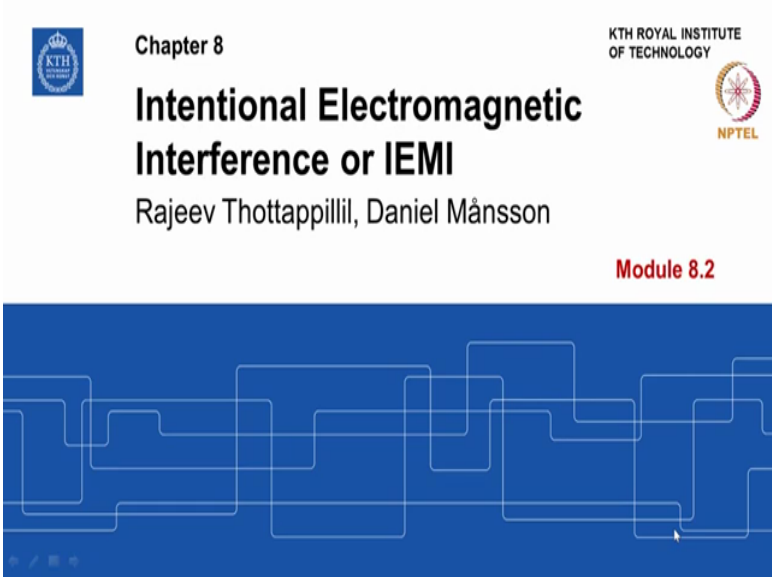
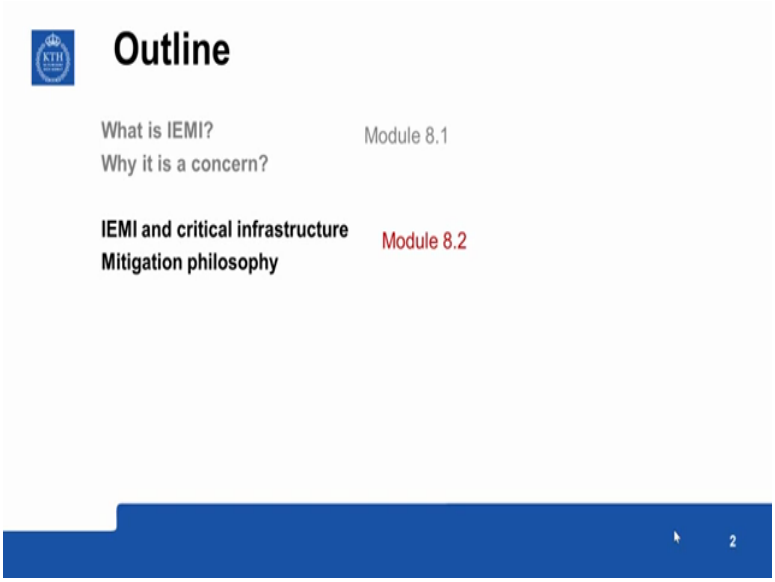
Electromagnetic compatibility, EMC
Professor Rajeev Thottappillil, Daniel Mansson
KTH Royal Institute of Technology
Module 8.2
Intentional Electromagnetic Interference or IEMI

(Refer Slide Time: 0:14)



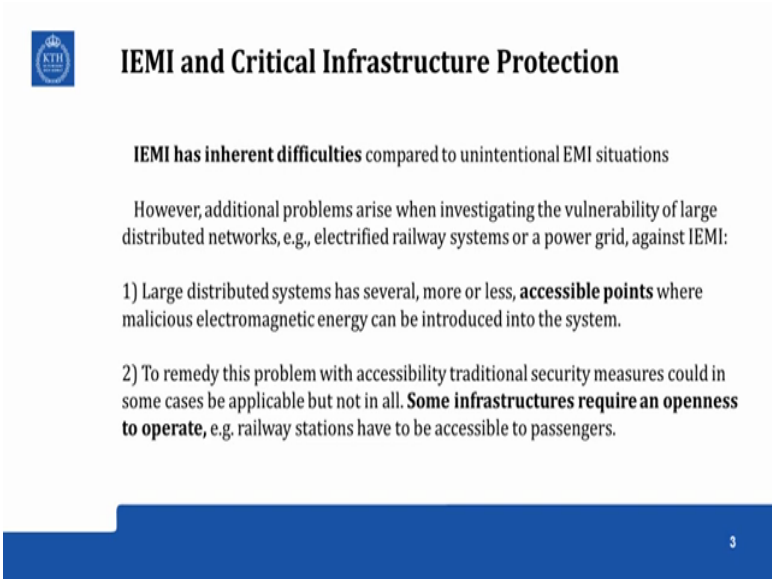
Intentional Electromagnetic Interference or IEMI module 8.2.

(Refer Slide Time: 0:22)



In this module we specialize on critical infrastructure, what are the special problems associated with IEMI scenario for critical infrastructure protection and discussion of some mitigation philosophy.

