Local authorities facing flood related networks failures in France

Violette Gallet[1,a], Nicolas Bauduceau[1]

[1] *European center for floodrisk prevention (CEPRI), BP 2019, 45010 Orléans cedex 1, France*

Abstract. Network critical infrastructures have become vital to keep our societies running in every-day situations, but also during crisis and recovery. Involving many stakeholders at different scales, they form a complex system that can be easily disturbed by internal or external events, because then all the dependencies that allow to optimizing their working become flaws that help failures to spread beyond the flooded area and from one network to another. Thus every flood reminds us how vulnerable infrastructures are and how much it costs when they fail. But whereas it isn't so difficult to adapt new urban development, what about all the existing and exposed infrastructures? CEPRI carried out research on encountered difficulties and good practices to understand the situation and consider improvement opportunities. We worked out three steps to a better territory resilience to flood. First, get a better knowledge of networks. Then, as far as possible, reduce networks vulnerability. Finally, as risks of network failures always remain, get prepared to cope with disruptions! CEPRI gathered many experiences to illustrate and strengthen its work, which aims at helping local authorities to reduce their vulnerability to flood and related networks failures.

1 About studying networks and floods

Technical networks have become vital to keep our societies running in every-day situations but also during crisis and recovery. Facing the fact that networks failures resulting from floods can generate major disruptions in the crisis management and in the recovery phase, CEPRI decided to study this subject. It also followed a work concerning business continuity [1], of which the issue on networks appeared to be a logical continuation.

To do so, we read a lot about experiences and strategies of French or foreign places: OCDE study on Ile-de-France [2], studies on the Rhône [3] and Loire [4] rivers, Prague [5], New York [6-8], United Kingom [9-11]… We also interviewed many stakeholders to gather different points of view. We talked to national operators: Orange (telephony), ERDF (electricity distribution), GRDF (gas distribution); local operators: RATP (public transports in Paris and surroundings), CPCU (district heating in Paris). We also interviewed French cities and local authorities whether as users or operators of networks: city of Saintes, city of Nantes metropolitan district council, city of Orléans district council, city of Paris, city of Lyon, city of Gennevilliers, city of Blois district council, department and prefecture of Val-de-Marne.

All this information allowed us to have a global point of view of the situation in France, with some ideas coming from other countries. Thus we could emphasize obstacles and levers and then determine keys and strategies to go forward less vulnerable networks facing floods.

[a] Corresponding author: violette.gallet@cepri.net

2 Territories facing networks failures

2.1 A danger for human life

2.1.1 When networks fail during a flood

Many lives depend on the proper functioning of networks: electricity for people that need a machine to breath (in hospitals or at home), water for dialysis, roads to be easy to reach by ambulances… As vital networks collapse, these people are endangered, but this is on the whole a huge loss of comfort for everyone.

Without tap water, hygiene issues increase and local authorities need to settle an organization to give out water by alternative ways. The foul water network is often forgotten but is in fact a worsening factor during a flood: foul waters flowing back from sewers in homes, public places or in the street result in insalubrious areas that need to be evacuated.

As the water level rises, some roads become impassable. Then houses, public places or even whole towns can become islands and thus are difficult to reach for emergency support, for food or medicine supply…

Finally, the loss of telecommunication utilities prevents people from calling for help or to give some news to reassure their family. That can be a factor of anxiety.

2.1.2 When networks keep working during a flood

Actually during a flood the danger can also come from networks that weren't stopped in time. As water reaches a distribution board, transformer or any other electrical device, people around it can be electrocuted. It can also generate fire issues.

District heating systems can also become dangerous during a flood. Even if they are insulated, pipes that dispatch very hot flows are very hot themselves and they can explode as cold flood water reaches them.

Low pressure gas pipes are also vulnerable to the pressure of the water. There can be leaks as these pipes are submerged. Like any other gas leak, this could be an emergency situation.

2.2 Disastrous results on the economy

2.2.1 From a material point of view

The deterioration of networks infrastructure is a loss for the stakeholder that invested to build them and spent money to operate and maintain them. Furthermore, if infrastructures are damaged, they need to be repaired or replaced, which can be costly.

