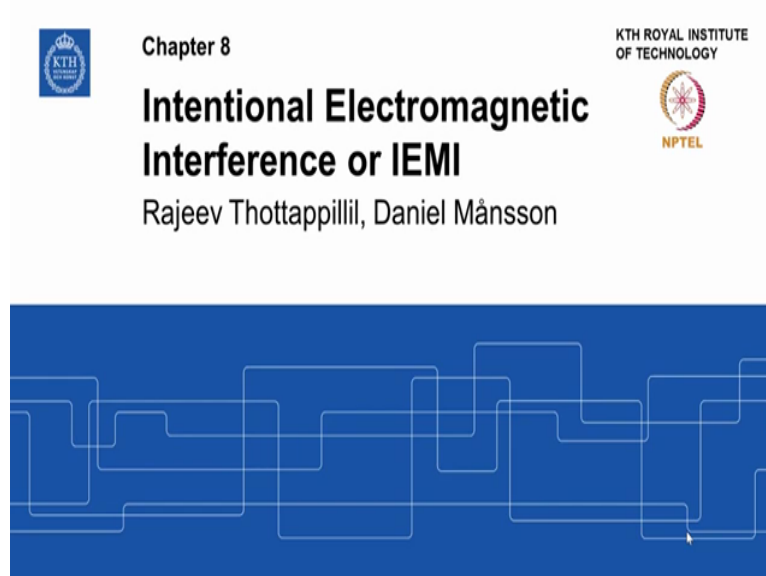


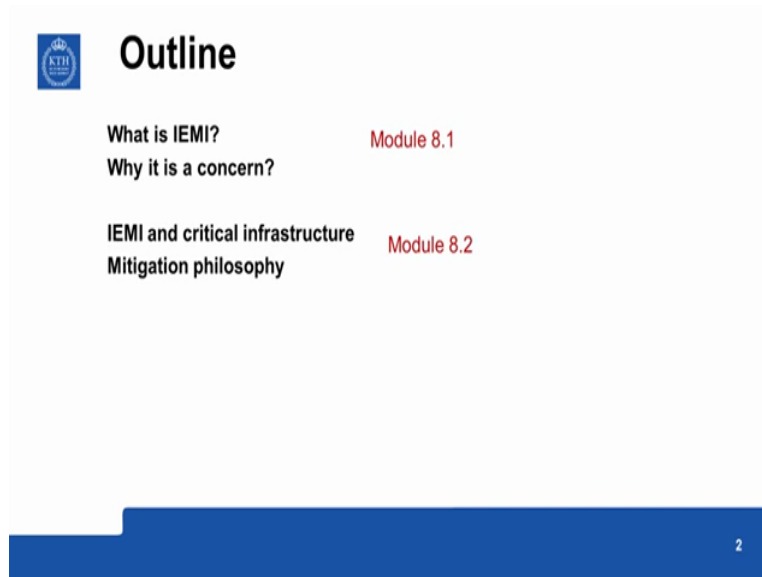
Electromagnetic Compatibility, EMC
Professor Rajeev Thottappillil, Daniel Mansson
KTH Royal Institute of Technology
Module 8.1
Intentional Electromagnetic Interference or IEMI

(Refer Slide Time: 0:17)



Chapter 8 intentional electromagnetic interference or IEMI, so far we have been dealing with EMC issues where the source occurs naturally either due to natural phenomena or due to the inherent nature of the equipments that we use interference created by equipments or by lightning. But it is also possible to intentionally create electromagnetic fields with the sole purpose of disturbing sensitive systems this can be done by wrong elements in the society or even enemy countries. So this chapter will deal with some of the special issues related to that type of a scenario.

(Refer Slide Time: 1:14)



The slide features the KTH logo in the top left corner. The title "Outline" is centered at the top. Below the title, the content is organized into two main sections. The first section, "Module 8.1", includes the topics "What is IEMI?" and "Why it is a concern?". The second section, "Module 8.2", includes "IEMI and critical infrastructure" and "Mitigation philosophy". A blue footer bar at the bottom right contains the number "2".