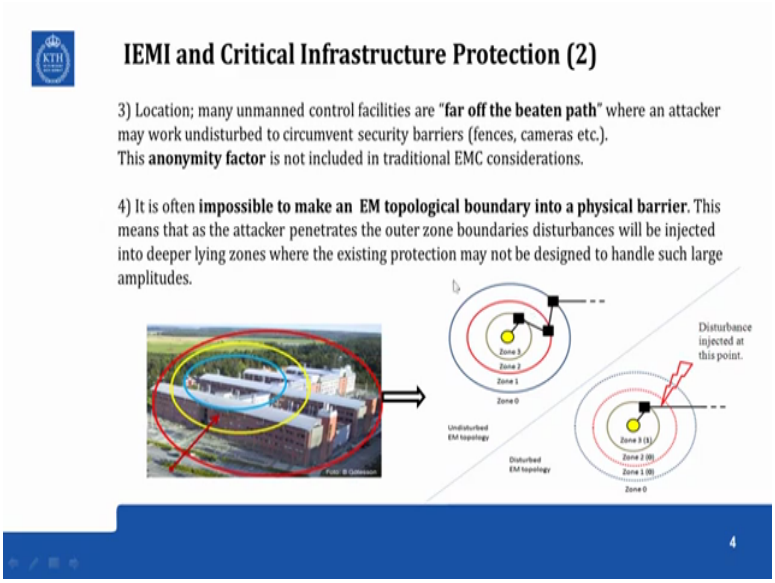
(Refer Slide Time: 0:42)



IEMI itself is a challenge and when it is applied to critical infrastructure it has got several other special issues. Examples of critical infrastructure are electrified railway systems, power grid, communication system, etc and all the systems are distributed systems spread over large geographical areas and that itself gives some speciality to it in terms of protection, main difficulty is how to estimate the vulnerability of such systems. It is very easy to estimate the vulnerability of very small system that are confined one can do test in the lab or one can you know inspect and know everything about the system and try to estimate the vulnerability, whereas distributed systems possess a big challenge.

One challenge is that it has got several accessible points where malicious electromagnetic energy can be introduced into the system and often you may not know everything about these accessible points because systems are so complex and distributed. Then we cannot restrict access to critical infrastructure often I mean to some points we can access say for example the control centre or critical equipments but otherwise it has to be quite open because people has to use it like a bank or railway stations, etc.

(Refer Slide Time: 2:48)



Then locations, some of the locations where critical infrastructure is present or in remote areas and you do not have normally any surveillance of those areas so far off the beaten path and there the attacker can you know try several times certain attack strategies and that becomes a threat. So the anonymity factor is normally not included in the traditional EMC consideration, whereas with critical infrastructure protection in the light of IEMI that has to be considered.

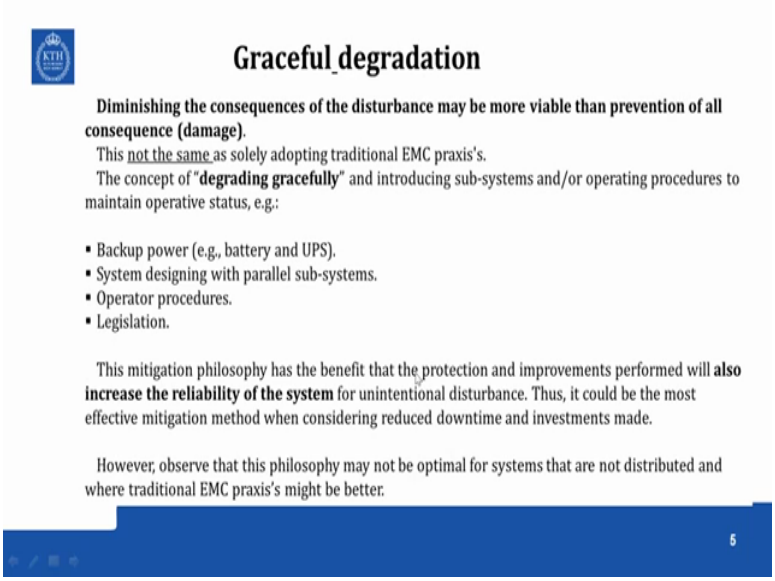
Another difficulty is that it is not possible to make an EM topological boundary into a physical barrier. So this we have seen in the previous chapter, so what is meant by this? This can be illustrated here. Imagine this is a building complex, well it is not a critical infrastructure but suppose that if it is a critical infrastructure it can be a very important control centre let us say.

Then well how do we protect the system using the topological zoning concepts? We can have several circles or several you know layers let us say need not be circles say for example outside of this building can be zone 0 where you can have all kinds of disturbances from severe sources. Then that there is a zone boundary from the topological point of view and anything any service that is going into or anything that goes into are controlled and its boundary can reduced to zone 1, then here the EM specification electromagnetic specification for sources are less severe compared to zone 0 because you have already mitigate, already reduced it, attenuated it with these measures at the boundary between zone 0 and zone 1.

Then between zone 1 and 2 again you have some controls and between zone 2 and 3 you have controls and by the time it reaches to the most critical and vulnerable part you have reduced your sources to such a great extent that the protection is realizable. Now imagine the case of IEMI scenario where you do not have a physical barrier between zone 0 and 1 the perpetrator can get inside can come across the doors and deep into the different zones EM topological zones and may be over here there is a boundary in terms of a lock room or something like that.

But the type of disturbance that you find in zone 0 can be suddenly introduced into zone 2 and only one boundary between zone 2 and 3 is now in between and this may not be adequate. So you are compromising the zone boundaries in the IEMI scenario, so this is a huge challenge.

(Refer Slide Time: 6:45)



So it is not often certain that one can have any full proof protection for IEMI in our cases especially when it comes to critical infrastructure. So often one adopt strategy of graceful degradation, so here the assumption is that okay there can be some attacks that is happening that are not always predicted by normal EMC standards of testing, then when this type of attacks happens the system will respond but make sure that system is gracefully degrading, it means that you do not have any catastrophic failure but system is degrading in the control manner so that still critical functions are going on and without any catastrophic failure it you know shuts down or something like that so this has to be built into the system.