2.2.2 From an operating point of view

Most businesses depend on networks to run properly. If the flood disrupts the proper functioning of networks, those businesses and industries may encounter difficulties to keep running normally, and they may even have to stop their activity.

Disruption can issue from a direct impact of networks on the activity: no industrial process without electricity, gas or water, no exportation without cleared roads, no clients orders without telecommunications…

But one shouldn't underestimate the impact of a flood on the staff. Whether their house is submerged or their way to work is impassable (submerged road, public transport unavailable…), businesses often meet workforce issues during a flood. [12]

2.2.3 An obstacle for the society

Networks failures take part to the weakening of the society that ensues from a flood. Businesses show heavy losses, people lose their job, their house, and nothing will get better as long as networks don't run properly: need of water to clean up buildings and roads, need of electricity to dry buildings and to get every machine back to work…

2.3 Consequences for the environment

When sewers flow back foul water or when a sewage treatment plant is out of use, all the foul water goes into earth, rivers, ground water. This can be a significant source of pollution.

Networks infrastructures include treatment plants or transformation sites that use chemicals or that keep materials in stock. These are potential sources of waste and pollution if the water reaches them.

The destruction of networks infrastructures finally generates waste and appeal to new resources in order to rebuild them.

2.4 Impacts on the common heritage

Some network infrastructures may be registered as part of the common technical or architectural heritage. They also represent a large investment, and are part of common utilities.

Moreover, let's not forget that without electricity or water, fire safety systems or burglar alarms can't work properly, which weakens any common heritage building or site.

2.5 Propagation and series of effects

Disorders in a network's infrastructure equipment can generate failures in other installations of this network or in another network's installation. There are different ways a malfunctioning can spread. It depends on the relationships between networks.

Some of them are linked by a geographical dependence, which means that they are close from one another, in such a way that the disruption of one may affect the other. For example, shall a road be ripped off by the water; it could also cut wires that run under it.

Other networks are linked by a functional dependence. It means that one of them brings part of the resources the other needs to work properly. For example, the drinking water distribution system needs electricity to work.

Some of these dependences are reciprocal, they are called interdependences.

Thus, during a flood, the failure of one network's installation can generate disorders across the entire network, but also in all the networks which depend on it, and so on. As a result, networks can be cut off, even away from the flooded area, which worsens even more the crisis generated by the flood. It can be difficult to foresee this or to explain it to the concerned users.

3 Networks facing floods

3.1 About networks

3.1.1 Several types of network infrastructure

Many networks give structure to urban areas and lands. CEPRI studied some of them concerning energy (electricity, gas, hydrocarbon, district heating), water and waste (drinking water, wastewater, waste), transportation (roads, urban public transport), and telecommunications (landline and mobile telephony).

Depending on their goal and on their nature, networks are not structured the same way. Some of them aim at distributing a resource (electricity, gas…) and have an arborescent structure, whereas others collect the resource

(wastewater, waste): they have an inverted arborescent structure. Finally, there are networks where any installation is both a receiver and an emitter (roads, telephony…). They may be called woven networks. The structure of the network influences its vulnerability to dysfunction (that can be generated by floods).

3.1.2 Comprehending this complex system

All these networks constitute a complex system that can be difficult to comprehend. Thus it is possible to order them, depending on: how many networks they depend on, how many networks they influence and how critical they are to keep the society running. Roads, electricity and telecommunication networks are usually designated as the most critical infrastructures for society functioning, crisis management and recovery.

Ordering networks helps ordering actions that need to be organised to reduce the vulnerability of networks infrastructures to floods.

It is important to notice that the criticality of a network or of one of its installation depends on the scale that is used (something important for a local authority may not have priority from a national point of view). The criticality of an installation may also be influenced by the equipment it supplies (hospital, crisis management centre, shelter area…).