Outline

What is IEMI? Module 8.1
Why it is a concern?

IEMI and critical infrastructure Module 8.2
Mitigation philosophy

2

The outline, so first module 8.1 we will look at what is meant by IEMI? What are the main characteristics and how intentional EMI is different from the normal electromagnetic interference issues and why it is such a concern now? Then after that in module 8.2 we will take the critical infrastructure, critical infrastructure means you know in society power lines, communication lines, economic infrastructure so everything that is required for the smooth functioning of the society because often for the wrong elements this type of critical infrastructure is attractive target. So we will look into what are the special issues related with that and talk about the mitigation philosophy applied to IEMI.

(Refer Slide Time: 2:19)



The slide features the KTH logo in the top left corner. The title "Intentional Electromagnetic Interference (IEMI)" is centered at the top, with "Module 8.1" in red text to its right. A central text box contains a definition of IEMI. Below this, there are two paragraphs: one for "Unintentional EMI" and one for "Intentional EMI". A blue footer bar at the bottom right contains the number "3".

Intentional Electromagnetic Interference (IEMI) Module 8.1

"Intentional malicious generation of electromagnetic energy introducing noise or signals into electrical and electronic systems, thus **disrupting, confusing or damaging** these systems for **terrorist** or **criminal** purposes"

Unintentional EMI. Taken care of by legislation and standards, e.g.:

- European directives requiring CE marking and other international and national standards on EMC
- Special directives for civil aircraft issued by civil aviation authorities.

Intentional EMI. In civil scenarios often denoted *Electromagnetic Terrorism*. Usually much higher threat levels than unintentional EMI

3

First of all what is meant by intentional electromagnetic interference? It is often defined by this following code “intentional malicious generation of electromagnetic energy introducing noise or signals into electrical and electronic systems, thus disrupting, confusing or damaging these systems for terrorists or criminal purposes”. So here there are several elements to it, first of all in IEMI there is a component of intention, it is something not that just happens it is intentionally created.

So that itself introduces several challenges, we will see that, then this whole purpose is not any useful purpose it is for disrupting, confusing or damaging these systems. So it is not just accidental, then the idea is to create chaos into that particular system or particular establishment.

Now unintentional EMI, that is usually taken care of legislation and standards and we have seen EMC testing and standards in the previous chapter and we have seen the different principles that are used in protecting the systems. So unintentional EMI are usually taken care of by this type of measures and say for example if any product is marketed in European union the European directives requires the CE marking that you can see in the products and other international and national standards in EMC are also available in all countries.

Then when it comes to aircraft you have much more stringent condition for EMC because of the catastrophic consequences of (EMC) EMI into aircraft. So there are special directives for civil aircraft issued by civilian aviation authorities including protection against lightning one of the severe electromagnetic disturbance that you can find in the aviation circles. So all this will take care of unintentional EMI.

Now when it comes to intentional EMI you know it is still developing the regulations and other things and often it is so difficult to make regulations because often it is the intent that creates these problems. So in civil scenarios it is often denoted as electromagnetic terrorism because it is for terrorising the civil society that sometimes you know this type of issues comes and the levels of EMI are usually much higher the threat levels are much higher than unintentional EMI because there is an intention behind it.

So it is much more complicated to take care of intentional EMI situations using the normal civilian standards, so that is the focus of these modules.

(Refer Slide Time: 6:20)



Reasons for the society's increased vulnerability to IEMI.