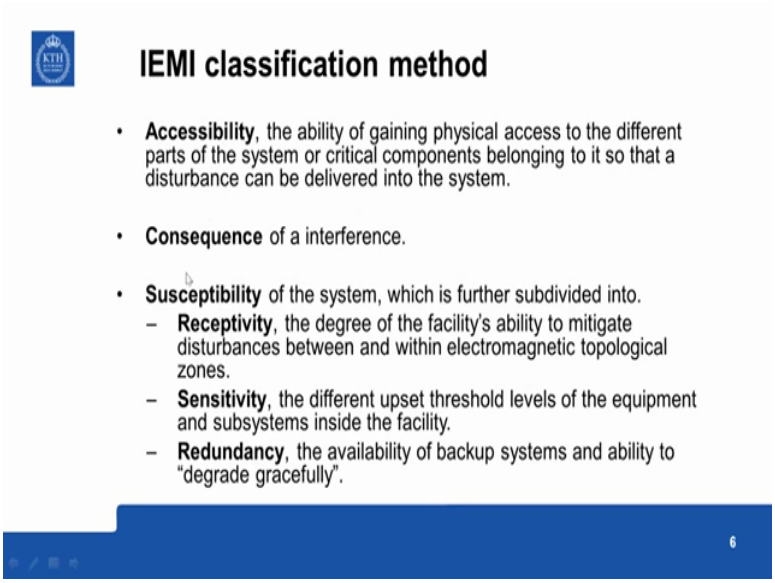
So diminishing the consequence of the disturbance may be more viable than the prevention of all consequence so that is a basic approach that is being taken in the case of IEMI. So it is not the same as just adopting the traditional EMC, it is much more than that. so the concept of degrading gracefully and introducing sub systems or operating procedures to maintain operative status. So you can decide that when the system is under attack and it cannot function normally as it should atleast some basic functionality should have to keep the most essential part of the system still running. So this has to be built into the system in terms of sub systems and operating procedures.

One common example can be backup power for all critical systems like battery, UPS and things like that with more extended capabilities and automatically kicking in. Then system designing with parallel sub system, so if one system is disturbed and all automatically a parallel sub system that can mimic the function can take into control and often parallel sub systems are widely employed when this comes to power control centres because even if one control centre is done then other control centres will take up the same function at geographically separate distance, so this often there with some of the critical infrastructure system so this is another strategy duplication of the control function.

Then operator procedures how to deal with there has to be establish procedures how to deal with suspected attack. Then legislation because when systems are build, economy is something very important and unless protection against IEMI or those type of rare events are built into the legislator into the rules, not enough money and resources will be allocated for this protection. So these are the various ways in which critical infrastructure protection can be approached.

The mitigation philosophy has the benefit that the protection improvements performed will also increase the reliability of the system even for unintentional disturbances. So if you design for IEMI surely it will have a extremely good design for normal EMC also, so that is a bonus point your overall reliability of the system is increased.

(Refer Slide Time: 11:08)



Now let us look at how we can put this type of philosophy into practise because it is one thing to know the principle involved but how do we quantify the system? Say for example how do we evaluate a system and say that okay this system is protected against IEMI or it has certain degree of protection, so this system is system A is more vulnerable to IEMI then system B or system C is more harden then system A and B so how do we say these kind of things by looking into evaluating a system? So you need some sort of a classification method and quantification of various factors so that is what is being talked about now in this.

So looking at the property and the process of IEMI one can think of a parameter accessibility that is how easy to gain physical access to different parts or critical components of a system because only when one is having access to physical access the disturbance can be delivered into the system, so how easy it is? So this is one scenario, so physical access means that it can be for a person or it can be for a signal or so it can be through some other means so this need to be evaluated.

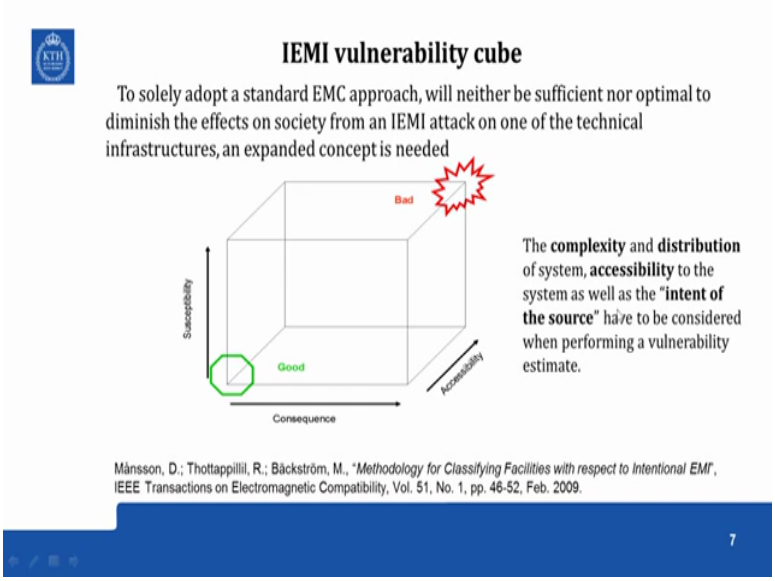
Second thing is if there is an interference what is a consequence? Because there can be systems in which you can have a interference system is getting damaged or it is getting down, temporary damage, upset but in the consequence may not be great in one system but similar kind of damage in that sub system but when it is used in a critical function can have much larger consequences so one need to have a measure for the consequence of interference.

