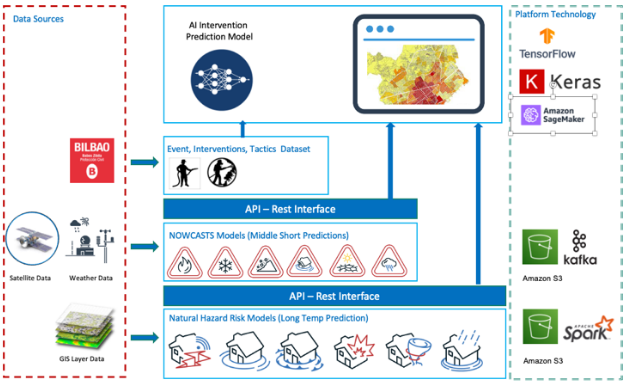
Technical Specification Double-side Page

1. **TECHNICAL SCOPE:** Summarize the mock-up devised during the EXPLORE phase: how have you addressed the challenge/Theme Challenges and tackled with its requirements and data. Include a diagram.

CySytellar will solve the Bilbao City Council challenge to predict the probability of an increase or decrease in the different types of emergency situations in a 15-day time frame, with the aim of providing support to managers when sizing emergency teams. Using insurance actuarial AI prediction models, the solution provides a geospatial Biscay Province Hazard Index (the solution could be easily extended to the whole country of Spain). The Risk Index leverages source data for natural hazard and community risk factors to develop a baseline relative risk measurement for each census tract of the considered province.



The Risk is defined as the potential for negative impact (leading to firefighter department interventions) as a result of hazards. The initial natural hazards that we have included into the Biscay Hazard Index are: earthquake, riverine flooding, coastal flooding, flash flood, high wind, hail, snowfall, cold waves, lightning, wildfire and landslide. This data originates from the insurance actuarial models developed by CyStellar and using various EU data sources in addition to the weather data provided by the City of Bilbao.

The risk estimation solution three components: a natural hazards component (Expected Annual Loss), a consequence enhancing component (Vulnerability), and a consequence reduction component (Community Resilience). Vulnerability is the susceptibility of social groups to the adverse impacts of natural hazards, including disproportionate death, injury, loss, or disruption of livelihood. Hazard Index correlates well with expected damages (as measured by insurance claims) and potential civil protection unit interventions. Short term predictions in the range of a 15-days' time frame will also use the near real-time satellite and weather data. We will provide the City of Bilbao with a complete geospatial platform deployed on the cloud for continuously monitoring risks probabilities.

2. **ALGORITHMS, TOOLS AND CONCLUSIONS:** Detail the algorithms and tools identified to accomplish the challenge/Theme Challenges. Show clear understanding of the used REACH dataset/s and addressed challenge/Theme Challenges.

The AI models will be developed in Python, using Keras and Geospatial Data Abstraction Library GDAL library when necessary, running on top of Tensorflow, and trained and deployed on an Amazon Sagemaker infrastructure. For the production deployment, we will use Amazon Elastic Kubernetes Service (Amazon EKS) a managed container service to run and scale Kubernetes applications in the cloud to preserve the privacy, security, and trust requirements of the proposed data solution.

The results will be accessible to the Data Challenge provider through a cloud-based geospatial intelligence platform deployed using Node.js and React technology. The Platform will provide secure user management and authentication module for the protection of project and user data. If requested, the results can be also made available through API so that the platform can be interfaced with existing strategic planning and scheduling tools available at the hosting organization. During the project, we would test Proregister and the Audit Messages Storage Tool from the tools available at the REACH Toolbox for storing application system health logs in a secure an immutable way.

3. **SCALABILITY AND FLEXIBILITY OF THE SOLUTION:** Discuss whether the solution can truly cope with humongous and increasing datasets and how flexible it is to adapt to other related domains

The CyStellar platform is a multi-tier and multi-tenant SaaS architecture which allows us to on-board multiple partners and customers (multi-tenancy) on the same server infrastructure and resell or assign them licenses of different types (multi-tier). This allows a high utilization of available system resources, simplify SaaS solution's provisioning, management and update experience, and helps us maintain cost-effective operations for our customers. It also fits well with our continuous delivery and agile software development process. The challenge solution will be integrated into our platform as a microservice and will seamlessly integrate and access data from other modules through API connections. Weather data acquisition modules and satellite image acquisition and processing pipeline is already part of our platform.