Victim side	Source side
Our society is today extremely dependent on interconnected electrical and electronic systems for its function.	Vulnerability to EMI of critical systems invite terrorists or criminals to intentionally damage those systems.
Increased use of sophisticated and sensitive COTS (Commercial Off The Shelf) electronics for critical equipments.	More components available that can be assembled to homemade sources. Much information via Internet.
Miniaturization of components and lower signal levels are used in systems.	More commercial EM sources that can act as weapons.
Legal EMC-requirements for civil products are in general insufficient for protection against IEMI. Civil aircraft is the only major exception to the rule.	IEMI attacks (rather than traditional terrorist acts) can be performed anonymously and covertly

4

Now why the reasons for societies increased vulnerability to IEMI, so why society is increasingly vulnerable to IEMI? So there are different reasons for that so we can look at these reasons from let us say from the victim side or looking from the source side. So from the victim side we can see that society is extremely dependent on interconnected electrical and electronic systems for its function, this was not like that several decades ago.

Now imagine in (7:06) societies if there is a power outage due to certain incident you know wide spread power voltage then power is gone communication systems will die down soon because battery backup will be gone, then water distribution system, transportation system all of them are dependent upon power and communication or financial transaction systems.

So you can imagine a scenario in which there is no power in the society for you know several hours and all the systems can be disturbed and since modern society especially in the western societies these systems are so well functioning that you do not often have backup, normal homes or normal business establishment do not have backup power generators because power voltage is such a (8:08) phenomena, then increased use of sophisticated and sensitive commercial of the shelf electronic for critical equipments.

Now several decades ago often in critical equipments there are especially made components being used made for that and one can harden the systems as one (8:37) but due to the pressure to reduce cost and other reasons often now you know commission of the shelf

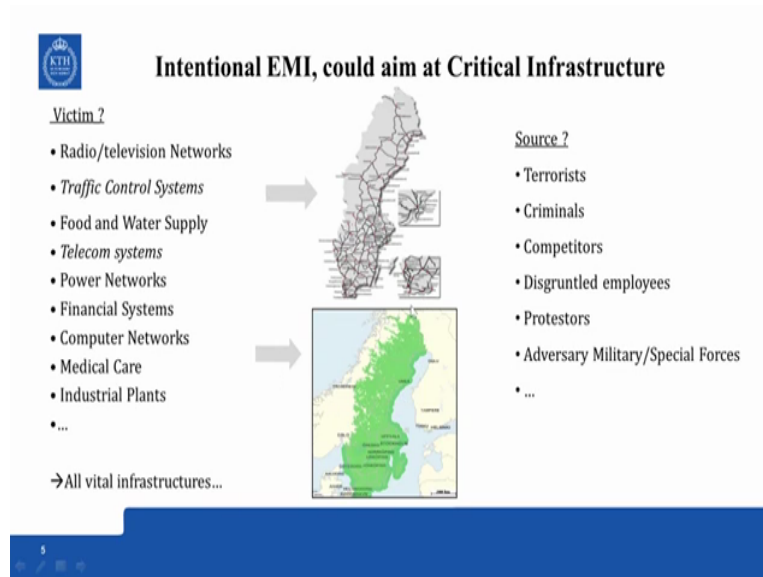
equipments are used for even for critical systems because you need so many systems and it is often easier to buy those things rather than mixed specifically for those applications.

So these system are tested against normal EMC in its normal environment, so they are not really meant for (9:17) intentionally created EMI, when the miniaturization of components make it that even normal level of signals are used in the system and you do not require that high levels of disturbance to penetrate into a system for destroying it, then legal EMC requirements for civil products are in general insufficient for protection against IEMI because you do not expect such high levels of source or maybe civil aircraft is the only major exception to the rule because there you specifies such a high level of EMI you expect such high levels of electromagnetic interference that civil aircraft can withstand usually IEMI scenario.

Now on the source side you know this is kind of a dual system when the society is becoming more and more dependent on interconnected electrical and communication systems for smooth function terrorists and other criminal elements are more attracted towards targeting those type of systems so there is a motivation for them to do that and often they can do this type of attack anonymously because you do not leave any trace behind unlike other type of sabotage electromagnetic sabotage does not leave that much stress behind because it is just a transient event.