Then susceptibility of the system, how susceptible the systems are to certain levels of interference at certain frequencies and all, so here it can be further divided into sub traces say

for example the receptivity to disturbance. You can apply a signal a transient to a system but the system may not be receptive to that. So the degree of the facility's ability to mitigate disturbances between and within electromagnetic topological zones so this is called receptivity because you have quite good protection, zonal boundaries and all so that need to be quantified.

Then sensitivity, the different upset threshold levels of the equipment and subsystems inside the facility how sensitive the systems are? Some systems may be too sensitive compared to some others so this need to be determined. Then redundancy, so even if one system is down can that function be taken over by another system and can this be taken over automatically without intervention of human beings? So this redundancy is associated with degrading gracefully so how do we combine all these three characteristics?

(Refer Slide Time: 15:38)



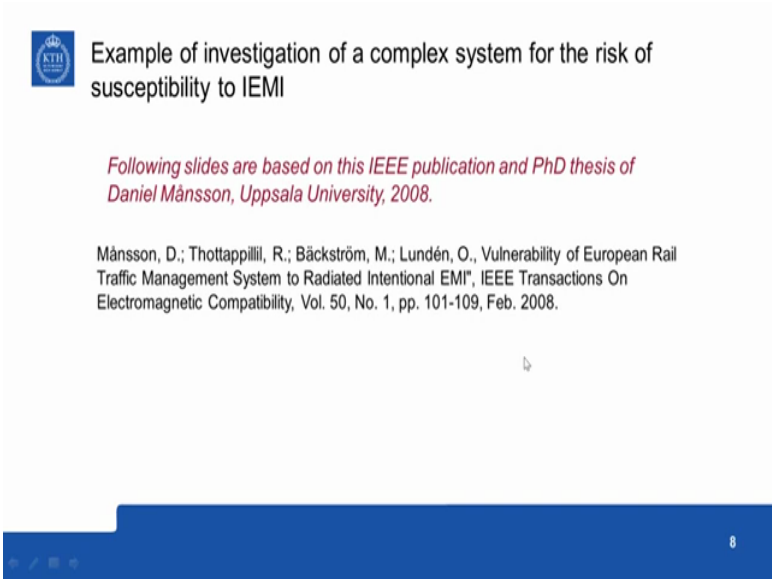
So one can think of a intentional electromagnetic interference vulnerability cube so this is taken from this publications (())(15:45) EMC. So in this cube you have three access, one is the consequence of an attack and first of all how accessible the system is accessibility in one access, then how susceptible the system is to the attack, then what is the consequence of the system being down or what is the consequence of the response of the system to the attack? So these three access one can quantify and plot.

Then suppose if you are in this corner somewhere then of course system is good, so the accessibility is bad you do not have accessibility system is not very good for the attackers even if this attack the susceptibility of the system is not that great it is not very susceptibility

so it is lower in this access. And even if something happens consequence is not great again lower in the access, so of course this is the ideal case but of course no case will be here, it can be that some systems the type of method being used in protecting the system is well make accessibility almost impossible.

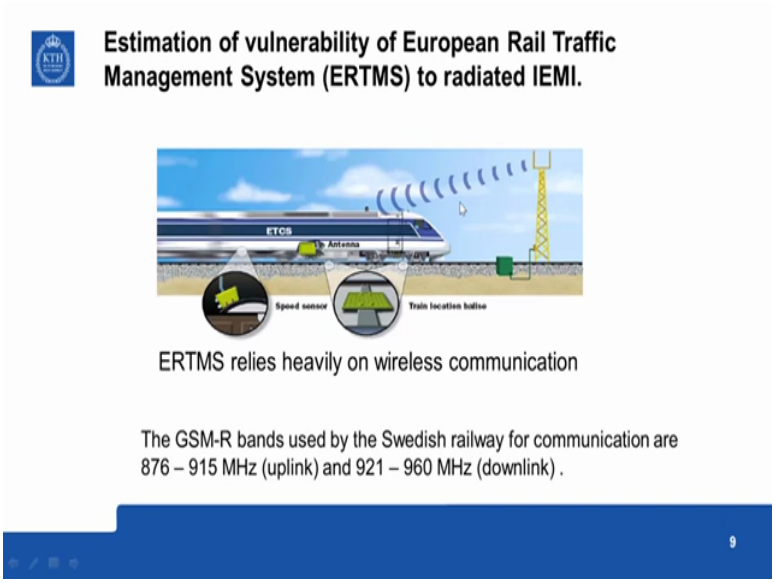
So if you do not have any accessibility even if the system is susceptibility and the consequence of the susceptibility is high you are still over here at this corner of the point. Then suppose if the system is not at all susceptible then you are kind of at this corner over here. So likewise you can consider different corners and if you can get it somewhere over here then that may be a fairly good system somewhere in the middle of the cube if you can get it so this is just a concept and each access has to be determined individually and quantified.

(Refer Slide Time: 18:38)



Now an example of investigation of a complex system for the risk of susceptibility to IEMI that is described in the next few slides so this is taken from this particular thesis PhD thesis as well as this publication in IEEE, EMC.

