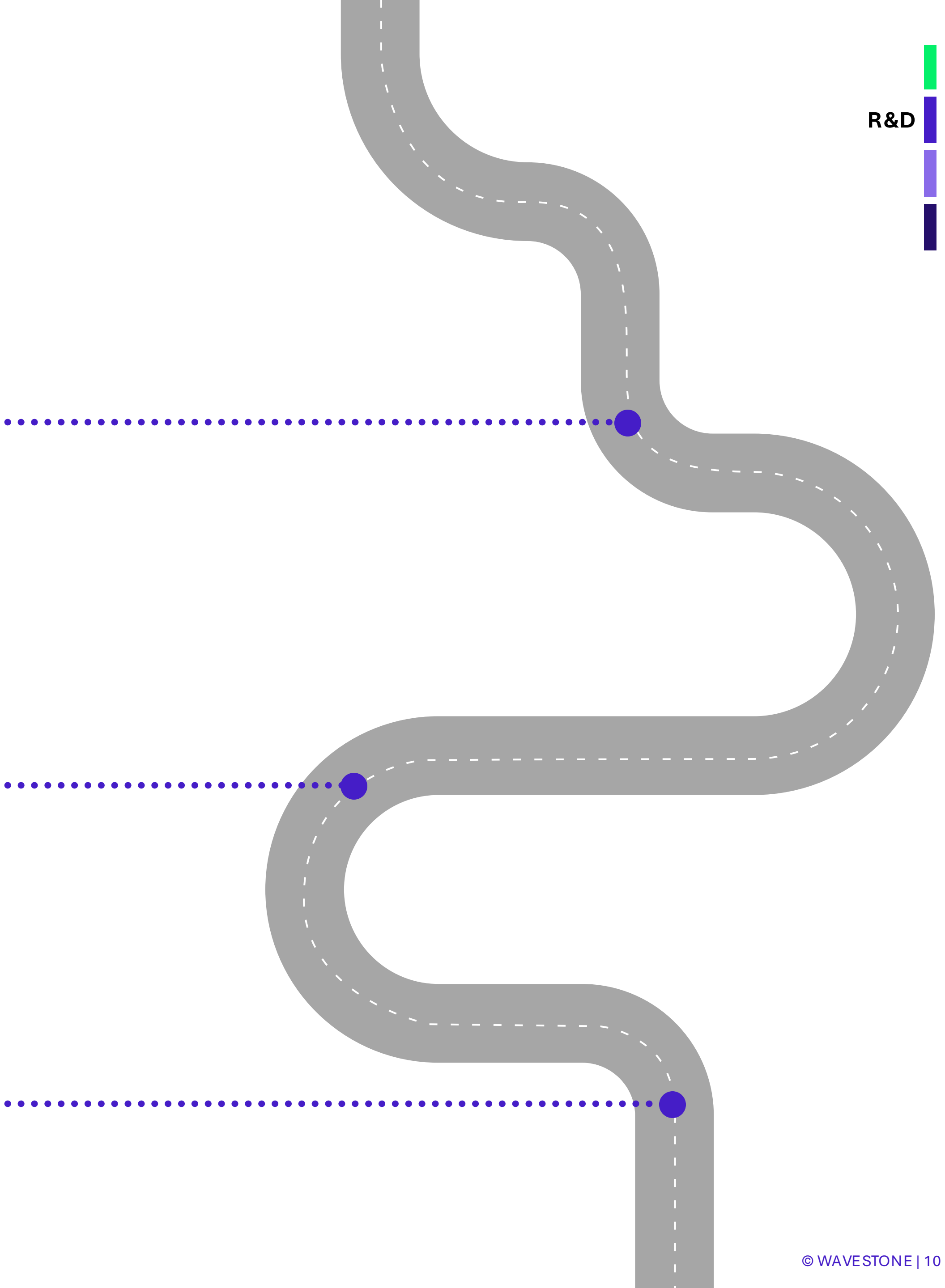
THREAT & RISK ASSESSMENT

Risk is a combination of impact of a potential attack and its likelihood of occurring. Identifying the security risk associated with a product is essential when making informed decisions about which security features are really required - in accordance with the budget.
This risk-based approach relies on (a) defined attacker models, (b) a realistic scope for possible attacks on the product and (c) a qualitative analysis of attacker capabilities and threats that results in a reproducible and comparable assessment.

RD3

SECURITY CONCEPT & ARCHITECTURE

Identified risks that exceed an acceptable level for a product must be mitigated with a combination of a security-by-design architecture and of dedicated security mechanisms that directly mitigate risks such as the encryption of sensitive data during communication. It is also crucial to formulate understandable and testable requirements on a system level.



HOW TO DESIGN A SECURE PRODUCT?

HOW WE CAN SUPPORT YOU?

Because security strategy success is a matter of people, processes and technology, our experts help with setting up all required risk management processes and enable your teams with coaching and training sessions to be compliant with the defined policies and guidelines.