3.2 Vulnerability factors

3.2.1 A long story between floodable areas and networks

Networks infrastructures have naturally been developed along areas which are at risk of flooding (river, coast, valley, plains…). They are indeed suitable places for such infrastructures: flat, sometimes straight, offering an access to fluvial or maritime transportation. Moreover, urbanized areas, which are generally in these places, appeal infrastructures and vice versa. Network infrastructures appeal each other too, especially roads, as they allow the access to other networks infrastructures. Finally, some networks infrastructures need, for technical or logistical reasons, to be near from rivers or from the coast (wastewater treatment plants for example).

3.2.2Internal vulnerability factors

Many factors can weaken a network. First of all, there are inherent factors. The lack of resistance to the water element or to the pressure and strength of water means that some parts of the network can fail or can be destroyed if they are submerged. A low ability to stand and absorb dysfunction (shall it be internal or external) prevents the network to adapt and keep running in case of a disruption. An insufficient capability of recovery extends the period before the network can run properly again. All of this results in larger damages, more disruption to the crisis management, a longer period for everyone's recovery and heavier financial losses.

3.2.3 External vulnerability factors

But networks also depend on external resources: services provided by other networks, chemicals or materials provided by suppliers, subcontractors… Shall any of those resources fail; it could be an issue for the network. However, many network managers, as they plan their organisation in case of a flood, do as if all those resources will keep running properly. But they should, on the contrary, plan their flood crisis management with this hypothesis: zero external resource, which is much closer from reality.

4 Everything should be ok, say the laws?

4.1 European critical infrastructures

Council Directive 2008/114/EC of 8 December 2008 [13] relates to the identification and designation of European critical infrastructures and the assessment of the need to improve their protection. It is part of a project supported by the European Programme for Critical Infrastructures Protection (EPCIP), which mostly deals with the risk of terrorism, but also addresses the risk of flooding. So far, the directive is about energy and transportation networks infrastructures, but information and communication networks may be next.

The directive gives criterions in order to identify European critical infrastructures (ECI). Whatever the network is, there are 3 factors: the potential number of casualties (fatalities or injuries); the economic effects (significance of economic loss and/or degradation of products or services) and potential environmental effects; and public effects (loss of confidence, physical suffering, disruption of daily life, and loss of essential services). Then there are specific criterions for each type of infrastructure.

Each Member State is responsible for the appliance of ECI managers to the Directive. One of the obligations of the operators is to elaborate an 'operator security plan' (OSP). Its minimal content is detailed in the Directive.

4.2 Some examples from EU members

4.2.1 Germany

Since 2009 Germany has its own national strategy to protect national critical infrastructures (CI). A guide goes along with this strategy to give resistance and resilience solutions for critical infrastructures to face floods.

The chosen criterions to identify those CI are the following: consequences of the disruption on human life and health; period between the disruption and the outbreak of its consequences on the service; the extent of these consequences on the production or on the service; contractual, penal and judicial impacts for the operator; and economic consequences for the operator.

4.2.2 United Kingdom

In United Kingdom, critical infrastructures are part of the national infrastructures. They are listed and classified into 6 categories of criticality (CAT0 to CAT5). Each infrastructure is assessed according to defined criterions and thus is given a score. If this score leads the infrastructure into CAT3, CAT4 or CA5, then it is considered as a critical national infrastructure.

The classification considers: the significance of the services supplied by the infrastructure; the impacts of its disruption on the economy and on human life; the level of degradation of the service supplied by the infrastructure; the duration and the extent (area and population) of the disruption. [14]

4.2.3 France

In France network infrastructures are considered as supplying a public utility. Thus, they have to respect a principle of continuity of functioning and a principle of satisfaction of the primary needs of the population.

The strategic installations of critical networks are identified as 'installations of vital significance'. This status gives them a more constraining frame to manage their functioning, including regular reporting to authorities. If a disruption occurs to their sources of supply (electricity, hydrocarbon, water, chemicals…), then they will have priority to be supplied first.

4.3 The limits of the law

Looking at the legislation, all the critical networks should be resilient or at least they should be on the right path leading to less vulnerability. But this is clearly not the case. Admittedly, a significant work has been accomplished concerning strategic installation and critical, large scale networks. However, concerning local networks and infrastructures, the situation is very different from one area to another, from one type of network to another.