(Refer Slide Time: 19:02)



Now the system investigated is the European Rail Traffic Management System ERTMS and what kind of threat is posed to that system by radiated intentional electromagnetic interference. ERTMS is the upcoming railway signalling system railway control system that are being deployed in European countries including Sweden, already several lines are converted into ERTMS. So in the ERTMS system you do not have any optical signalling and you do not have definite blocks, so this will ERTMS will allow much more denser railway network, it is possible to have.

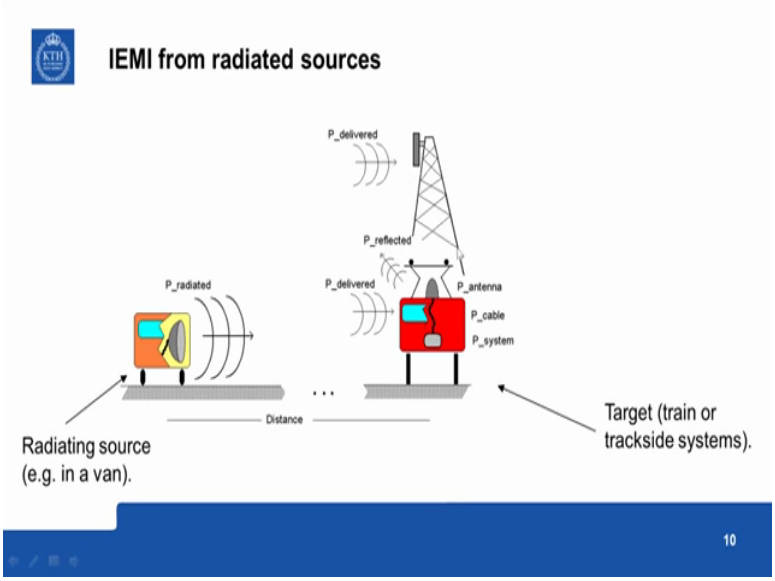
So trains can follow one another within a minute or so because you have kind of a moving boundaries for the block moving blocks and there are no light signals like green, red or ampere signals, instead everything is controlled by radio communication. So there are equipments within the train facilitating that in terms of several antennas and other things, then you have on the track also there are several equipments.

So in the train you can have speed sensors and in the track you have (())(20:38) embedded into the track the (())(20:41) will have information on what is happening ahead whether you have a block that is coming in or where is the next train and all kinds of information can be there in (())(20:55), so there are stationary systems on the track and (())(21:00) are normally you know broken in I mean turned on into life by an (())(21:08) that is being illuminated into it suddenly breaks up and it release its information to the train and train will now what has happened.

So all the (())(21:21) are there but the most critical thing for obvious are the communication system between the trains which uses this track side antenna and also to the stations. So these communication systems so they are called GSM-R communication systems and they are operating at this frequencies 876 to 915 megahertz and 921 to 960 megahertz for downlinks so these are the communication standards used in Swedish Railways for ERTMS.

So the investigation being conducted is that if someone is trying to disturb the communication you know how can we evaluate that threat if someone is aiming at this communication in tampering the communication.

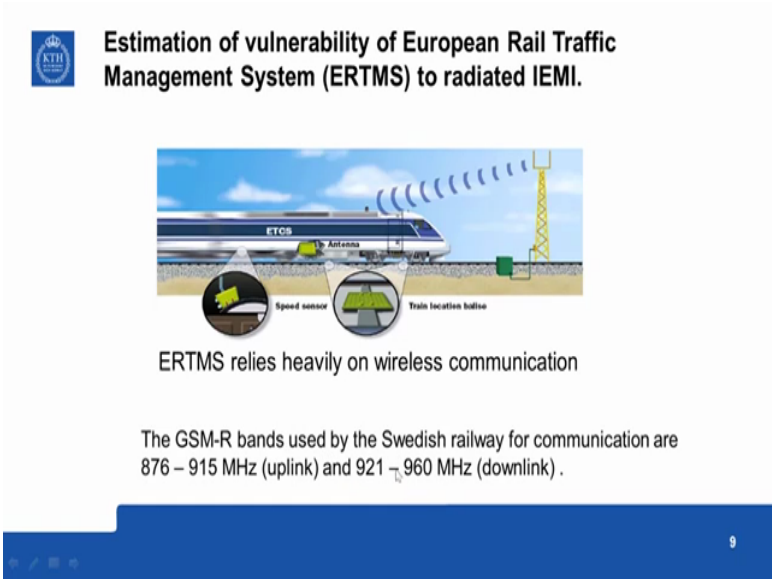
(Refer Slide Time: 22:24)

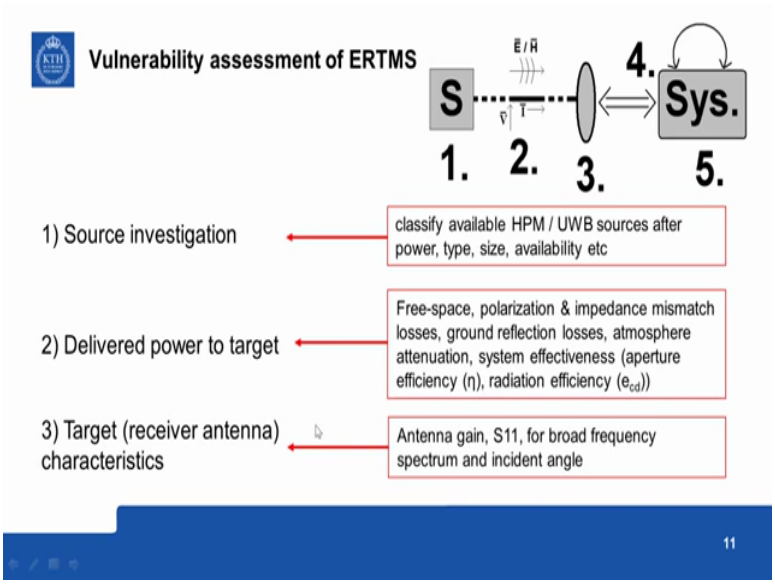


So the scenario is like this, suppose some wrong element is coming with a VAN with a powerful microwave or UWB or HPM sources radiating then either it can affect the train communication system the communication antennas mounted on the trains and the equipments in the train or the track side stationary antennas on (())(22:51). So what is more important is track side because that is stationary trains are moving.