This project has received funding from the European Union's Horizon 2020 research and innovation programme under grant agreement No 951981

To support dynamically increasing demands from multi-tenants, load balancing mechanisms are also implemented.

4. **DATA GOVERNANCE AND LEGAL COMPLIANCE:** Describe the security level of the proposed solution, i.e. how authentication, authorization policies, encryption or other approaches are used to keep data secure. Explain how will be compliant with the current data legislations concerning security and privacy (e.g. GDPR).

GDPR is an integral part of the technological development at CyStellar and our Data Protection Policy comply with the Privacy Principles by Design and by Default (Article 25 of the EU GDPR). CyStellar ensures that privacy is built into our system during the whole life cycle of the system and processes (including internal projects, product development, software development, IT systems, business activities). Once CyStellar's product or services are released to the public, the strictest privacy settings apply by default, without any manual input from the end user (Privacy by Default). In addition, any personal data provided by the user to enable a product's optimal use are only kept for time necessary to provide the product or service.

CyStellar has an appointed Data Protection Officer. Additional information is available in "CyStellar Privacy Policy and Data Retention Policy (GDPR)" document available upon request as part of data protection audit process. CyStellar also guarantee to its business partners to undergo assessment and audit to verify the compliance with GDPR Regulations if requested. We use pseudonymisation and anonymisation procedures of personal data in compliance with GDPR regulation when working with personal data. Our data encryption solution(s) meet current standards such as FIPS 140-2 and FIPS 197. Third-party data centres used in for this project will be deployed in EU Region (Stockholm, Ireland, Frankfurt).

5. **QUALITY ASSURANCE AND RISK MANAGEMENT:** Describe the quality process planed for the final product. Technologically, which are the potential risks in all the phases of the project (design of the solution, development, testing, deployment…) and indicate mitigation plans to still fulfil the challenge/Theme Challenges and data provider requirements.

Quality Assurance: As an InsurTech company, CyStellar follows ISO 9001, ISO/IEC 27017 and CMM (Capability Maturity Model) criteria for quality management to ensure that we meet our customers' needs within statutory and regulatory requirements related to a product or service. Our software development process follows an agile framework (SCRUM methodology) with two weekly development sprints, sprint review and continuous deployment to the customer. CyStellar has also adopted a SSDLC (Secure software development life cycle) development processes integrated with Snyk for securing code, dependencies, containers, and infrastructure as code.

CyStellar, as part of the product deployment infrastructure, already has a customer support online ticketing system that is deployed with the software for each customer. Support tickets and queries are automatically routed to the right support engineer and prioritized accordingly. For high value customers, CyStellar appoints a Key Account Manager who constantly monitors the performance, usage and customer satisfaction of the deployed platform.

Risk management: During the Exploration phase, CyStellar has performed a project risk assessment along 4 categories of risks: Management, Technical, Commercial and Financial. The Project Governance Documents (Project Plan and Risk Register) are continuously updated and reviewed fortnightly during the duration of the project. Sample extract from the project Risk Register highlighting a few technical risks:

Risk (Technical)	*Impact*	*Likelihood*	*Mitigation plan*
Data that needs to be collected is massive and diverse, there is a risk that analysis would be expensive and difficult.	High implementation costs	High	Reuse existing data collection modules from the CyStellar platform. Integrate solution as a microservice into the multi-tier SasS architecture
The solution needs to use data from and output data to the customer's platform there is a risk that the data is not easily accessible via standard communication interfaces.	Lower platform usability	Medium	Work together with the challenge provider (customer) in devising the communication interfaces between the customer's platform/data and CyStellar's platform
Issues with scalability, the processing speed and capacity of the platform to accommodate meta data and AI	Lower platform performance and functionality	Medium	We will mitigate this through development of the technology stack, enabling the platform to only access the required services when required. Furthermore, cloud-based servers will allow the platform to scale up processing power when necessary to. The risk will be considered as an element of the exploitation plan.
Misinterpretation leads to technical errors	Lower platform reliability and delivery delays	Low	Agile development means that issues will be found quickly and rectified. Biweekly project progress meetings and online space for documents will ensure technical information is clear/accessible.

This project has received funding from the European Union's Horizon 2020 research and innovation programme under grant agreement No 951981