One major obstacle to the reduction of vulnerability is that networks predominantly exist, since new projects or deep renewals are done very gradually. Yet it is very costly to modify or to adapt existing infrastructure, especially for floods.

So we have to face the fact that most networks infrastructures will remain the way they are until they are flooded, heavily maintained, or updated. Of course this concerns structural adaptations. It doesn't prevent operators to plan crisis management with those vulnerable installations.

5 Some keys to struggle with networks vulnerability

5.1 Three steps for a better project structure

As local authorities start a process to reduce the vulnerability of their land to floods and related networks failures, they don't have the same background. In France, some of them are operators themselves, others have already begun to work in collaboration with operators… Depending on the situation, the local authority won't look for the same information, nor will proceed the same way. Thus we brought out three types of situation. A local authority can face the three of them at the same time on three different networks.

5.1.1 For a better knowledge of networks vulnerability

First, there are local authorities that start (almost) from scratch. It means that they don't know how the networks they depend on will work if a flood occurs. In that case, the local authority needs to gather information about the flood hazard and to share it with the operators. The purpose is that every stakeholder has the same knowledge of the hazard. Then it is up to the operators to assess the physical and functional consequences of the hazard on its network. Once this is done, the local authority that leads the process, gathers the information provided by operators and share them with all the stakeholders. Thus they all know what the others will endure in case of a flood, and what they plan to do to protect their infrastructures. This sharing aims at identifying cascading effects, which enables operators to adjust their assessment of the disruptions they may face in case of a flood. After this shared diagnosis, each stakeholder should have a better knowledge of the hazard, the direct impacts it may cause on infrastructures and the disruptions that may come from other networks they depend on.

That is methodology. Once again, the reality can be quite different. In this case, it is actually uneasy to get data from operators for several reasons: confidentiality (for commercial or security reasons), competition, or a lack of knowledge about the flood risk. Hence the leader of the process has to find a consensual strategy so that it is possible to improve the knowledge concerning networks vulnerability, without putting operators in a difficult position. It is also generally useful (at least in France) for the leading local authority to have the support of a recognized and strong authority.

5.1.2 Reducing networks vulnerability

As the local authority is aware of the vulnerability of the networks that supply its territory, it will logically try and mobilize operators to reduce this vulnerability, but how? It appears that there are several technical and organisational ways to reduce the vulnerability of networks [15].

As far as infrastructures are concerned, one solution is to avoid water, whether by settling installations out of flood prone areas or by raising their height (or the height of their sensitive components). Then, for the infrastructures that are still exposed to flood, sometimes it is possible to reinforce them, so that they are less damaged by the influence of water (Archimedes thrust, strength of the stream…), or to improve their watertight.

Finally, whether the previous solutions are applied or not, it is generally useful to weave the infrastructures. That means to create or to multiply installations or connexions between them. It aims at increasing possibilities for the resource (or service) to reach its users. However a woven network may be prone to an easier propagation of disruptions. This is why it is important in that case to also keep a possibility to divide it, in order to contain the spread.

Telling the truth, it is very expensive and sometimes technically difficult to apply those solutions on existing networks. Thus those solutions will generally be applied on new infrastructures or on existing ones that need heavy repairing.

5.1.3 Putting up with networks failures

In many situations it is not possible to reduce the vulnerability of a network, at least not within short or medium term. Thus operators, local authorities and users have to find solutions to be able to face networks disruptions during a flood (or any other event).

For example, limiting the use of the network can be enough to enable it to keep working. This limitation can come from the network (e.g. diversion) or it can come from users (instructions given by authorities). But then the question is whether to cut everyone for a few priority users, or to keep a damaged service for every user. Sometimes however the technical context doesn't give any choice. In some cases, it is possible to use mobile components (pump, treatment unit, generator…) to maintain the functioning of the network.