So this study is presented now, so radiated power some of them will be attenuated you have to estimate that and some of them will be received here then it will be transferred to the electronics so all this one has to follow all this chains.

(Refer Slide Time: 23:25)





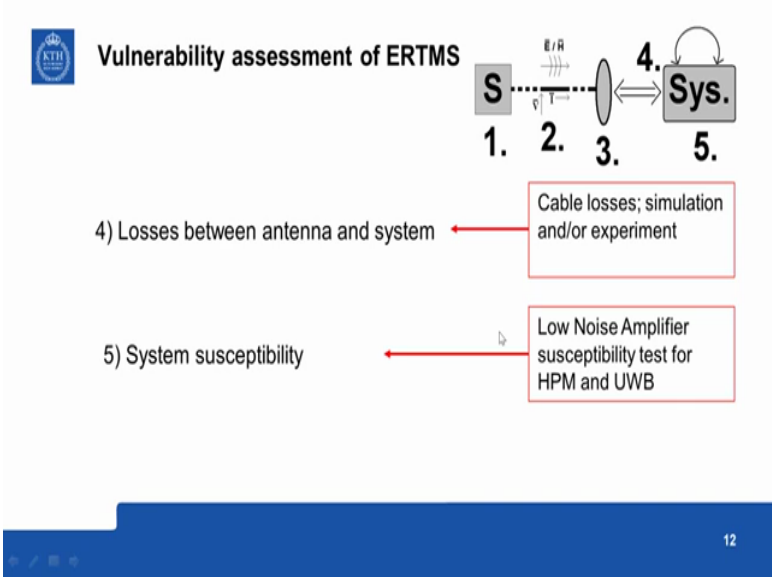
So we couple it with our standard EMC components in a system you can divide into source, victim, coupling path, etc so this figure standard figure comes in many contexts so basically the enhances method is the same except that regarding the source of investigation we will take not something that is naturally occurring but in this enrolment but something that is intentionally introduced.

So we will look at what are the available HPM high power microwave say for example a microwave oven or something like that in the public sector, classify available HPM and UWB sources after power, type size and availability because these are the kind of sources that will be available for perpetrators. Then suppose we know the source and how much power can be delivered to the target the track side antenna, so there we look into free space polarization,

impedance mismatch losses, ground reflection losses, atmospheric attenuation, system effectiveness for example aperture efficiency, radiation efficiency, etc so all these things are brought into picture.

Then after that you know that how much the target will be received, how much power will be or how much energy will be available at the receiving antenna, then of course receiving antenna has got certain polarization characteristics and because of that it has got certain gain and you know depending upon the incident angle what is being received can be different and here one need to be careful for the specification may be this bands but actual antenna work not only at this band because the antenna may be optimized to have maximum gain at these bands, but that does not mean that it is not responding to the frequencies outside this band, of course it will respond to frequencies outside that band also sometimes as effectively as this band so even that has to be considered while looking at the frequency spectrum of the wave following on the receiving antenna.

(Refer Slide Time: 26:28)



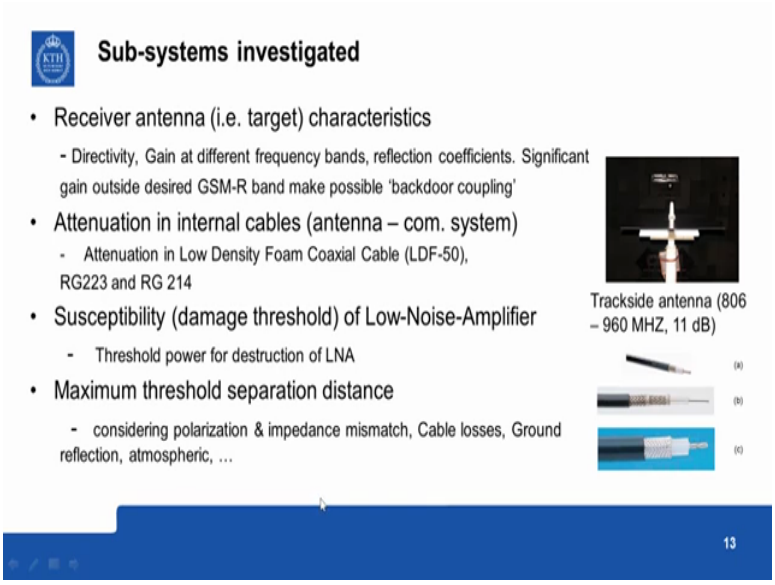
Then losses between antenna and system, so there will be cables from the antenna to the electronics certain length of the cables how much will be lost so you have to know about the cable characteristics and the pulse propagation along that cable, this can be found either by simulation or by experiments or using manufacturer's data. Then the signals are amplified the actual signals so of course the noise also will be amplified.