We help to identify product security risks and to define appropriate remediations concept that mitigate the identified risk in order to achieve the desired security level.

RD1

RISK MANAGEMENT IN PRO

Alike to the corporate governance
necessary for the security in proje
test must be addressed, but depe
ways, i.e., by accepting the risk if i
requires a clear path of escalation
people to be able to make this dec

RD2

THREAT & RISK ASSESSMEN

Risk is a combination of impact of
the security risk associated with a
which security features are really
This risk-based approach relies o
attacks on the product and (c) a q
results in a repro- ducible and con

RD3

CYBER SECURITY STRATEGY

Cyber Security is not a sprint, but
support the activities. Once you have assessed your risks and the threats you face, it becomes essential to draw a roadmap with priority actions.

WHAT ARE THE FUNDAMENTALS TO ENSURE SECURITY IN CODE?

RD4

SECURITY SOFTWARE SPECIFICATIONS

Software specifications must be defined by breaking down the security concept into software requirements and configuration parameters. Indeed, a good security measure must be appropriately configured to provide adequate protection. Additionally, the agile software development approach requires to integrate security acceptance criteria in stories which can be derived from the software specifications.

RD5

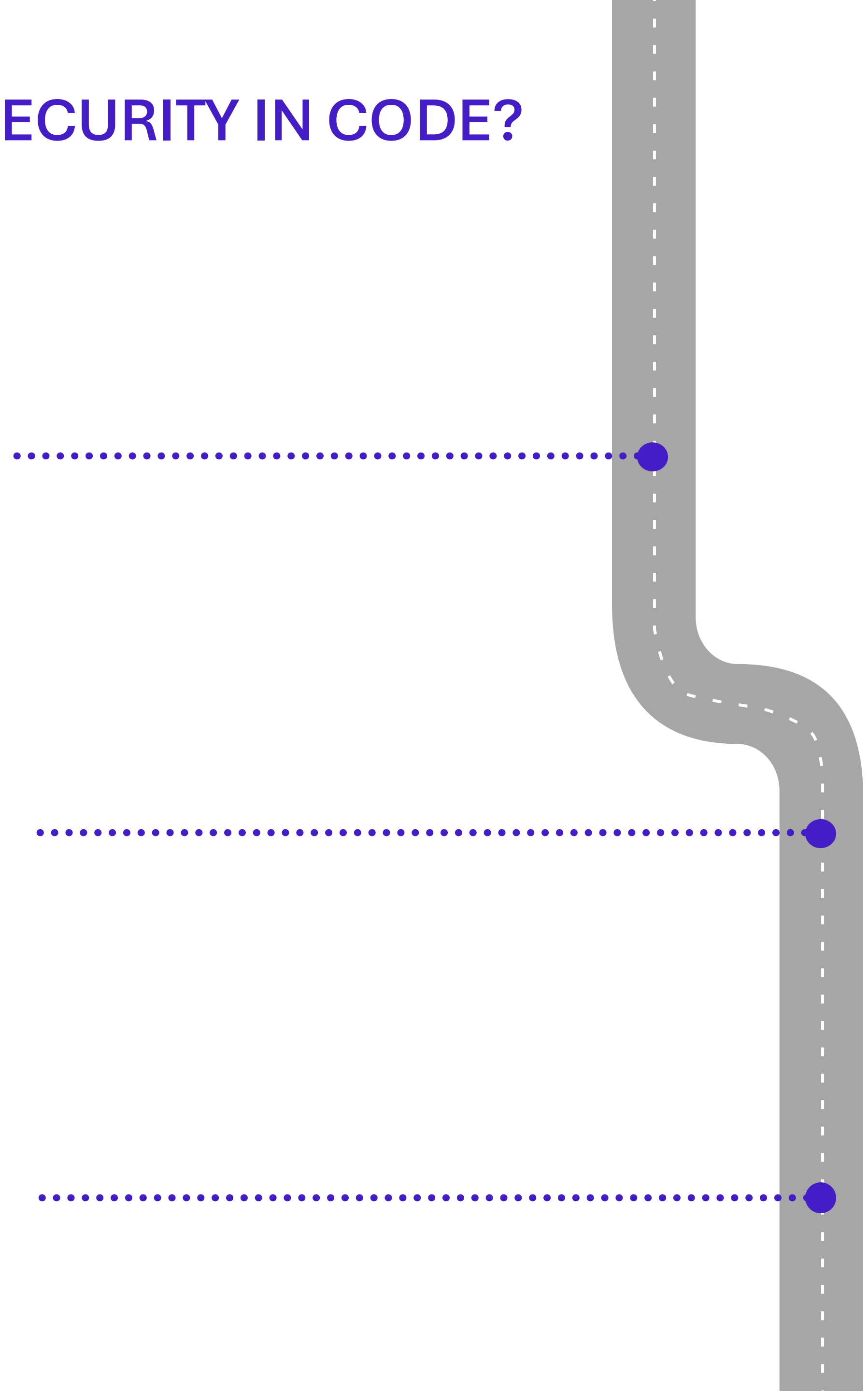
DEVELOPMENT ENVIRONMENT

There are many challenges concerning the security of development environment, but aside from the regular IT Security and governance topics, the most important ones are a secure supply chain (e.g., vetted third-party libraries) and a vulnerability discovery and management process. While a Continuous Integration (CI), Testing (CT) and Deployment (CD) toolchain can address these topics, its central position in the development process requires specific attention to guarantee its protection.