When the network is completely out of order, the user has to find another way to get the resource or the service expected from it. Sometimes the alternative is offered by the operator (e.g. distribution of bottles of water if tap water isn't available). Sometimes it's up to the user to take precautions. The alternatives used by the 'user' can be permanent or temporary, depending notably on the quality of service they bring. Taking the reasoning to extremes, one last solution for the user can be to refrain from using the resource brought by the network temporarily (candle instead of lamp) or permanently (mechanical systems instead of electronical ones).

Finally, operators should never underestimate the importance of flood related networks failures on staff. Indeed, some employees may not be able to come to work because their way of transportation is unavailable (flooded roads, public transport out of order…). This is a quantitative and qualitative matter. If the operating area of a network is divided by the flood, the operator should check that the right skills are in the right place. For example, the department in charge of waste management for the district of Orléans (France) made sure that its employees were evenly dispatched on both banks of the river Loire. Indeed, in case of a major flood, it will be impossible to cross the river and the waste management department will have to split into two entities with equal abilities. [16]

5.2 A global strategy

5.2.1 A two-tier strategy

Let's face it, there is no way operators are going to reduce the vulnerability of their network just for the sake of floods. The main reason is that it would be indecently costly and technically difficult, since it would require huge works to replace and adapt a large part of existing installations. Moreover, some installations are so old that they use technologies that are no longer available, thus their replacement needs a complete work from design to fabrication, so it can take a lot of time.

Local authorities have to accept that the reduction of networks vulnerability will take time, because it will be done gradually. Being realistic, there are only few specific situations when the operator does work to adapt an existing network (apart from gradual renewal or heavy maintenance): after some installations have been damaged by a flood; if an infrastructure is regularly disrupted by floods; or if the failure or the damaging of an installation would have disastrous consequences for the society or the operator (e.g. tens of thousands of people affected, or years of works to recover). Of course if the local authority is ready to pay, things can go faster, but the trend doesn't really go this way.

As operators and local authorities are thinking about long term, coordinated solutions to reduce the vulnerability of the territory and of its networks, short term and easy solutions must be found to wait until they are operational. These short term solutions may be temporary or reversible. They are meant to put up with flood related networks failures that may occur while the operator is gradually adapting installations.

5.2.2 Seizing opportunities and finding synergies

As it is very long and costly to reduce the vulnerability of networks, every opportunity must be seized, even if the first purpose of the operation isn't the flood hazard. Similarly, adaptations allowing to reduce the vulnerability of a network may become more attractive if they have other advantages. For example, improving the watertight of drinking water pipes reduces the vulnerability of the water supply network, because it lowers the risk that polluted flood water enters the pipes. But it is also very interesting because it spares the resource by reducing leaks (which spoil many litres of water each year). So it is a better yield, an improved quality of water, a good picture of the operator and saved money for everyone. Another interesting example is the one of the city of Saintes (France), which bought metallic gangways to enable people to keep walking through the city even during frequent floods. As the floods occur only during late autumn and winter, the gardeners of the city decided to use them as a support for their plantations during the summer months. This is a good way to optimize the use of these gangways, which would barely be used once a year otherwise.

6 Toward flood resilient networks and territories

6.1 Many stakeholders to be put in contact

It is vital that as many stakeholders as possible take part in this process of vulnerability reduction. It is especially the case for networks operators, since they are the only ones who can diagnose networks vulnerabilities, help to understand the dependencies between them and their consequences, and suggest solutions to improve the situation. It is all the more important to mobilize operators since many local authorities have delegated networks management to them. Thus they may lack knowledge concerning these networks.

Many types of stakeholders are concerned by the process: local authorities, State services, running operators, maintaining operators, users… The process of vulnerability reduction is meant to be collegial, mobilizing all operators at once, even if each operator may also be guided and followed individually. A collegial process is indeed a good way to emphasize dependencies and cascading effects.

Hence the role of the local authority that manages the area on which the process is carried out is essential. It re-attaches operators to local issues, to the users. The local authority is there to give them a common methodology, a common knowledge of the flood hazard. It is the place where information can be gathered, combined, analysed and shared. Even if the process request comes from a superior administrative level, the role of the local authority remains important to keep it operational.