So there is a low noise amplifier (susceptibility) low noise amplifier (())(27:09) at the input the first stage of the electronics and how these low noise amplifiers because they are working

with several hundreds of megahertz or even bothering on gigahertz so how this will respond to the transients the intentional EMI of the characteristic of HPM and UWB so that need to be tested and see if those low noise amplifiers will be destroyed, so this is perhaps the most vulnerable part in the volt chain so one has to have very good idea about it.

So these are the several steps involved in the investigation and real systems were tested in (()) (27:59) chamber you using other test facilities.

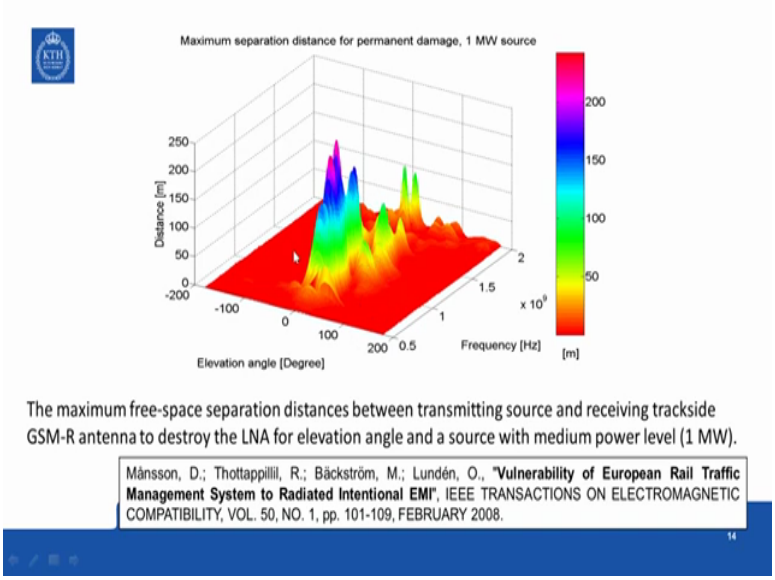
(Refer Slide Time: 28:04)

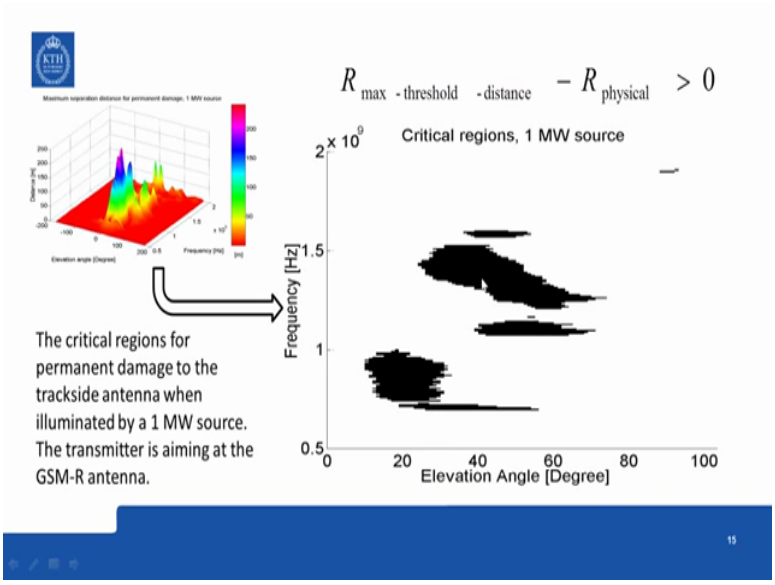


And the some of the details are given here. Say for example receiving antenna characteristics so this is the track side antenna one example of that. So directivity, gain at different frequency bands, reflection coefficients, significant gain outside the desired GSM-R band so that is kind of back door coupling all this were found out. Attenuation in internal cables between antenna and the communication system electronics so the attenuation in three types of cables that are used low density foam coaxial cable with a solid shield LDF-50, then braided shield cable RG223 and RG214 transferring (())(29:01) and all these characteristics attenuation all these are investigated.

Then susceptibility or damage threshold of low noise amplifier, what power is required for destruction of LNA and whether the signals reaching the LNA is above that values so this attenuation has to be made. Maximum threshold separation distance say for the given source that are available in the public domain what is the maximum separation distance required? Not to have destruction to the system so this should consider polarization, impedance mismatch, angle of illumination, cable losses, ground reflection, etc.

(Refer Slide Time: 29:56)





When one get into results like that so what is shown here is the maximum free space separation distance between transmitting source and receiving track side GSM-R antenna to destroy the low noise amplifier because that is the most sensitive part of the system for elevation angle and a source with medium power level 1 megawatt. So this may be like a small car mounted on (())(30:28) source.