And more components are available that can be assembled to homemade sources, even microwave that you use in homes as a powerful source a powerful microwave source which couple with antennas can be made as a good electromagnetic weapon and there is lot of information in the internet and expertise is widely available nowadays and even commercial high power EM sources can be just bought of the market like use (11:49) and other (11:51) are freely available which can be converted into weapons. Couple with this availability of sources and anonymity that IEMI attack often provides becomes more attractive for the criminals to use those type of methods.

(Refer Slide Time: 12:15)



Now a biggest concern regarding intentional EMI is critical infrastructure for various reasons you know if you have a small device with well-defined boundary that can be measured in submitters I mean like a cube or something you can encase it in steel armour or you know shielding and such protection components occurs of EMC mitigation we have used just increase the specifications and you can have fairly good protection against IEMI also, but that is not possible with distributed infrastructure.

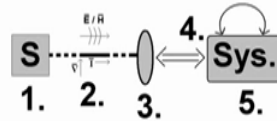
Say for example if you take Sweden this is map of Sweden, many of the critical infrastructure it expands the whole country that is more than 1000's of kilometres and they are all interconnected radio television network, traffic control system, food and water supply, telecom, power financial system, computer networks. So if power and telecom is targeted often the rest of these things (())(13:29) so they are all interconnected.

And the sources can be wielded by criminals, competitors you know if it is kind of industrial complexes, disgruntled employees there were cases like that when disgruntled employees were trying to sabotage their own factories or business establishment, protestors, then even military adversaries you know because IEMI does not leave much stress behind and then even without declaring a war one can target you know other countries infrastructure so these are the issues.

(Refer Slide Time: 14:22)



Knowledge needed for reaching a state of EMC in case of IEMI more difficult:



- 1) A source has to be defined (frequency envelope, power, polarization, angle of incident etc.)
- 2) Coupling paths of the electromagnetic energy, (near/far field situation, properties of medium or e.g. Cables)
- 3) Receiver boundary (apertures, filters, etc.)
- 4) Internal coupling of receiver (re-radiated; absorbing material, ground planes etc.)
- 5) Response of component.

6

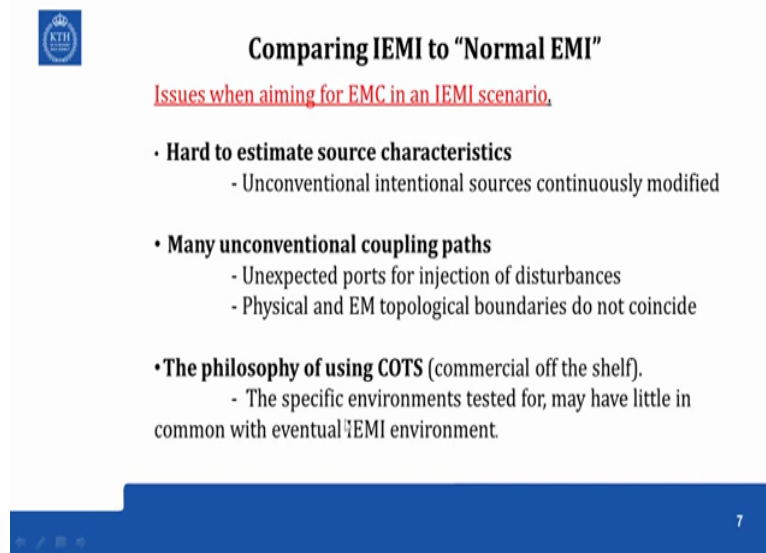
Now we have seen this classical picture from before the basic decomposition of an EMC problem. So you can have a source and you can have a victim and there is a coupling path in between source and victim. So 2 is the coupling path, 3, 4, 5 are you know the victim where you have this front door kind of coupling then internal coupling and the system plus powers etc.