RD6

SECURE CODING

A development environment tailored for security is not the only key factor when developing a secure product. The development team must adhere to the language specific secure coding guidelines and best practices. It applies to the entire product with an extra care given to security-sensitive parts. For instance, only vetted security libraries must handle cryptographic primitives, input validations should be systematic, use type-safe language whenever possible, etc.



WHAT ARE THE FUNDAMENTALS TO ENSURE SECURITY IN CODE?

RD4

SECURITY SOFTWARE SPEC

Software specifications must be c
requirements and configuration p
appropriately configured to provid
development approach requires t
derived from the software specific

RD5

DEVELOPMENT ENVIRONM

There are many challenges concern
regular IT Security and governance
vetted third-party libraries) and a vu
Continuous Integration (CI), Testing
central position in the development

RD6

SECURE CODING

A development environment tailo
secure product. The development team must adhere to the language specific secure coding guidelines and best practices. It applies to the entire product with an extra care given to security-sensitive parts. For instance, only vetted security libraries must handle cryptographic primitives, input validations should be systematic, use type-safe language whenever possible, etc.

HOW WE CAN SUPPORT YOU?

In a "hands-on" position or as security advisor, we support your teams by deriving software specifications from a system level concept - including acceptance criteria. We provide security trainings tailored to the developers' needs to evangelize best coding practices. Additionally, we also offer a detailed guidance on security sensitive parts to ease their implementation. Finally, we help you to secure your development environment and to detect and mitigate any leaks of sensitive information.

HOW TO VALIDATE THE PRODUCT SECURITY?

RD7

SOFTWARE SECURITY TESTING

Delivering a secure product requires rigorous testing of the software and hardware. A good set-up ensures regular functional testing of all security measures and their integration into the product functionality. These tests should be tool-supported e.g., in a CI/CD environment, and should include automated vulnerability scanning in addition to manual code reviews and fuzz-testing to discover any potential flaws.