For operators, that kind of process is an opportunity to get data concerning the flood hazard, or to get familiar with the planned proceedings and the representatives of public services and other operators.

Working groups or exercises are a good way to keep up the issue of networks vulnerability reduction.

6.2 Planning is vital

6.2.1 Improving the knowledge of networks vulnerability for a better planning

Having a better knowledge of networks vulnerability is very useful, even without being able to reduce it. Indeed, this knowledge is also very important in order to face these vulnerabilities.

It allows each operator to take into account internal and external disruptions when planning his organization to face floods in order to maintain his activity, or at least to limit damage. As they share their flood emergency plans, operators can notice duplicate measures, and thus mutualize their efforts. Operators may also find out that some of their planned measures are incompatible (in the timing of their settlement for example) or prejudicial for another operator. Then they can work together to find out new solutions.

As the operator knows what may fail first or what type of component may be predominantly damaged, he will be able to adapt his emergency teams and his back up material stocks. Aware of the flood risk, the operator can position this back up stock away from flood prone areas, but even so near from areas at risk. This knowledge is also a good indicator to establish priorities in the long term program toward the reduction of networks vulnerability to floods.

Being informed about what will happen to networks in case of a flood is useful for any user, within or out of the flood prone area. From businesses to local authorities, they all need to know if they will be able to keep working on site or not. If they need to evacuate because of the flood, they want to find a backup site they won't need to evacuate because of networks. Furthermore, the local authority, responsible for the crisis management of the global area, needs to know on which resources it will be able to rely on, and for which resources it will have to compensate. It can indeed have a major influence on the strategy chosen to manage the flood (e.g. to decide whether to evacuate a district or not).

Finally, as the local authority and the operator know the vulnerability of a network, they will be able to think about improving the situation every time they have an opportunity: regular maintenance works, new urbanization, urban renewal… Thus it may lead to a more adapted territory in the future.

It is important that all the stakeholders understand these advantages of sharing information to improve common knowledge about networks, so they will show goodwill to be part of it more easily.

6.2.2 Beware of uncertainty!

But the reality is not always that simple and obvious. In many cases, there are uncertainties concerning the flood hazard (height, kinetics…) or the reaction of the network (efficiency of measures, resistance of installations, or availability of the staff…). Thus one has to be careful when he plans for his crisis management.

For operators or users like local authorities or businesses, it can be wise to make provision for several backup solutions, like various withdrawal sites or several contracts for generator rental.

It is also very important that operators learn to plan their crisis management with realistic hypothesis, that is to say with a 'zero external services' hypothesis [17]. Operators plan their flood crisis management too frequently as if they were the only ones impacted.

Finally, training helps a lot to manage unusual situations, or situations that go beyond what was planned. So let operators train on their own, but also together and with local authorities. Exercises are also a great opportunity to share information, to confront flood management plans and to adapt them. [18]

6.2.3 The role of authorities in France

Authorities have an important role to play in the reduction of networks vulnerability. They have the means to give directions and goals to operators or to sensitive users (hospital, prison…).

At a local scale, authorities can reaffirm national directions and even reinforce them. They are the key to hazard data for operators. Local authorities have a central role to mobilize the stakeholders and to make sure they all have the same knowledge of the flood hazard. The local authority can lead the process towards more resilient networks, gather the information provided by operators and be the place to share and co-construct a less vulnerable territory.

The local authority is also the one that checks renewal or development project, so it can make sure that flood-adaptation rules are respected.

Finally, during a crisis, the local authority will be the centre of the crisis management. Thus it will coordinate the action of operators.

6.3 Awaited improvement

Local authorities that want to make progress concerning networks vulnerability to floods are looking for a model methodology, with standard questions, that would help them to find pertinent data and build a global project. Experiments have been carried out to find such methodologies and grids to analyse the vulnerability of networks and their dependencies. For example, a very promising study was held in Paris [19]. It highlighted how much networks are dependent from one another. It also led to the development of a digital tool to model networks vulnerabilities and the propagation of disruptions through them [20]. Another process was used in different areas in southern France. This one begins with crisis manager's needs, which emphasize vital networks. Then a collegial work is done to lead to solutions that can help to reduce the vulnerability of the networks [21]. Since it is difficult to carry out such processes that reach consensus with operators and local authorities, it is very important that stakeholders share this experience.