Say for example a source has to be defined for a sample frequency envelope, power, polarization, angle of incident, etc and one of the basic talents of EMC I mean EMI mitigation strategy for achieving EMC is that we know something about this source that is going to happen in that equipments normal environment of use. So we have some idea about frequency envelope, power, polarization, angle of incident, source characteristic, etc. So this is a basic assumption, with IEMI we do not know we cannot be sure because you know it can be any source.

Then coupling paths of electromagnetic energy because it is near or far field coupling, properties of the medium whether it is conducted coupling through cables, etc we have some knowledge. And receiver boundary what are the apertures, filters or the equipment, etc. Internal coupling of the receiver whether things are re-radiated, what are the absorbing materials there, ground planes this knowledge we have. And response of the component how the system will respond so this is we tried to understand all these 5 elements in a normal EMC scenario.

Even IEMI this is the same strategy that we will be using, so there is no difference in the approach, the only thing is that we need to have some extra thinking to be put into those. So this we will see with an example later in later in the module 2.

(Refer Slide Time: 16:54)



The slide features the KTH logo in the top left corner. The main title is "Comparing IEMI to 'Normal EMI'". Below the title is a red underlined heading: "Issues when aiming for EMC in an IEMI scenario." The content is organized into three bullet points, each with a sub-bullet:

- **Hard to estimate source characteristics**
 - Unconventional intentional sources continuously modified
- **Many unconventional coupling paths**
 - Unexpected ports for injection of disturbances
 - Physical and EM topological boundaries do not coincide
- **The philosophy of using COTS (commercial off the shelf).**
 - The specific environments tested for, may have little in common with eventual IEMI environment.

At the bottom right of the slide, there is a blue navigation bar with a white number "7".

Now comparing IEMI to normal EMI, issues when aiming for EMC in an IEMI scenario so let us look into that and try to see what are the difference between normal EMI and IEMI situation intentional EMI situation. First of all regarding the source in normal EMI we assume that we know something about the source in that particular environment but however in the IEMI scenario it is very hard to estimate the source characteristics because we do not know what kind of source the (())(17:38) will be having so unconventional intentional sources are continuously modified, so you need to have a continuous evaluation of the perception based on freely available technologies in the society.

Then in normal EMI we have a fair idea of the coupling path, say for example if you have a building and if there is a lightning happening to that building we know that okay it is the air termination where the lightning will be attaching to, but of course you can have lightning type of pulses that can be generated in an equipment I mean at least small lightning can be generated by small equipment and if these type of things are directly injected into a cable coming into the building or a power socket outside then of course the building is not designed for that type of source appearing in that type of places.


So you can have many unconventional coupling path because of that, so unexpected ports for injection of disturbances, so this is a big challenge in the IEMI scenario. And therefore the

physical and electromagnetic topological boundaries do not coincide. Say for example you know perpetrators can come into a building with powerful sources unless there is a possibility that these type of sources can never enter that area.

Suppose if electromagnetic topologically we have defined zone number 1 like that and defined what are the sources inside zone number 1 and if we do not have a physical boundary for that then perpetrators can bring in sources more powerful into that particular zone. So this is what is meant by that physical and EM topological boundaries do not coincide because you do not expect a lightning type of pulse directly striking inside a building, whereas in the IEMI scenario it is possible to that I am just giving an example it can be some other source necessarily lightning.

Then the philosophy of using COTS commercial of the shelf, so that equipments are tested for specific environments where normally it is meant to be used and it may have very little common with eventual IEMI environment because the normal COTS equipment that used in a place where you know it is not an attractive target for perpetrators then of course it will function in that environment but when it is used in the environment where someone is targeting with an IEMI source then it will not function.