RD8

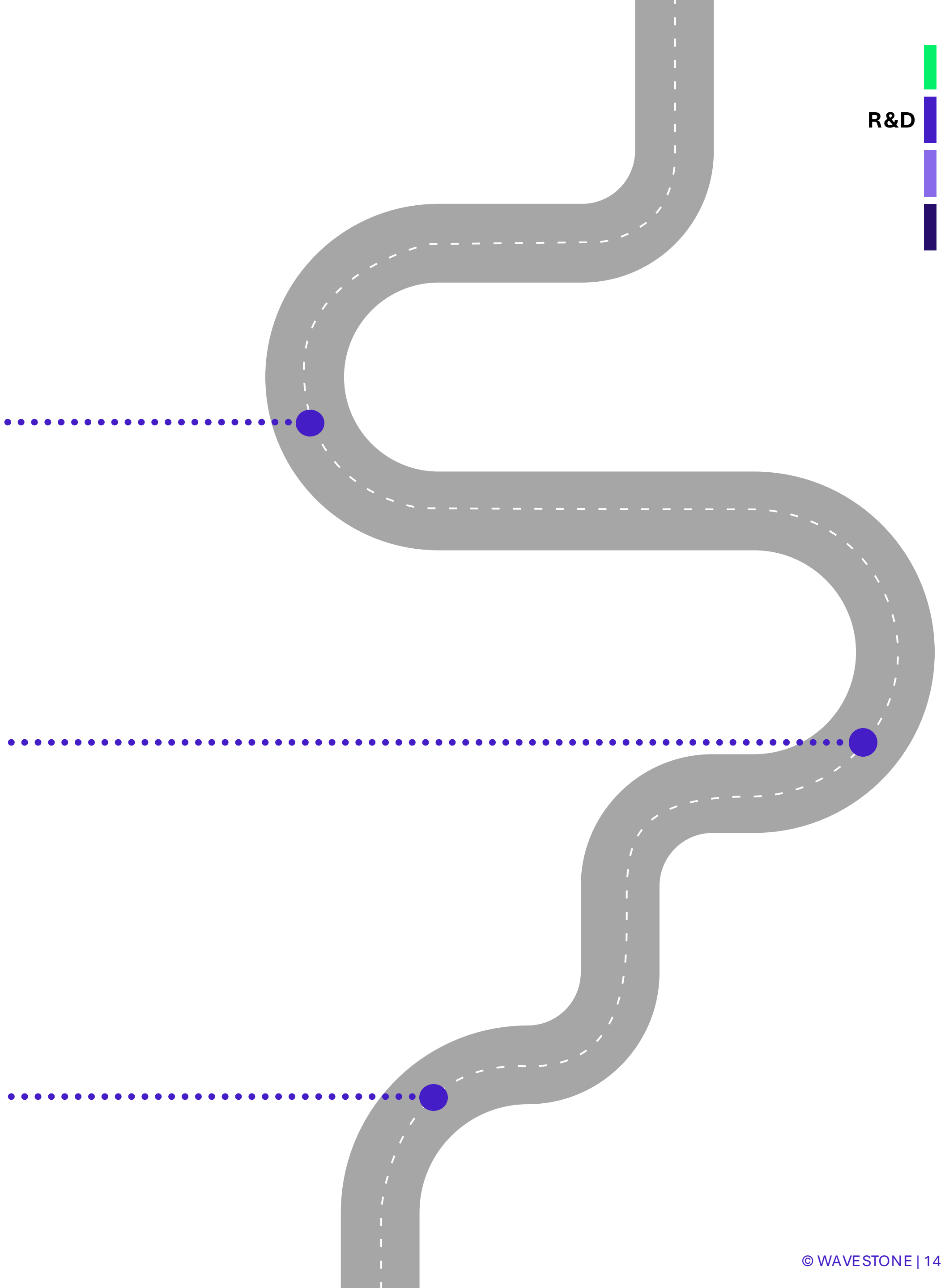
PENETRATION TESTING

External verification of the product is essential to reveal security flaws. This can be achieved by verifying only parts of a products (e.g., only the software), or the entire system is tested end-to-end (software, firmware and hardware). Furthermore, the combination of the different approaches allows you to tailor your penetration tests. On one hand, a white-box test (with all code and documentation available) will enable to find more vulnerabilities in your code, while a black-box test (just the product without any additional resources) will reveal flaws in the product under a different attack scenario.

RD9

THIRD-PARTY SECURITY CONTROLS

Products may rely on software and hardware supplied by third parties. It is not only essential to require compliance with standards (e.g., ISO/SAE 21434) and to make agreements about security responsibilities for products (e.g., Developer Interface Agreements), but also to verify and control the adherence to the agreements (e.g., black-box penetration tests). For integrated third-party FOSS libraries, their open nature makes it simpler but does not remove the diligence and necessary budget to be spent on the verification of the supply-chain's security.



AUTOMOTIVE CYBER SECURITY FRAMEWORK

HOW TO VALIDATE THE PRODUCT SECURITY?

HOW WE CAN SUPPORT YOU?

Our Experts support testing activities by writing concepts focused on the security testing. We help you to deploy adequate testing solutions in your development environment. In addition, we offer penetration test of your product or of a third-party supplied component. We can also evaluate existing reports and advise about findings / recommendations.

RD7

SOFTWARE SECURITY TEST

Delivering a secure product requires
ensures regular functional testing of
functionality. These tests should be
include automated vulnerability sca
and fuzz-testing to discover any pote

RD8

PENETRATION TESTING

External verification of the product i
verifying only parts of a products (e.g
(software, firmware and hardware).
you to tailor your penetration tests. C
available) will enable to find more vu
without any additional resources) w

RD9

THIRD-PARTY SECURITY CO

Products may rely on software and hardware supplied by third parties. It is not only essential to require compliance with standards (e.g., ISO/SAE 21434) and to make agreements about security responsibilities for products (e.g., Developer Interface Agreements), but also to verify and control the adherence to the agreements (e.g., black-box penetration tests). For integrated third-party FOSS libraries, their open nature makes it simpler but does not remove the diligence and necessary budget to be spent on the verification of the supply-chain's security.

PRODUCTION PLAYS A CRUCIAL ROLE IN THE SECURITY CHAIN.

WHAT & WHY

Besides classic OT security threats, the switch from R&D to production is critical for the product security. It is the final stage of the development to address risks and to lock down the product before it is released to clients. It is also the moment when individual cryptographic secrets are integrated into each vehicle; hence production is an important element in the security chain.

MAJOR CHALLENGES

In mass production, the pressure for delivery is extreme. With multiple parts coming from different providers, it is complex to integrate individual keys or certificates for each product and to ensure closing open interfaces. Moreover, the industrial environment is a tricky one to keep secrets; older technologies, many employees involved, etc.

OUR CONVICTION

The Production phase will face a major change in the next years with the increase of the software part inside the vehicles and the associated crypto-graphic secrets to be deployed to guarantee the security. The production capabilities must be considered during the security-by-design phase. Also, the security topic shall not be underestimated when considering the upgrade cycle of factories and production equipments (Industry 4.0).

HOW TO GO FROM THEORY TO PRACTICE?