Another very promising project is one called ACCELL (for spatiotemporal evaluation of stakes located in flood prone areas, in the Loire catchment). Through a thesis lead between 2010 and 2013, the researchers built a tool that helps ordering the evacuation of a whole area, while taking into account the nature of people in each building (age, autonomy…), the traffic, the condition of roads (e.g. flooded or not) etc. It enables authorities to decide where people should be evacuated (several gathering points), when they should leave and which way they should take. [22]

7 Conclusion

The progressive reduction of networks vulnerability is possible, provided that developed strategies combine different types of solutions. Settling durable solutions requires a long lasting dialog between stakeholders. That means that we need temporary, maybe low quality solutions while waiting for an improvement of the situation.

Each local authority and operator is at a different level of progress. It appeared to us that the intervention of State representatives to launch or to follow such collegial processes is generally useful to give it impetus. The role of urban examining services is very important to make sure that the principles of the strategy are applied, and that every opportunity is seized to improve the situation of networks in flood prone areas.

Finally, we still need to work out synergies in order to make the reduction of vulnerability to floods more relevant and attractive. Every positive experience is worth being shared so everyone can make progress.

8 References

1. CEPRI (2011). *Bâtir un plan de continuité d'activité d'un service public*
2. OCDE (2014). *Etude de l'OCDE sur la gestion des risques d'inondation : la Seine en Ile-de-France – Rapport d'étude*
3. MEDAD, SOGREAH Consultants and DIREN Rhône-Alpes (2008). *Assistance à maîtrise d'ouvrage pour la mise en place et le suivi d'une démarche de réduction de la vulnérabilité des réseaux aux inondations du Rhône – Rapport d'étude*
4. Colin R. (1998). *Evaluation des conséquences des inondations sur les réseaux en Loire Moyenne*
5. Sternadel J. (2008). Galeries multiréseaux – L'expérience de Prague, *Travaux*, n°857
6. Guillois R. (2012). *Retour d'expérience dur l'inondation de novembre 2012 du métro de New York*
7. The City of New York (2013). *PLANYC – A stronger, more resilient New York*
8. HCFDC (2013). *RETEX suite à l'ouragan Sandy sur la côte Est des Etats-Unis*
9. Cabinet Office (2011). *Keeping the country running: Natural Hazards and Infrastructure*, United Kingdom
10. Department for Transport (2014). *Transport Resilience Review – A review of the resilience of the transport network to extreme weather events*, United Kingdom
11. CIRIA (2010). *Flood resilience and resistance for critical infrastructure*, C688
12. Cf. [1]
13. (2008) *Council Directive 2008/114/EC of 8 December 2008 on the identification and designation of European critical infrastructures and the assessment of the need to improve their protection*
14. Cf. [11]
15. OSORIO B. (2012). *Concepts and technologies for flood-proof road infrastructures,* FloodProBE
16. Cf. [1]
17. CGEDD (2013). *Vulnérabilité des réseaux d'infrastructures aux risques naturels*, Rapport n°008414-01
18. http://www.prefecturedepolice.interieur.gouv.fr/Sequana/EU-Sequana-2016
19. Toubin M. (2014). *Améliorer la résilience urbaine par un diagnostic collaboratif – L'exemple des services urbains parisiens face à l'inondation*, Thèse de doctorat, Université Paris Diderot

20. http://www.plateformesolutionsclimat.org/solution/creer-une-connaissance-commune-de-la-resilience-des-services-urbains/
21. CETE Méditerranée (2011). *Démarche RESAU² : Résilience des acteurs de l'urgence et réseaux – Guide méthodologique*
22. http://projets.plan-loire.fr/33695/35?plateforme=rdi