So in this picture this is the distance between the receiving antenna and the source, this is the elevation angle at what elevation angle the source need to be of course not all these elevation angle are possible because practically you are at ground level and we (())(30:54) this on a mass so you have certain angle for the elevation, then this access shows the frequency upto 2 gigahertz and the colour coding is for distance in meters you can say 200 meters here, 150

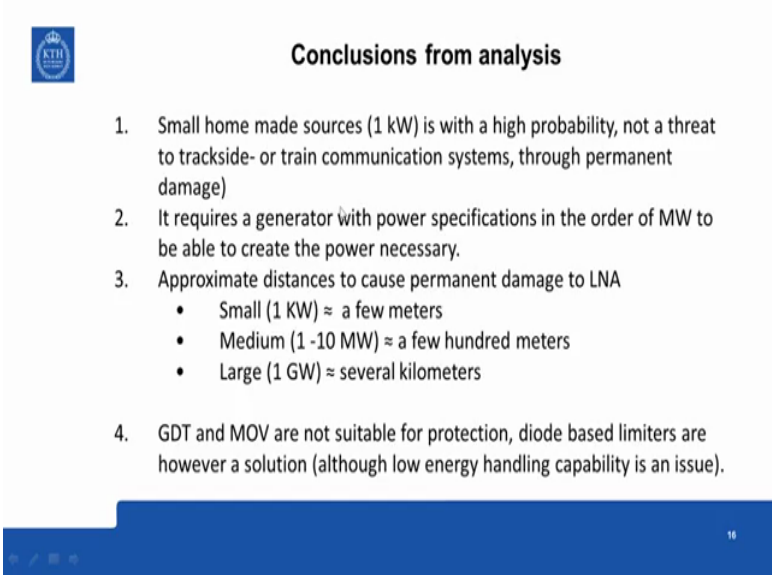
meters like that but mostly at this elevation angle so you have to have the bore side and as elevation angle increases then you have distances are also changing in frequency.

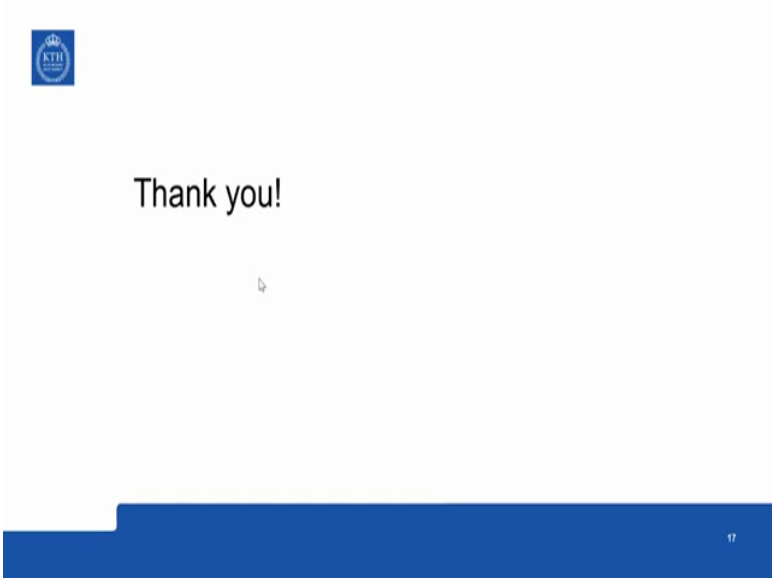
So this is a very complex picture in 3D and to get a more easily understandable figure one can translate that into this for example frequency versus elevation angle and what is shown here in dark are the critical regions so when the source is mounted in these regions with respect to the antenna then you can have disturbances. The critical region for permanent damage to the track side antenna when illuminated by a 1 megawatt source. The transmitter is aiming at the GSM-R antenna.

So say take the example of say 1.3 gigahertz you know the dominant frequency HPM source let us say so if the angle made between the receiving antenna and the source is around 40 degree or something like that you can have trouble over there, but if the distance is in such a way that the angle is beyond that then you do not have trouble. So likewise you know that where the van has to be positioned to be a threat to this antenna. So what does you know this you can make you can have physical barrier so that no one can approach the antenna at this vulnerable distances and angles.

So this is one way of achieving IEMI trying to achieve IEMI by doing the system analysis, I mean achieving EMC in the presence of IEMI using detail study of system analysis. You can see that we have used this classical EMC analysis here so there is nothing new in that, it is only a different way of thinking regarding the source and possibilities of approach of source to the victim that is being introduced.

(Refer Slide Time: 34:01)





Now the conclusion from this analysis as published in that publication you know small homemade sources of 1 kilowatt you know with a high probability one can say that is not a threat to trackside or train communication system, you may have maximum that can happen is some temporary absent but nothing is anything permanent. It require generators with power specification of the order of megawatt to be able to create the power necessary for permanent damage so that is much more harder to compile.

So the approximate distance is from the antenna to the source to cause permanent damage to LNA low noise amplifier, if it is a small source one has to come close as close as a few meters so you have to climb up the tower to be that is not usually possible. If it is a medium source 1 to 10 megawatt even from a distance of a few hundred meters one can have permanent damage that is along a road that is nearby or approach road. And if it is large you know military kind of systems with one gigawatt even from several kilometres one can do severe damage.

So one can clearly have an idea of how to characterize the accessibility to the source from this analysis and one has also found the susceptibility of the source from this analysis and identifying the critical system which is the LNA and we know the threat levels required for that. So this also can be quantified and of course consequence is that what is the consequence of train system? Of course trains can be stopped or the traffic can completely disrupted.

Now so one can reduce some special protection for this LNA, so normally there are some protection for protecting a (())(36:24) noise (())(36:26) etc. The gas discharge tubes and normal varistors may not be suitable for protection because GDT sometimes is low in

responding depending upon the rise time of the applied device and the MOV can have very large parasitic capacitors and inductance that is not suitable.

So often diode based limiters are used for this type of protection but one drawback is low energy handling capacity. So this is kind of a conclusion from the analysis and that ends this module, thank you very much.