PRODUCTION

P1

CRYPTOGRAPHY INTEGRATION IN VEHICLES

Encryption and authentication rely on cryptographic materials, like private keys and certificates. These secrets are integrated into the vehicles during the production phase and should follow a very meticulous process to ensure that it is not leaked during the operation. It is also crucial to keep track at all times of what cryptographic material is present in which product.

P2

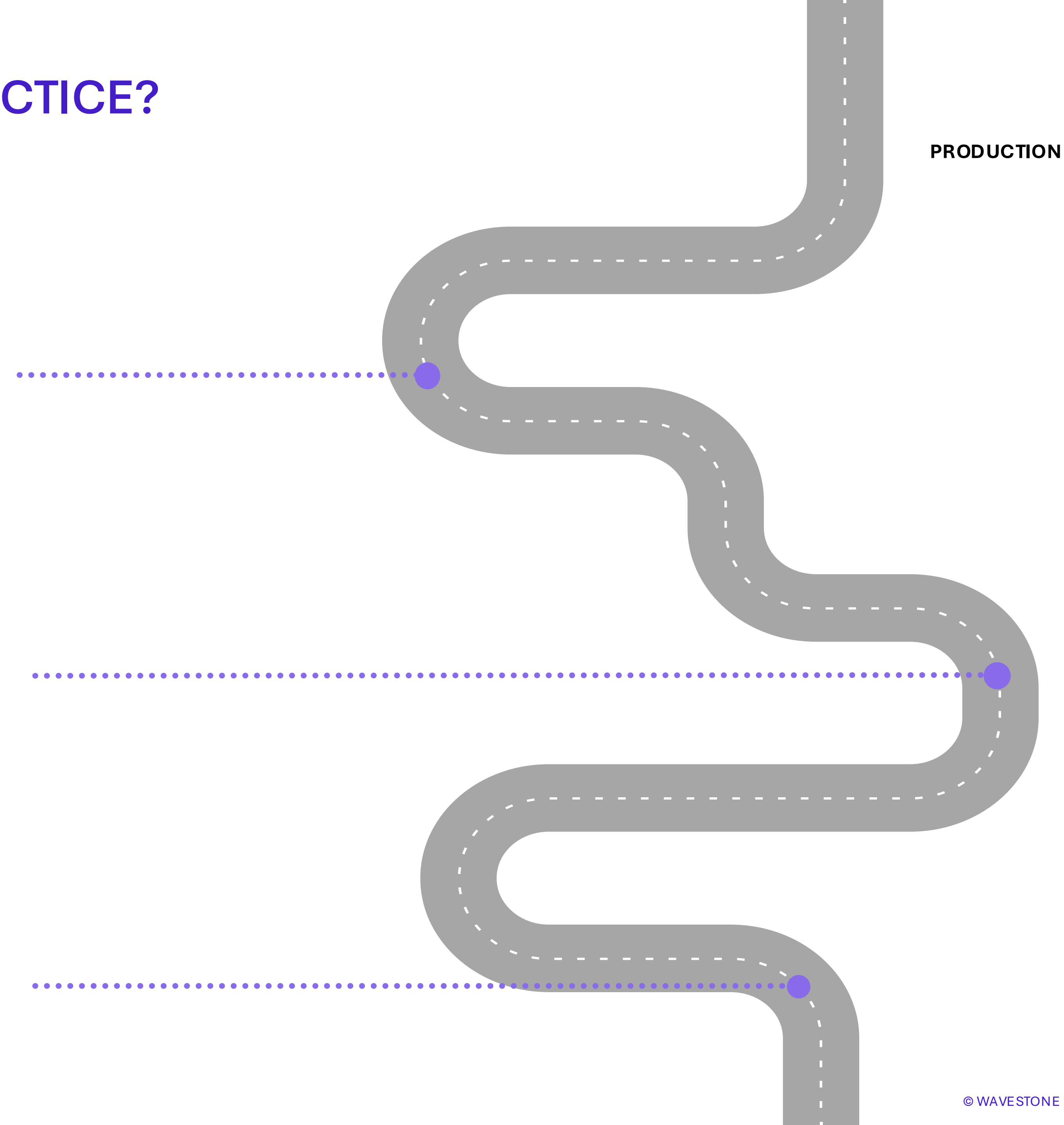
INTEGRITY & SECURITY CHECK

Multiple actors took part in the R&D phase and, for functional or testing reasons, some security mechanisms may have been bypassed e.g. hardware debuggers. It is essential to conduct several checks, for instance: authenticity of the flashed software, security measures in place, access to unnecessary interfaces disabled, etc.

P3

OT SECURITY

The factories are vulnerable environments. Because of the expensive investments in machines and high availability requirements, systems are older than in the classic IT world and rarely updated.
The interruption of these production systems can have severe financial consequences. Also, if compromised, the systems can jeopardize the safety and the security of the assembled vehicles.



HOW TO GO FROM THEORY TO PRACTICE?

PRODUCTION

HOW WE CAN SUPPORT YOU?