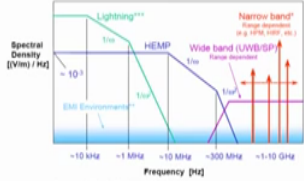
(Refer Slide Time: 21:22)



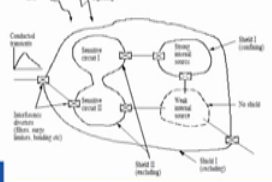
The challenge of Intentional EMI or IEMI

- Difference between EMI and IEMI (intent)
- Compromise of zoning concepts
 - Topological and physical boundaries do not coincide
 - Unusual port of entry
 - Unexpected source characteristics
- Significant challenge for large distributed systems like railways

Possible spectra of IEMI



EMI Environment



Zoning principles may be compromised

So the challenge of intentional EMI we have seen that the main difference between EMI and IEMI is the intent and because of this intent it is very hard to predict what resource will be in a given situation. So this picture you have seen what are the possible spectra, possible EMI spectra. Now we have to say that the (())(21:53) spectra can have the potential to be used for

IEMI attacks. So it can be even injecting a DC current into a ground telecommunication ground to create disturbance.

So here in the spectra you know you have this lightning spectra, you have normal EMI environment spectra 10 kilohertz, 1 megahertz upto few megahertz you can have, then you have HEMP nuclear EMP high altitude electromagnetic pulse that can go upto few hundred megahertz, then you have now other type of sources used in military and other scenarios. For example you have narrow band high power microwaves and high intensity radiation fields, so they are basically short bits of sinusoidal pulses at you know few gigahertz if you take the frequencies so it will be very narrow band you know like very targeted kind of band. So military system use this, there are HPM weapons used by military in destroying enemy systems and all so these are narrow band system.

Then there is another type of pulse ultra wide band so the more definition you will see in the next page, so ultra wide band is also a big concern. So as the name suggest it is a impulse wave not sinusoidal but just an impulse and impulses have what very wide frequency bands so frequency band can be of the order of hundreds of megahertz for this and they are not be of extremely high power compared to HPM maybe of less power but then attractiveness of this as IEMI source is that it can excite several frequency bands in the equipment where it can introduce some resonances and all.


So with HPM enrol it is just one narrow band and if you strengthen those narrow band protection against those narrow bands then of course your equipment is saved, but with ultra wide band it exposes the system to extremely wide frequency range and unfortunately there can be some frequencies where the system may go into resonances or it may be susceptible. So this is what difference between EMI and IEMI intent. So the (0)(24:55) frequency spectrum is open for IEMI.


Then compromise of zoning concepts, zoning principles may be compromised we have seen in chapter 5 what is the electromagnetic zoning principles like say this is zone 0, where EMP and lightning and all kinds of things may happen then inside you expect that this shields and other interference, diverters will reduce the intensity of the sources to certain level. So you have some idea of what these levels should be then again to sensitive circuits you have another zone (2) 0, 1 and 2 so there it will be even less.

But this is workable with naturally occurring EMI and normal equipment EMI but if suppose this is a big industrial complex and someone is entering with a source hidden then immediately you are you know breaking this electromagnetic topology (())(26:17) boundary because there is nothing preventing that person from entering with a source inside. So once can come to the most sensitive part of the facility and you have a source that is totally unexpected.



So compromise of zoning concepts is possible in the IEMI scenario, topological and physical boundaries do not coincide, you can have unusual port of entry that normally you do not expect and unexpected source characteristics so all these things are possible. Then this is especially a big challenge for large distributed system like railways because if it is an industrial complex or an equipment you can have the zone boundaries like this I mean to some extent, equipments it is possible you can protect (())(27:11) even with a physically limited industrial complex you can try to have some sort of like a nuclear reactor complex you can have some kind of a control but completely distributed system like railways, power systems, communication system, etc it is more difficult.