We support your teams in the transition from product development to production phase (e.g. injection of cryptographic materials, security measures implementation before series, etc.). We can also help to secure your OT world, from risk analysis to technical and organizational concepts to increase your protection level during this critical step.

P1

CRYPTOGRAPHY INTEGRATI

Encryption and authentication re
like private keys and certificates.
the vehicles during the productio
meticulous process to ensure th
operation. It is also crucial to kee
cryptographic material is presen

P2

INTEGRITY & SECURITY CHE

Multiple actors took part in the R
testing reasons, some security m
e.g. hardware debuggers. It is ess
for instance: authenticity of the f
in place, access to unneces- sar

P3

OT SECURITY

The factories are vulnerable environments. Because of the expensive investments in machines and high availability requirements, systems are older than in the classic IT world and rarely updated.

The interruption of these production systems can have severe financial consequences. Also, if compromised, the systems can jeopardize the safety and the security of the assembled vehicles.

SECURITY MUST BE CONSIDERED ON THE ROAD.

ON THE ROAD

WHAT & WHY

Vehicles are increasingly defined by software - amplified by connected and "partly-automated" driving functions. In this context, Security can only be maintained if software and security measures can be upgraded. Additionally, and despite all measures, incidents will happen. OEMs must prepare to react accordingly - while cars are running on the streets.

MAJOR CHALLENGES

The quick addition of software features in released products will increase the vulnerabilities; dealing with them while the cars are in the field - sometimes offline - is a real challenge. This trend will be amplified by over-the-air updates - a Software Update Management System (SUMS) will have to be set up. In order to manage this post-production phase, it requires operational security teams with associated processes and incident/crisis management capabilities. This is expensive and demands a lot of resources and competencies.

OUR CONVICTION

Automotive world has been for long focused on development phases, to implement safety, and now security. However, the operational part, post-production, remains a dead-angle of the security concept. OEMs shall take the complete end-to-end security chain, from development to decommission, to ensure security and safety into consideration. These operational costs for continuous update and monitoring may even result in a service-oriented business model!.

UP-TO-DATE AND SECURE.

OTR1

SW DEPLOYMENT & MAINTENANCE

Software in automotive is today mainly developed and deployed in a static way, during the production phase. But the emergence of software-defined - and connected - vehicles demands continuous code improvement. Processes for software updates must be deployed alongside specific tools, also when vehicles are offline for long periods. New systems - such as the "Digital Twins" model - can improve the security and reliability of the software deployment.