(Refer Slide Time: 27:40)

 Unexpected port of entry - example



- Locked perimeter fence
- Steel plate construction (wood covering)
- No windows or openings
- Power socket outside
- Cables from underneath



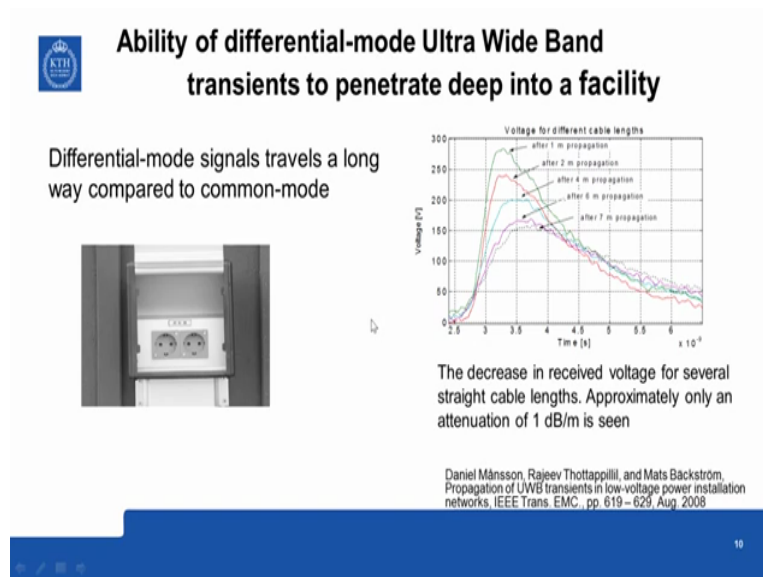
9

Now we will see some example unexpected port of entry, this is an example of a control centre automatic control centre for railways you keeping track side equipments you have a antenna on top of this mass for communications, etc and cables going into the building. So nicely constructed building with shield cladding inside, no windows, there is a perimeter fence so (())(28:15) is very difficult, etc but at the same time perimeter fence is mainly for keeping out animals and people straying into it you know out of curiosity not meant for

someone determined to get into the things. Say for example you can easily scroll into using this through these gaps, etc.

Then once you come to the building you have equipments outside power sockets outside and the building is on top of pillars like this so you have all kinds of cables coming inside so it is very easy to access the cables and power sockets outside, but in the normal EMC scenario you do not have to worry about it because you do not expect any these are just for convenience these power socket outside for cutting the grass and other maintenance things, but if someone is injecting in high impulse into this then it goes into the sensitive system inside distributed into inside or through the cables it can be you know (())(29:31) can be brought inside. So this shows the unexpected port of entry in the case of IEMI scenario.

(Refer Slide Time: 29:44)

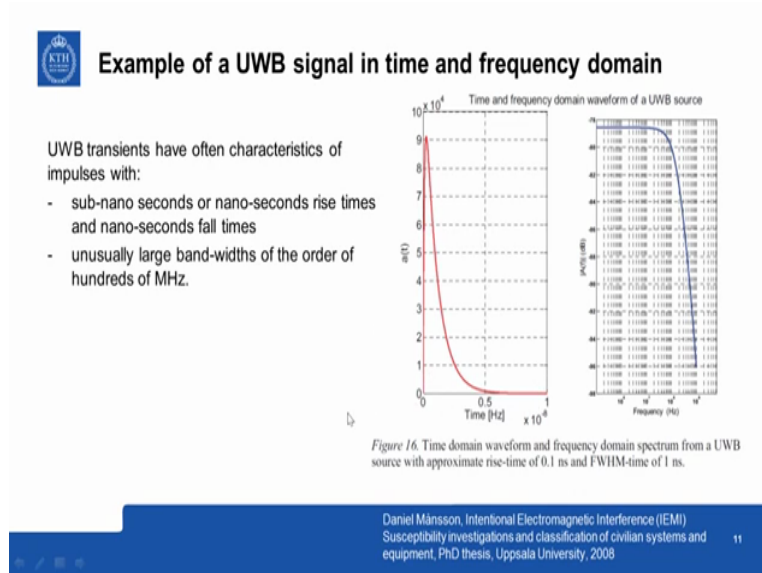


Now there have been experiments conducted that experiments are reported in these publications to see the ability of differential mode ultra wide band transients to penetrate deep into the facility, ultra wide band have extremely large frequencies and so often it is thought that okay it will be dissipating very fast, but not necessarily if it is in the differential mode, differential mode is more like a transversal dramatic mode with very loss very low loss.

So it can really travel a long way compared to common mode where most of the energies radiated out and dissipated. So this is from a generator differential mode signals that is injected in a building outside the power socket between phase and neutral or between one of these conductors on the earth wire, then you see how it is propagating inside after 1 meter of propagation you know you can you have this particular level of voltage and after 2 meters of

propagation this voltage, it is (31:08) but not fast enough, so you can penetrate deep into the facility in the differential mode ultra wide band.

(Refer Slide Time: 31:18)



Say what is meant by ultra wide band signal that can be quite attractive for perpetrators for IEMI purposes. So these are transient signals, so this is an example taken from this thesis that can have rise times sub-nano seconds rise times or even nano seconds rise times and fall times of the order of nano seconds. So here it is time so this is 10 nano seconds, 5 nano seconds so within few nano seconds the pulse is over.

So this has got extremely wide band so you can see that this is of the order of ten megahertz here, hundred megahertz here so you can have if you take you can have several hundreds of megahertz in bandwidth. So sub-nano seconds or nano seconds rise times and nano seconds fall times unusually large bandwidths of the order of hundred megahertz. So due to this large bandwidth it can excite several vulnerable frequencies within the victim.

(Refer Slide Time: 32:45)



Estimated Distance of Action for HPM Sabotage.

From HPM Tests of Cars, PC's etc. Unprotected Equipment.

HPM-SOURCE	DISTANCE			
	In close vicinity	15 meter	50 meter	500 meter
HPM Van ** (10 MW, 10J)	Irrelevant	<i>Permanent physical damage</i>	<i>Upset^{#)}/ Damage^{*)}</i>	<i>Upset^{#)}/ Damage^{*)}</i>
HPM Suitcase ** (100 kW, 0.1 J)	<i>Permanent physical damage</i>	<i>Upset^{#)}/ Damage^{*)}</i>	<i>Upset^{#)}/ Damage^{*)}</i>	<i>No Effect/ (Interference, in-band FD)</i>

#: May cause permanent functional damage!

*: Front-door coupling (FD) in-band (interference at much larger distance).

** : UWB/HPM gives similar distances, but permanent damage likely requires a very high PRF.

M. B. Backstrom and K. G. Lovstrand, "Susceptibility of Electronic Systems to High-Power Microwaves: Summary of Test Experience", *IEEE Transactions on Electromagnetic Compatibility*, Vol. 46, No. 3, August 2004

12

Now HPM are more narrow band, we have discussed that before high power microwaves you know shot short burst of sinusoidal waveforms separated in time, so they are quite narrow band. Now HPM has been you can have extremely powerful sources with HPM, so HPM sources have everything to do physical damage on common systems unprotected equipments, say for example cars, personal computers etc has been done in this publication so this table is taken from there.

So they have seen that if you have an HPM van so 10 megawatt source because they are quite huge, 10 joule energy capacity. So then you know well you do not come close to a critical system but suppose you are 15 meter away then it can create permanent physical damage and 50 meters it can do (upside) upset and damage and 500 meter it can create upset and damage so this may be one can recover from it or one can after sometime but when the source is ON the system is not available. Now HPM suitcase so in a suitcase it can penetrate much deeper into the vicinity so in the tool close vicinity it can come to the source is atleast thousand times less in power but still you know hundred times less but still you can have permanent physical damage in close vicinity and it is a threat upto several tens of meters.

When similar kind of effects can happen with ultra wide band or high power microwaves systems but permanent damage likely requires very high pulse repetition frequency. So there were several tests done like this on equipments to see what could be the possibilities and it is known that it is possible to disturb systems by you know sources that can be carried in small briefcases, suitcases 8.1.