OTR2

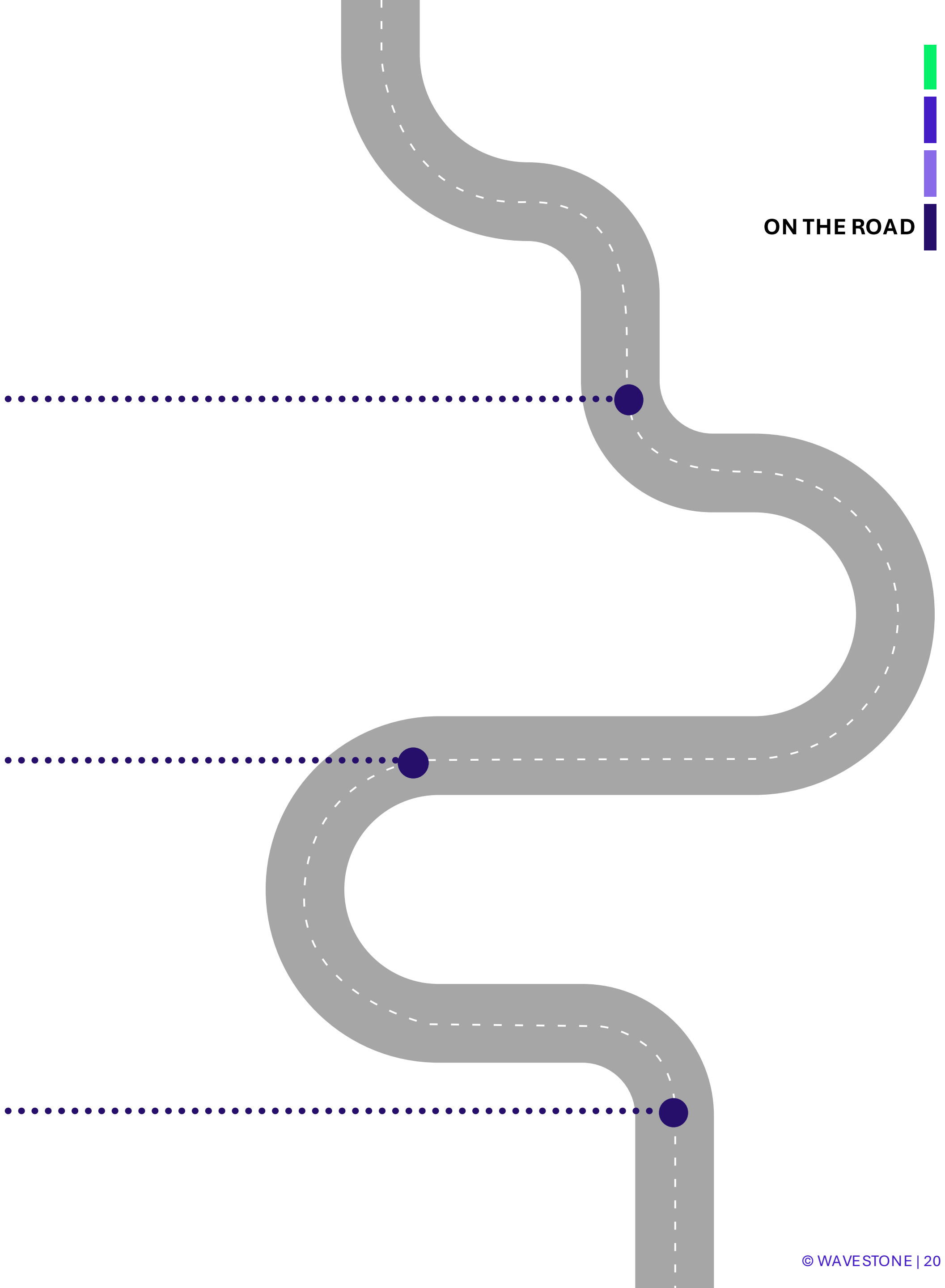
CONTINUOUS HOMOLOGATION & CERTIFICATION

When released, software must be certified to ensure Security and Safety. With continuous software deployment, the homologation procedure needs to be adapted both to assess impacts on security and to deliver new certifications for software in a more agile way. To this purpose, new platforms must be developed together with the certification authorities in order to automate the process - for instance using simulation models and "Digital Twins" models.

OTR3

SW DOCUMENTATION & VERSIONING (RXSWIN)

To provide artefacts and documentation for compatibility and homologation checks, before an update release, is critical. As much critical is keeping track of the newly deployed software in the vehicles fleets. The regulation UN R156 also requires to assign a Software Identification number (RXSWIN). For these three examples, a Software Update Management System must be implemented; it will play a key role to deploy new features and security updates.



UP-TO-DATE AND SECURE.

HOW WE CAN SUPPORT YOU?

We support the implementation of your Software Update Management System (SUMS) and the required tooling and concepts for software deployment across your fleet of vehicles.

We enhance your homologation process to shorten the time-to-market and to improve your agility at deploying new features and security updates.

OTR1

SW DEPLOYMENT & MAINT

Software in automotive is today m
production phase. But the emerge
continuous code improvement. P
specific tools, also when vehicles
Twins" model - can improve the se

OTR2

CONTINUOUS HOMOLOGA

When released, software must be
software deployment, the homol
impacts on security and to delive
purpose, new platforms must be
to automate the process - for inst

OTR3

SW DOCUMENTATION & VE

To provide artefacts and documentation for compatibility and homologation checks, before an update release, is critical. As much critical is keeping track of the newly deployed software in the vehicles fleets. The regulation UN R156 also requires to assign a Software Identification number (RXSWIN). For these three examples, a Software Update Management System must be implemented; it will play a key role to deploy new features and security updates.

BE PREPARED: WHAT HAPPENS IF EVERYTHING GOES WRONG?

OTR4

CYBER INCIDENT DETECTION & RESPONSE, THREAT INTELLIGENCE

OEMs and suppliers must develop strategies and technics to detect and respond to near real-time Cyber Security incidents, whether it is for regulation reasons (WP.29 UN R155) or for anticipating security breaches in their vehicles. Monitoring and attack prevention shall occur onboard and offboard and can be passive or active with the support of threat intelligence services. This is the only way to know if the vehicle (or a complete fleet!) is under attack and collect evidences about your actual level of protection.

OTR5

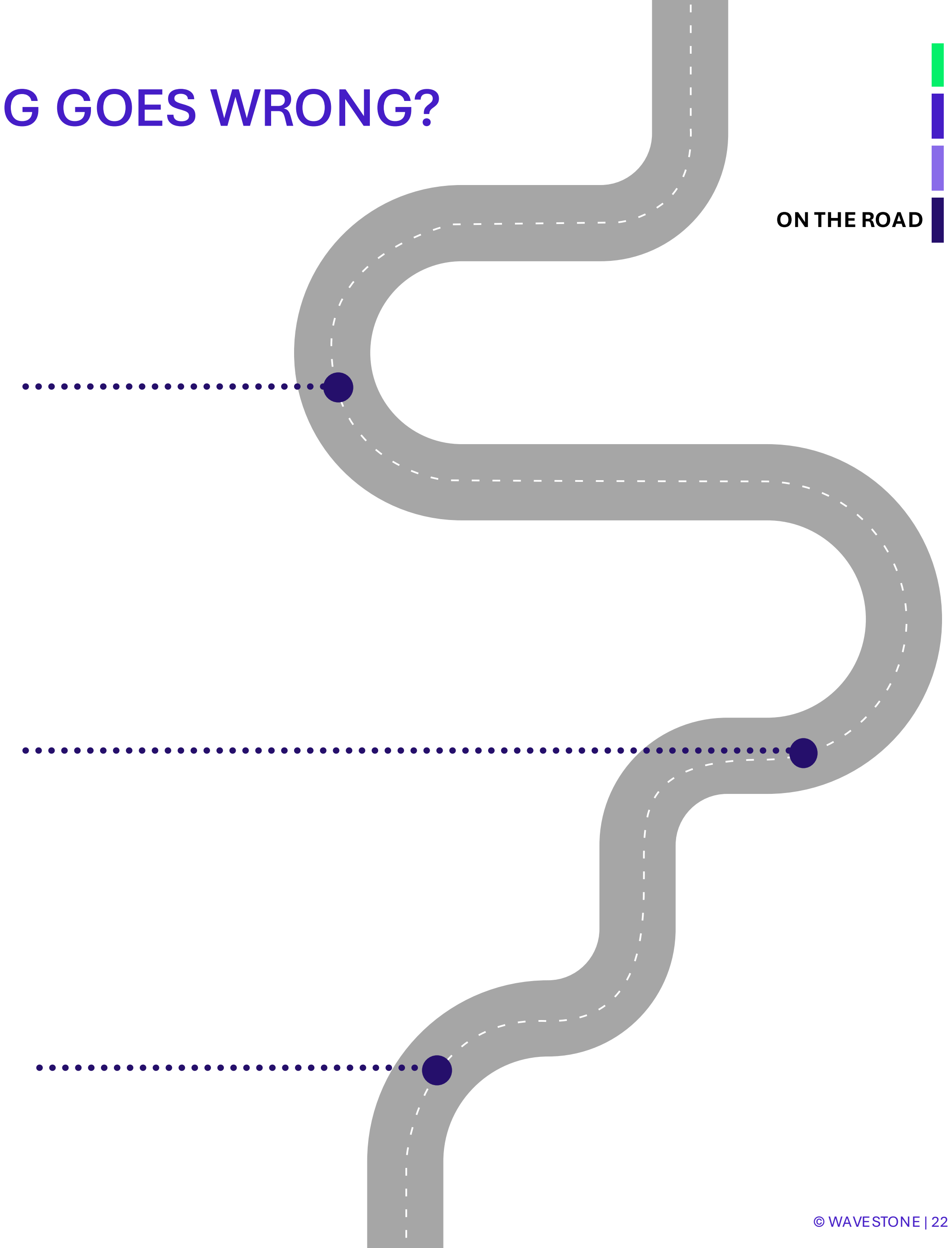
CYBER CRISIS MANAGEMENT & RESILIENCY

If it is not if, but when. One day, an incident will have a severe impact on one or a fleet of your vehicles and a crisis. will happen. A crisis management cannot be improvised; it requires a lot of preparation and training, and dealing with potentially life-threatening objects running in the streets is something new. You need to define playbooks, roles and responsibilities, and to train people in your company to react very fast. Also, by preparing such crisis scenarios, you can improve your resiliency - that is to say the possibility to operate in a limited, but safe mode, and to recover from this situation.

OTR6

ON THE ROAD VULNERABILITY MONITORING & PATCH MANAGEMENT

Tracking vulnerabilities in released products is an art; security issues must be fixed without disrupting the functions. While it is already a challenge in the IT domain, the automotive world must implement a similar process and maintain the security within vehicles for years, sometimes even decades, depending on the vehicle security lifecycle concept.



BE PREPARED: WHAT HAPPENS IF EVERYTHING GOES WRONG?

OTR4

CYBER INCIDENT DETECTIO

OEMs and suppliers must develop st
Security incidents, whether it is for reg
breaches in their vehicles. Monitoring
be passive or active with the support o
vehicle (or a complete fleet!) is under a

OTR5

CYBER CRISIS MANAGEME

If it is not if, but when. One day, ar
vehicles and a crisis. will happen.
of preparation and training, and d
streets is something new. You nee
people in your company to react v
improve your resiliency - that is to
and to recover from this situation

OTR6

ON THE ROAD VULNERABIL

Tracking vulnerabilities in released products is an art; security issues must be fixed without disrupting the functions. While it is already a challenge in the IT domain, the automotive world must implement a similar process and maintain the security within vehicles for years, sometimes even decades, depen- ding on the vehicle security lifecycle concept.

HOW WE CAN SUPPORT YOU?

We support your SOC Team with the design of incident detection & responses processes, and by evaluating the tooling and assisting its implementation (probes, SIEM, SOAR, etc.). We stand by your side to prepare crisis scenarios with playbooks definition and associated trainings. We help you developing a vulnerability management program for your offboard and onboard systems.

WAVESTONE